The Price to Play: a Privacy Analysis of Free and Paid Games in the Android Ecosystem

Pierre Laperdrix, Naif Mehanna, Antonin Durey, Walter Rudametkin

The Price to Play: a Privacy Analysis of Free and Paid Games in the Android Ecosystem

Pierre Laperdrix
Univ. Lille, CNRS, Inria
Lille, France
pierre.laperdrix@univ-lille.fr

Naif Mehanna
Univ. Lille, CNRS, Inria
Lille, France
naif.mehanna@univ-lille.fr

Antonin Durey
Univ. Lille, CNRS, Inria
Lille, France
antonin.durey@univ-lille.fr

Walter Rudametkin
Univ. Lille, CNRS, Inria
Lille, France
walter.rudametkin@univ-lille.fr

ABSTRACT

With an ever growing number of smartphone users, the mobile gaming industry is booming and reached more than 2.6 billion players worldwide in 2020. While some mobile games charge a relatively modest fee to be played, the vast majority are free and rely exclusively on ads or tracking for their revenue streams. Over the years, Google and Apple have tightened their privacy requirements for apps. They perform thorough app scanning to detect abusive behaviours and require developers to provide a privacy policy on how they collect and handle user data. Yet, little is known about the data collection that fuels the advertising and tracking industry behind mobile games. Players can see the ads that are presented to them but they may not be aware of the invisible trackers that collect valuable data in the background.

In this study, we aim to shine a light on the tracking ecosystem in mobile games on Android and understand how different monetization models can impact user privacy. We introduce a pipeline that collects both free and paid games and we use the static analysis provided by the Exodus audit platform to detect the trackers present in them. We analyse a total of 6,751 games, including 396 paid games. Our results show that paying for a game does not necessarily shield users from data collection. We find that 87% of free games include at least one tracker, compared to 65% of paid games that do. On average, free games have 3.4 times more trackers and request twice more dangerous permissions than paid games. We also notice that the genre of the game and its targeted audience impact the number of trackers. Games in the *Casual* category presents the most trackers while those in the *Educational* one have the least.

CCS CONCEPTS

• **Security and privacy** → *Economics of security and privacy*; • **Information systems** → *Online advertising*.

WWW '22, April 25–29, 2022, Virtual Event, Lyon, France

ACM ISBN 978-1-4503-9096-5/22/04…$15.00
https://doi.org/10.1145/3485447.3512279

KEYWORDS

mobile games, tracking, online privacy

ACM Reference Format:
Pierre Laperdrix, Naif Mehanna, Antonin Durey, and Walter Rudametkin. 2022. The Price to Play: a Privacy Analysis of Free and Paid Games in the Android Ecosystem. In *Proceedings of the ACM Web Conference 2022 (WWW '22), April 25–29, 2022, Virtual Event, Lyon, France.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3485447.3512279

1 INTRODUCTION

Smartphones are in the pockets of 6.3 billion users, which represents more than 80% of the worldwide population [24]. As every single one of these devices has the capacity to play games, the potential market for mobile gaming is huge. In 2021, 2.66 billion mobile gamers [4] spent collectively more than $116 billion USD on mobile games [34], surpassing the revenue of all other gaming sectors combined [32]. As users were faced with a global pandemic, they spent more time at home and on mobile games [3] with a lasting effect and further gains that can already be observed in 2021 [30].

Amidst this booming market, publishers are exploring different ways to monetize their games, as detailed by Tang [47]. More than 95% of games on the Google Play Store are free [16], while the others can be accessed for a relatively small price with most paid games being priced under $10 USD. Games can also earn revenue by showing personalized ads to players or by selling in-app purchases (IAP) (e.g., to unlock levels, buy in-game currency). Inspired by streaming services, some games also offer subscriptions in the form of *battle passes* [8] that offer in-game rewards (e.g., extra content, boosts, skins, new levels). Although each of these methods contribute to generating revenue, as detailed by Unity's Game Report [5], ads and IAPs capture the lion's share of the revenue with IAP slowly starting to surpass advertising revenues in different markets.

Interestingly, at a time where online privacy is at the forefront of discussions regarding the Web, with the development of anti-tracking technologies [18, 20, 27], the upcoming deprecation of third-party cookies [7] and the design of privacy friendly tracking alternatives [31], mobile gaming seems to be have been saved from these discussions. On the one hand, users care about data privacy with 79% willing to spend time and money to protect their data [9]. On the other hand, the pervasiveness of ads and trackers in mobile games seems to be the complete opposite, where users accept opaque data collection and data sharing operations performed

by a lot of unknown tracking companies. A survey of US gamers conducted in 2018 revealed that 82% of users preferred free mobile games with ads compared to paid mobile ones without [1]. 74% would also watch an in-game ad if they get an in-app perk in return.

As ads are an integral part of mobile gaming, what implications does it have on users' privacy? What is the true privacy cost of free games? Does paying for a game up front truly ensures better privacy guarantees?

In order to answer all these questions, we analyse in this paper 6,751 games, including 396 paid games, and compare the trackers present in them. Section 2 describes the related work. Section 3 introduces the pipeline that we built to collect our dataset of games. Section 4 presents the result of our analysis by considering different dimensions like the number of trackers, the included permissions, the category of a game, its base price and its intended audience. Section 5 discusses our findings while Section 6 concludes our paper.

2 RELATED WORK

In the field of Android security, there is an extensive literature on how to analyse apps, through the use of static analyses to dynamic approaches or even instrumenting firmware or proxying traffic. Some examples include using taint tracking like Flowdroid [36], Taintdroid [37] or AndroidLeaks [38] to capture data leaks, explore how permissions can be circumvented to collect sensitive data [44], or simply look at detecting malware [42]. However, only a handful of studies look at the presence of trackers in mobile applications and if there are differences between free and paid applications.

Tracking in mobile applications. Razaghpanah et al. studied the mobile advertising and tracking ecosystem by analysing real-world mobile network traffic [43]. Thanks to an app called Lumen, installed directly on users' devices, they were able to capture where the data from mobile apps was being sent. They also traced back the parent companies behind many different tracking services and found, in particular, that Alphabet was present in over 73% of the 14,599 apps in their dataset. Finally, they discovered that 39% of the tracking services they identified were also present as third-parties in at least one of the Alexa Top 1,000 websites.

Reyes et al. analysed 5,855 of the most popular free children's apps on Android to see if they were compliant with the Children's Online Privacy Protection Act (COPPA) [45]. They instrumented the APIs that access sensitive resources and used Lumen to detect if data from those APIs was sent over the wire. Their results showed that 19% of tested apps collected identifiers or personally identifiable information that should never have been transmitted.

Kollnig et al. compared the same 12k apps on both Android and iOS to see if there were any differences in terms of privacy [41]. In the end, they found no significant differences between the two platforms despite different architectures and requirements from both app stores. 88% of Android apps had at least one tracking library, while 79% of iOS apps did. In both stores, about 3% of apps had more than ten trackers. Android apps asked for more permissions compared to their iOS counterparts, but this was mainly due to platform differences where some resources on iOS were not gated behind a permission, contrary to Android.

Studying paid applications. There are few studies that include paid applications in their datasets, arguably because of the budget required to purchase them. In 2015, Seneviratne et al. collected the top 100 free and paid apps on Android in 4 countries [46]. They found that 60% of the paid apps included at least one third-party tracking library compared to 85% of the free ones. Moreover, the tracking behaviours of free apps were about the same as for paid ones since they found the same types of trackers in both. In 2019, Han et al. compared 1,505 free Android apps with their paid versions to see if differences could be observed in terms of privacy [39]. About half had an identical set of permissions and third-party libraries between the free and paid version.

More recently, Watanabe et al. performed a large-scale analysis of 2M free apps and 30K paid ones to detect software vulnerabilities [49]. The price of paid apps they studied ranged from $1 USD to $200 USD. By using vulnerability scanners and checking for dead code, they found that 70% of the vulnerabilities in free apps stem from software libraries, compared to 50% for paid ones.

Finally, Ishii et al. looked at the apps present in 13 different Android marketplaces [40]. They observed that some paid apps can be found for free in other marketplaces, with some even having their license verification library removed so that the pirated copy could bypass the control for an existing license.

Our work. In this paper, we investigate the tracking ecosystem in mobile games as we believe their unique economic models can have an impact on the tracking and advertising libraries that are embedded in them. As the studies discussed above perform measurements on all types of apps without differentiation, we focus here on doing measurements specifically for mobile games. Notably, we want to see if paying for games up front is more privacy friendly than playing free games.

3 DATASET

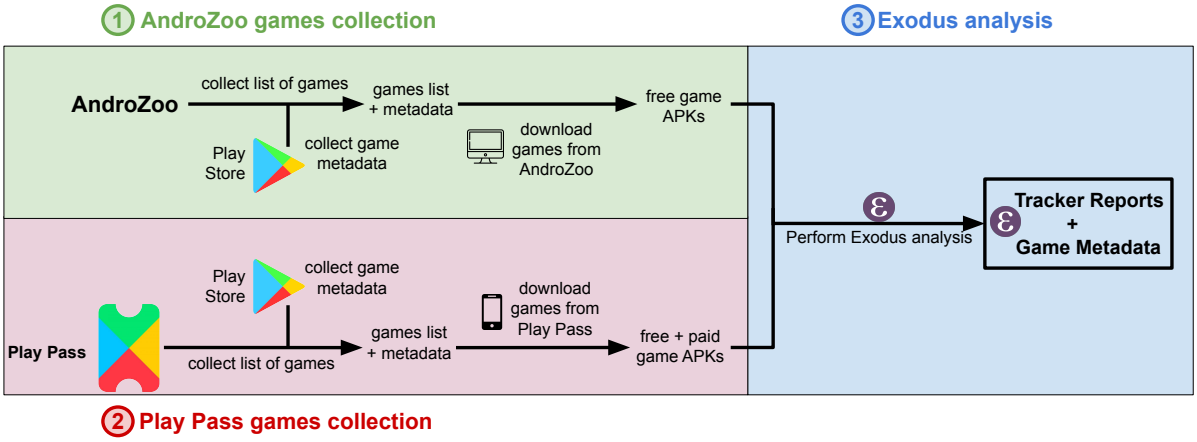
In this section, we detail the dataset that we used to perform our privacy analysis, how we collected it and why we did it that way.

3.1 Collecting Android applications

Challenges. Collecting mobile games directly from the Play Store is not an easy task. Google provides no list of all the games available on the Play Store. Querying the store through the search bar returns no more than 200 applications. The lists of top applications in different categories are also limited to 200 results. And to make an exhaustive search more difficult, rate limiting is applied on requests coming from the same account and the same IP address. Viennot et al. highlight how complicated it can be to actually collect apps on a large scale with their PlayDrone crawler [48]. They paid participants on Amazon's Mechanical Turk to create legitimate Google accounts to circumvent rate limiting. They also rented Amazon servers to have different IP addresses and queried the store using a 1 million word dictionary to extensively explore the application space.

Collecting free games. Because of the limitations imposed by the Play Store and how costly it can be to setup a crawling infrastructure, we relied on the AndroZoo dataset provided by the University of Luxembourg to collect free games [35]. This dataset is regularly

Figure 1: A representation of our pipeline to collect the applications and metadata required for our analysis.



updated and, in 2021, contains more than 17 million Android Package Kits (APK) with more than 14 million originating from the Play Store. For this study, we selected all of the free games from 2021 collected in the AndroZoo dataset, which includes games with as few as a dozen active users, up to popular games with millions.

Collecting paid games. In order to investigate paid games on the Play Store, we relied on Google's Play Pass [19], a subscription service for games akin to Subscription Video On Demand (SVOD) services like Netflix. By paying a fixed monthly fee, users get access to hundreds of apps and games as part of their subscription and they are all "completely free of ads and in-app purchases" [17]. Through the subscription, paid games can be accessed for free and free games become devoid of in-game ads and in-game purchases. For this study, we collected the 716 games included in Play Pass in November 2021. It should be added that the games downloaded as part of Play Pass are identical to those downloaded by non-Play Pass users. APKs are not built specifically for Play Pass users, everyone downloads the same APK that contains the same code and the same third-party libraries. The only difference is that the Google billing system recognizes if a user has a subscription and provides direct access to games and specific in-app products for no additional charge. This detail is especially important since we want to identify trackers that most users would be subject to and Play Pass gives us access to the proper APKs for our analysis.

3.2 Presentation of the hybrid pipeline

Figure 1 provides an overview of the pipeline we put in place to collect both free and paid games and analyse their content to identify trackers in them.

Step 1: Collection of free games. As detailed in the previous section, we relied on the AndroZoo dataset [35] to collect free games. We downloaded the full list of 17M+ APKs present [22] and identified the 111,035 applications added from the Google Play Store in 2021. This includes apps released in 2021 but also updates to apps released before 2021. Because the metadata in the AndroZoo dataset only includes the app ID, we used a scraper called `Google-play-scraper` [15] to collect additional metadata for each APK directly from the Play Store, such as the app's name, rating and categories. We discarded all apps that were not games and removed the ones that were no longer available from the store. Our final list includes the APKs and metadata of 6,035 free games available from the Play Store in 2021.

Step 2: Collection of games from Google's Play Pass. The biggest difficulty to collect all the games that are part of Play Pass is to get the actual list of what is included in the service. As Google does not provide access to the Play Pass catalogue from a Web browser, we used a Pixel 3 phone and manually added each Play Pass game to the account's wishlist. This way, we could use a Web browser to extract the IDs of all the games that are part of the service directly from the wishlist. Then, for each ID on this list, we used `adb`, the Android Debug Bridge, to direct the Pixel 3 phone to open the corresponding page on the Google Play Store and simulated a tap to proceed to the installation. After the game is downloaded, we extracted it from the phone for further analysis and uninstalled it. At the same time, we used the `Google-play-scraper` to collect the metadata available on the Play Store for each game, just as we did for the free games we collected. In total, we collected from this step 716 APKs, with 396 of them belonging to paid games.

Step 3: Analysis of APKs with Exodus. We sent all the APKs we collected in the first two steps to a local instance of Exodus, a privacy auditing platform for Android applications [11]. It statically analyses the content of an APK and returns the list of embedded trackers it has found by identifying specific third-party libraries or URLs associated with tracking companies [12]. It also provides the list of the permissions required by the application. In this study, we adopt the same definition of *tracker* that Exodus uses: "a tracker is a piece of software meant to collect data about you or what you do". As this definition is broad, it means that the trackers reported by Exodus present different levels of privacy intrusions. An ad company that collects the user's geolocation to serve personalized ads is more intrusive than a tracker that only collects bug fixing information when a game crashes. All in all, to paint a better picture of the privacy ecosystem in mobile games, we rely on the 6 different tracker categories that Exodus provides:

Table 1: Source of the games present in our dataset.

	Free games	Paid games	Total
AndroZoo	6,035	0	6,035
Play Pass	320	396	716
Total	6,355	396	6,751

- *Advertisements* for trackers whose aim is to serve ads;
- *Analytics* for trackers who collect usage data;
- *Crash reporters* for trackers that report application crashes;
- *Identification* for trackers responsible for determining your digital identity. One example is logging into an app with a Facebook account through Facebook Login;
- *Location* for trackers who determine your geographical location;
- *Profiling* for trackers that are focused on collecting as much information as possible on the user.

Overview of our dataset. Table 1 provides an overview of the games we collected from our two sources: the free games from the AndroZoo dataset and both free and paid games from Google's Play Pass subscription service. For each game, we have the following data:

- the APK with all of the game's files;
- the Exodus report with both the list of embedded trackers and the list of permissions requested by the game;
- the Play Store listing information with the game's name, the age rating, the review scores, the presence of ads, the presence of in-app purchases and the number of installations.

4 ANALYSIS

In this section, we aim to understand how various characteristics of a game, such as its economic model, revenue streams, genre, price or target audience influence the presence of trackers. We look at the presence of ads, the initial price of the game, its age rating and its number of users to provide insights into the tracking ecosystem in mobile games.

4.1 Impact of the economic model on tracking

4.1.1 Trackers. We find that about 2/3 of paid games have trackers, a 21% reduction compared to free games, and paid games, on average, have fewer trackers than free games. Table 2 provides an overview of the presence of trackers in all the games present in our dataset. The majority of free games have between $1 \sim 12$ trackers, while the majority of paid games have between $0 \sim 4$. Looking more precisely at the distribution of trackers in Figure 2, 10% of free games have more than 15 embedded trackers, with the highest having 36. For paid games, the top 10% have more than 5 trackers with the highest being 16. These results show as a general trend that paying for games is in general better, from a privacy point of view, but there are examples of paid games with plenty of trackers.

4.1.2 Permissions. As detailed by the official Android documentation [26], permissions are divided into groups with the two main ones being *normal* and *dangerous* (also called *runtime* permissions). A *normal* permission enables access to data and actions that present little risk to the user's privacy, while a *dangerous* one, like the user's location, or contact list, requires explicit consent. We analysed what permissions are used by both paid and free games, with a particular focus on *dangerous* ones:

- Free games: 9.16 permissions on average with 1.52 being dangerous ones.
- Paid games: 6.03 permissions on average with 0.73 being dangerous ones.

Table 3 shows the top permissions accessed by most free and paid games. The top 10 normal permissions shows some differences between the two. For example, the `receive_boot_completed` permission shows a 27% difference. According to an official Google forum [29], a change in a dependency in the Google Mobile Ads SDK caused this permission to appear automatically in a lot of applications. Since this SDK is used for Google AdMob, the most popular tracker in our dataset (see Table 5), this results in a high use of this permission. We expect this number to even go up as developers update their SDK to the newer version that includes this dependency change. Other differences exist but the main takeaway is that free apps, on average, request the top 10 normal permissions more often.

For dangerous permissions, access to external storage is at the top for both free and paid games. As mobile games can require extra storage space for textures and assets, it is common for developers to add support for external storage to free up the internal storage. To provide some indication of how large some Android games can be, a popular game called Genshin Impact requires more than 14GB of storage. Location access is high for free games with about 15% of them accessing it, while it is less than 1% for paid games. `read_phone_state` is also high, with 19% of free games asking for

Table 2: Overview of the presence of trackers in the games of our dataset

	Percentage of games with trackers	Average number of trackers per game	Standard deviation
Free	86.79%	6.11	6.65
Paid	65.31%	1.80	2.38

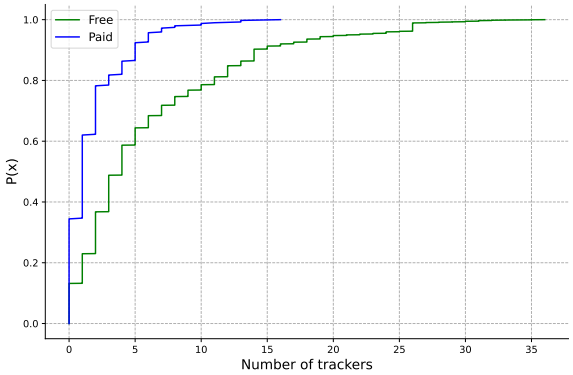


Figure 2: Distribution of trackers across free and paid games.

Table 3: Top 10 normal and dangerous permissions for free and paid games. Additional information on each permission can be found in the official Android documentation [23].

Normal				Dangerous			
Free		Paid		Free		Paid	
Permission	%	Permission	%	Permission	%	Permission	%
internet	95.32	internet	94.44	write_external_storage	52.22	read_external_storage	31.31
access_network_state	92.43	access_network_state	81.31	read_external_storage	32.66	write_external_storage	31.31
wake_lock	65.69	wake_lock	43.69	read_phone_state	19.18	get_accounts	4.80
access_wifi_state	53.19	access_wifi_state	34.34	access_fine_location	15.49	read_phone_state	2.02
vibrate	37.88	vibrate	21.97	access_coarse_location	15.36	write_settings	1.77
receive_boot_completed	32.43	foreground_service	11.36	write_settings	10.57	access_fine_location	0.76
foreground_service	13.28	change_wifi_multicast_state	7.07	record_audio	6.28	camera	0.51
bluetooth	9.00	receive_boot_completed	5.56	get_accounts	6.09	read_contacts	0.25
change_wifi_state	7.17	bluetooth	2.53	camera	4.16	record_audio	0.25
get_tasks	5.93	modify_audio_settings	2.27	read_contacts	0.29	access_coarse_location	0.25

Table 4: Overview of the presence of ads and in-app purchases (IAP) in games

Price	Contains Ads	Offers IAP	Number of games	Number with trackers	Avg number of trackers	Stand. Dev. of trackers	Number with advertising trackers	Avg number of advertising trackers
Free	No	No	694	243 (35.0%)	2.00	3.90	156 (22.5%)	0.74
		Yes	512	421 (82.2%)	5.20	4.11	237 (46.3%)	0.92
	Yes	No	3627	3394 (93.5%)	6.15	6.79	3339 (92.1%)	3.12
		Yes	1469	1412 (96.1%)	8.26	7.07	1375 (93.6%)	3.79
Paid	No	No	311	206 (66.2%)	1.68	2.13	77 (24.7%)	0.38
		Yes	58	33 (56.9%)	1.78	2.55	18 (31.0%)	0.50
	Yes	No	8	5 (62.5%)	2.12	2.47	3 (37.5%)	0.37
		Yes	19	15 (78.9%)	3.63	4.39	9 (47.4%)	1.58

this permission. This enables the game to access information like the user's phone number or the current cellular network. Finally, the `write_settings` permission can also prove to be dangerous as the game can modify system settings. In general, we see that paid games ask for less permissions than free games, resulting in less access to sensitive information.

4.1.3 In-game ads and in-app purchases. Table 4 splits our dataset into categories based on the presence or absence of in-game ads and in-app purchases (IAPs). First, the presence of either ads or IAPs shows an increase in the overall number of trackers, with an additional increase when both are present. The increase is smaller and more restrained for paid games as can be seen with the smaller averages and standard deviations. Second, there's a strong difference when free games are devoid of ads and IAPs, only 35% of them contain at least one tracker, compared to between 56% and 96% with at least one tracker for other categories. This may indicate that developers looking to monetize their apps are more likely to introduce a third-party tracker. Third, we see that the majority of paid games do not have ads or IAPs, which likely is in accordance with the expectations of consumers who pay up front for a game. However, the majority still do contain trackers. Finally, a curious observation is the presence of advertising trackers in the games that claim they do not contain any ads on the Play Store. This is possibly a limit of the static analysis which we discuss in Section 5. Some games might include advertising trackers without using them.

4.1.4 Price of games and IAP. Our dataset includes paid games with prices ranging from $0.99 USD to $35.99 USD. The vast majority of games are priced at less than $10 USD. We expected to see a significantly higher number of trackers for cheaper games, for which the price could be justified by higher expected advertising revenues, while more expensive games would need less advertising revenue due to their higher expected sales revenue. However, Figure 6 in Appendix A shows that the average number of trackers is not correlated to game prices. Indeed, both free and paid games include monetized content to increase revenue. While we previously noted that IAPs, on average, lead to the presence of a higher number of trackers in games, Figure 7 in Appendix A shows that the maximum IAP price does not seem to impact the number of trackers in the game. Similarly, with IAP prices ranging from $1.39 USD to $400 USD, the average number of trackers does not seem to be impacted by the pricing.

4.2 Tracker categories

Figure 3 provides an overview of the distribution of trackers across free and paid apps (see Section 3.2 for a short description of each category of trackers). The first observation is that advertising trackers are 5 times less present in paid games than in free games. Analytics is the most prominent category of trackers in paid apps compared to advertisements for free games. Then, regarding both profiling and identification trackers, there is a little use of them in free games

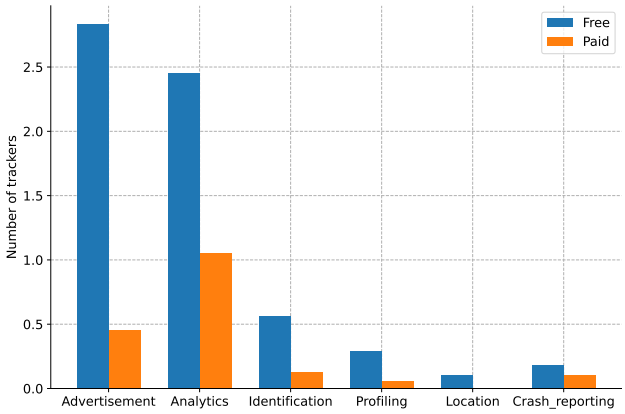


Figure 3: Average number of trackers per categories for paid and free games.

Table 5: Top 10 most popular tracker across all games

Tracker name	Categories	Games with this tracker
Google AdMob	Advertisement	4622
Google Firebase Analytics	Analytics	4110
Unity3d Ads	Advertisement	2203
Google Analytics 4	Analytics	1968
Facebook Ads	Advertisement	1758
AppLovin	Analytics, Profiling, Identification, Advertisement	1256
Google Tag Manager	Analytics	1158
IAB Open Measurement	Identification, Advertisement	1115
AdColony	Advertisement	1114
Facebook Login	Identification	1106

and almost non-existent use in paid ones. Finally, Table 5 reports on the top 10 most popular trackers across all games. Google has 4 different entries, with each tracker having its own well-defined purpose: Google AdMob serves ads directly in games, Google Firebase Analytics is analytics mainly targeted for developers, Google Analytics 4 is aimed at marketers and includes a "Games report" analysis to provide data on user acquisition, retention, engagement and monetization [14], and Google Tag Manager for managing the tracking tags in a game. Facebook follows closely with two of their own trackers: Facebook Ads and Facebook Login. All in all, the trackers in mobile games are predominately for advertisement and analytics.

4.3 Game categories

The Play Store groups games into various categories that the developers choose based on the game's content. Our dataset holds games from 17 categories, with the least represented being the *Casino* category, with a total of 88 games, and the most represented being the *Casual* and *Puzzle* categories, each containing respectively 1168 and 1099 games. Figure 4 shows the average number of trackers based on the game categories. *Casual*, *Sports* and *Casino* games are at the top while *Arcade*, *Music* and *Educational* games are at the bottom.

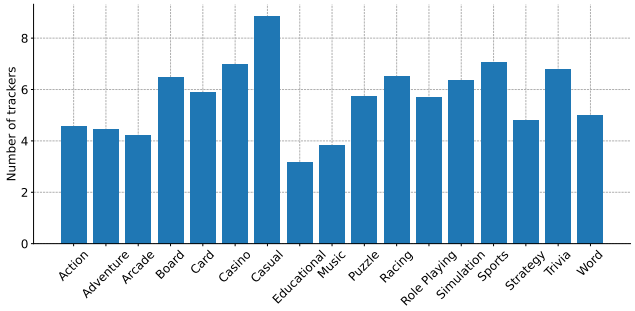


Figure 4: Average number of trackers per game genre.

One aspect highlighted by this graph is that the game genre has an impact on the economic model behind a game. The *Casual* category, which is the most represented in our dataset, also includes the highest number of trackers, with an average of over 8 trackers per game. This high number can likely be linked to what *Casual* games offer in terms of gameplay experience. They tend to be played more opportunistically for shorter sessions and they are uninstalled more frequently. They suffer from a lack of player fidelity and higher churn [2], thus introducing maybe the need or the possibility for developers to compensate by serving more ads, more aggressively, to increase revenue quickly. In contrast, game genres where players are more invested long-term, typically include a lower number of trackers. This is the case of the *Action* and *Strategy* categories, which normally capture users for longer sessions. Finally, the *Educational* games are shown to include the least amount of trackers, likely due to the nature of their content and the targeted audience. As detailed in Section 4.5, Google imposes strict policies on what can be included in a game targeted for a younger audience. Moreover, to maintain a playful aspect and provide a solid learning environment, game makers may opt to provide less ads to limit disturbances compared to other categories aimed at a more mature audience.

4.4 Top 10 games with the most revenue

To dive deeper into how different economic models may impact tracking, we look at the top 10 games with the most revenue on the Play Store in October 2021. Table 6 provides the details on these games. Surprisingly, only 3 games out of 10 contain ads, which means they rely mostly on IAPs or subscriptions for revenue. IAPs have a very wide price range, many are under $1 USD with one being as high as $374.99 USD. Regarding trackers, the numbers observed are similar to the average numbers seen in Section 4.1.1 with all of them including analytics and 8 including an identification tracker. Regarding permissions, the numbers vary between the ten games but they all access APIs needed for various features, like access to external storage to download additional assets or to the microphone for multiplayer games that provide audio exchanges

Table 6: Information on the top 10 games with the most revenue on the Google Play Store in October 2021

Revenue rank	Game category	Contains ads	Range of IAP	Number of installs	Number of trackers	Number of permissions (dangerous)
Gareena Free Fire	Action	No	$0.99 USD - $109.99 USD	1,000,000,000+	7	28 (6)
Candy Crush Saga	Casual	Yes	$0.99 USD - $149.99 USD	1,000,000,000+	7	11 (0)
Coin Master	Casual	No	$0.99 USD - $374.99 USD	100,000,000+	8	13 (1)
Odin: Valhalla rising	RPG	No	$4.99 USD - $89.99 USD	1,000,000+	3	16 (1)
PUBG Mobile	Action	Yes	$0.99 USD - $199.99 USD	500,000,000+	12	23 (4)
Pokémon GO	Adventure	No	$0.99 USD - $99.99 USD	100,000,000+	9	26 (7)
Roblox	Adventure	No	$0.49 USD - $199.99 USD	500,000,000+	3	13 (3)
Genshin Impact	RPG	No	$0.99 USD - $99.99 USD	10,000,000+	6	14 (3)
Gardenscapes	Casual	Yes	$0.49 USD - $99.99 USD	100,000,000+	11	13 (2)
Fate/Grand Order	RPG	No	$0.99 USD - $79.99 USD	1,000,000+	3	12 (1)

during the game. For Pokemon GO, it has the highest number of dangerous permissions but this is also inherent to how the game works. Pokemon GO relies on the player's location to spawn creatures and it uses the device's camera heavily for its augmented reality interface. Both permissions are gated behind explicit prompts because they are considered sensitive for users.

Finally, we can see that the game's category affects the game's source of revenue. For example, there are 3 RPGs in the top 10 that, despite having less than 10M users (compared to Candy Crush Saga's 1B+ users), have no ads and rely entirely on IAPs. This indicates that the type of mobile game can attract different player bases with different spending habits.

In the end, the top 10 provides a glimpse at how popularity and genre can impact the economic model of a game. While less popular games may rely on ads and trackers to bring in revenue, more popular games can also sustain themselves exclusively on IAPs, even in cases when they are otherwise free games.

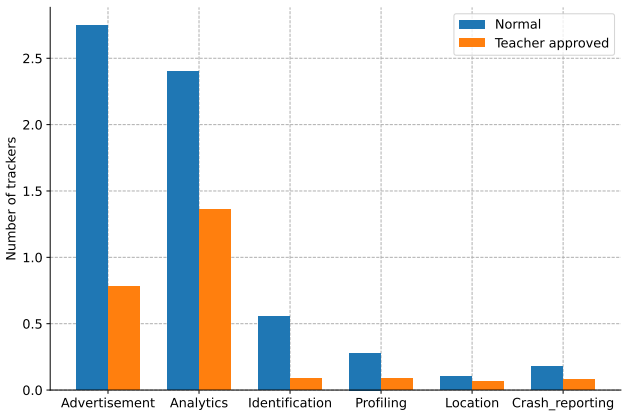


Figure 5: Average number of trackers per categories for Teacher Approved and regular games.

4.5 Google's "Teacher Approved" games

With children increasingly relying on technology for both education and entertainment, Google has recently unveiled a new gaming section labelled *Teacher Approved*. Apps that are designed for children must participate in a larger *Designed for Families* program [10], which opens their eligibility to be rated for the *Teacher Approved* program, without being guaranteed of inclusion. The program includes stricter policies that apps must follow in order to obtain the certification. These policies are verified by a panel of U.S based specialists, which includes teachers, and requires that the app's content and functionality be accessible and appropriate for children. Another major point of the *Designed For Families* program is that it imposes limits on advertising and tracking for children. Developers must follow the *Family Policy* when targetting children with ads, they can either take on these additional responsibilities when using in-house advertising, or they may use one of the self-certified ad SDKs [25]. Naturally, given these restrictions, approved apps are expected to contain less tracking and advertising libraries.

Our dataset includes 181 games with the *Teacher Approved* label, of which 110 are available for free. Our analysis shows that 75% of those games include at least one tracker, with almost 47% including at least one advertising tracker. As these results may look surprising, they are not unexpected as Google does not restrict approved apps from including trackers, but rather requires them to abide to stricter tracking and advertising practices, including using certified ads [13]. *Teacher Approved* apps still include a significantly lower number of trackers, with, on average, 2.12 trackers per game compared to 6.11 trackers for free games. We also note that the top three trackers used in *Teacher Approved* games make use of Google's APIs, namely, Google Firebase Analytics, followed by Google AdMob and Google Analytics. We notice however that other advertiser's APIs are also served. Although Google requires that only self-certified ad SDKs are authorized to serve ads to children in certified apps [25], we do note that 29 *Teacher Approved* games include trackers flagged by Exodus as Advertisement trackers that are not present in the list of Google's self-certified ad SDKs.

Figure 5 provides an overview of the average number of trackers split by different categories. It can be seen that even though profiling goes against the guidelines, trackers within this category can still be found in *Teacher Approved* games. We can however notice that the vast majority of trackers belong to the Analytics category, which follows with our previous observations. Overall, *Teacher Approved* games do seem to provide, from a privacy point-of-view, a better experience, with less ad and tracker frameworks.

5 DISCUSSION

5.1 Summary of findings and privacy implications

In this study, we saw that a variety of economic models are being used to monetize mobile games. Some games favour ads and in-app purchases for revenue, while others rely on the more classical approach of being purchased for an up front fee. Our analysis reveals that paying for a mobile game leads to, on average, a smaller number of trackers and little to no ads. Analytics are the most prominent form of tracking in paid games, while advertisement is very prominent in free ones. Different genres also have an effect on the number of trackers as the ways they engage users and encourage spending can vary greatly, as can be seen by the revenue models between a match-3 puzzle game and a fantasy RPG.

Yet, one of the most important results from our study is how developed the tracking industry is in mobile gaming. Out of 6,751 games, more than 85% had at at least one tracker embedded in it. In terms of privacy, this number paints a bleak picture as a lot of data is being collected on what the players do and how they play. Even though not all collected data pertains to the player's exact identity, a lot of it is still linked to a virtual identity and likely passed around for analyses and monetization between many companies. This shows that users are under constant scrutiny when using their smartphones for gaming, as a single tracker has the capacity to record anything from the smallest gestures up to getting the user's list of contacts.

Discussing monetization in mobile games would not be complete without mentioning the current state of the ad industry. As privacy is being put at the forefront of discussions about users' digital well-being, alternatives are being designed to protect users from invasive tracking techniques and it is leading to strong changes in the mobile ad ecosystem. A first example is the *AppTracking-Transparency framework* by Apple [33]. When launching a new app, the user can chose not to share their device's advertising identifier, which means trackers cannot link the activity of the user across different apps on the same device. While this does not prevent the collection of information, it limits the creation of very large user profiles based on the data from dozens of apps. Another example leading to changes is the return of contextual advertising [28]. Instead of personalizing an ad using all the information collected on the user, the ad will be based on the content of the page that the user is seeing. The intrusiveness of this technique on user's privacy is minimal as companies do not need to build and maintain user profiles based on behaviour, purchasing habits or other factors. In the end, it remains to be seen the impact that these changes will have on trackers in mobile apps and if it will indeed lessen the heavy scrutiny that users are subject to, often without their knowledge.

5.2 Limitations and future work

A first avenue for future research is to use dynamic analysis to go deeper into the analysis of tracking in mobile games. While static analysis reveals the presence of specific trackers, we do not capture how they are actually used in games and if they are triggered at all. Using a tool, such as Lumen [43, 45], combined with complex scenarios to exercise the game and explore as many options as possible, would likely help us identify the information being sent, how sensitive it is, and what the final destination is.

A second avenue is to look at games provided by marketplaces other than Google's Play Store, and platforms other than Android. As each marketplace has its own requirements when submitting an app, tracker analysis would reveal if players from different marketplaces are subject to less or more tracking than those who rely on the more popular Play Store.

Finally, a third avenue is to integrate the future evolution of the Android platform in a tracking analysis. Google has just announced that in February 2022, they will show a *Data Safety Section* on apps in the Play Store to indicate what user data each app collects and shares [21]. Integrating this data into our study could help refine its findings. Another evolution is the new Android App Bundle (AAB) format for Android applications [6]. Designed to be more flexible than the traditional APKs, apps delivered with the AAB format will be optimized for the user's device based on its configuration and language. What remains to be seen is how tracking companies will utilize this mechanism, for example, to deliver different trackers based on the device used by the user.

6 CONCLUSION

Games on mobile generate revenue in different ways: by showing in-game ads, by offering in-app purchases or by having an up-front cost on the store. In this paper, we investigate how these different economic models can impact user tracking by analysing the trackers present in 6,355 free and 396 paid mobile games. Overall, we found that free games have on average 3.4 times more trackers than the studied paid games and they request twice as many dangerous permissions. While the main trackers in free games are for advertisement purposes, analytics are the most prominent trackers in paid games. We also look at games aimed at a younger audience with the "Educational" game category and the presence of a "Teacher Approved" badge. We conclude that the stricter policies imposed by Google have had a positive effect on children tracking as there are less trackers in these games than in the other studied categories.

AVAILABILITY

The artifact accompanying this study can be found at https://github.com/antonin-durey/the-price-to-play and contains:

- The list of game IDs used for our study.
- The script to collect metadata from the Play Store.
- The scripts to collect APKs from AndroZoo and the Play Pass.

ACKNOWLEDGMENTS

We thank the Exodus Privacy team for their advice in this study. This research has been partially funded by the Hauts-de-France region in the context of the ASCOT project of the STaRS framework and by the ANR FP-Locker project under grant number ANR-19-CE39-00201.

REFERENCES

[1] 2018. Relaxing with a Game? Enjoy an Ad – eMarketer. https://www.emarketer.com/content/mobile-gamers-more-receptive-to-ads.

[2] 2019. Mobile App Trends Report – LiftOff. https://liftoff.io/wp-content/uploads/2019/10/2019-Mobile-App-Trends-Report.pdf.

[3] 2020. 75% of Pandemic-Driven Increase in Mobile Gaming Activity Will Persist Indefinitely, According to New IDC and LoopMe Report – IDC. https://www.idc.com/getdoc.jsp?containerId=prUS47906621.

[4] 2021. Number of mobile gaming users worldwide in 2021, by region – Statista. https://www.statista.com/statistics/512112/number-mobile-gamers-world-by-region/.

[5] 2021. 2021 Gaming Report – Unity. https://create.unity3d.com/2021-game-report.

[6] 2021. About Android App Bundles – Android Developers. https://developer.android.com/guide/app-bundle.

[7] 2021. An updated timeline for Privacy Sandbox milestones – Google. https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/.

[8] 2021. Battle Pass: Examples in Top-Grossing Games & Best Practices. https://www.blog.udonis.co/mobile-marketing/mobile-games/battle-pass.

[9] 2021. Building Consumer Confidence Through Transparency and Control – Cisco. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf.

[10] 2021. Designing Apps for Children and Families – Android Developers. https://support.google.com/googleplay/android-developer/answer/9893335.

[11] 2021. Exodus – The privacy audit platform for Android applications. https://reports.exodus-privacy.eu.org/.

[12] 2021. Exodus Tracker Investigation Platform. https://etip.exodus-privacy.eu.org/trackers/all.

[13] 2021. Families Ads Program – Android Developers. https://support.google.com/googleplay/android-developer/answer/9900633.

[14] 2021. [GA4] Games reports – Google. https://support.google.com/analytics/answer/9713967.

[15] 2021. Google-Play-Scraper – PyPi. https://pypi.org/project/google-play-scraper/.

[16] 2021. Google Play vs the iOS App Store | Store Stats for Mobile Apps – 42Matters. https://42matters.com/stats.

[17] 2021. Grow with Google Play Pass – Google. https://play.google.com/console/about/googleplaypass/.

[18] 2021. Intelligent Tracking Protection – WebKit. https://webkit.org/blog/category/privacy/.

[19] 2021. Introducing Google Play Pass – Google. https://play.google.com/about/play-pass/.

[20] 2021. Latest Firefox rolls out Enhanced Tracking Protection 2.0; blocking redirect trackers by default – Mozilla. https://blog.mozilla.org/en/products/firefox/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default/.

[21] 2021. Launching Data safety in Play Console: Elevating Privacy and Security for your users – Android Developers Blog. https://android-developers.googleblog.com/2021/10/launching-data-safety-in-play-console.html.

[22] 2021. Lists of APKs – AndroZoo. https://androzoo.uni.lu/lists.

[23] 2021. Manifest.permission – Android Developers. https://developer.android.com/reference/android/Manifest.permission.

[24] 2021. Number of smartphone users from 2016 to 2021 – Statista. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

[25] 2021. Participate in the Families Ads Program – Android Developers. https://support.google.com/googleplay/android-developer/answer/9283445.

[26] 2021. Permissions on Android – Google. https://developer.android.com/guide/topics/permissions/overview.

[27] 2021. Privacy features – Brave browser. https://brave.com/privacy-features/.

[28] 2021. Privacy regulations and comeback of contextual advertising – Gala. http://blog.galalaw.com/post/102h4vl/privacy-regulations-and-comeback-of-contextual-advertising.

[29] 2021. RECEIVE_BOOT_COMPLETED permission automatically added – Google Mobile Ads SDK Developers. https://groups.google.com/g/google-admob-ads-sdk/c/2OXYkWnMmI0.

[30] 2021. Sensor Tower: Mobile game spending hit $22.2B in 2021 Q1, up 25% from 2020 – VentureBeat. https://venturebeat.com/2021/04/05/sensor-tower-mobile-game-spending-hit-22-2b-in-2021-q1-up-25-from-2020/.

[31] 2021. The future of ads and privacy – Mozilla. https://blog.mozilla.org/en/mozilla/the-future-of-ads-and-privacy/.

[32] 2021. The Games Market and Beyond in 2021: The Year in Numbers – Newzoo. https://newzoo.com/insights/articles/the-games-market-in-2021-the-year-in-numbers-esports-cloud-gaming/.

[33] 2021. User Privacy and Data Use – Apple. https://developer.apple.com/app-store/user-privacy-and-data-use/.

[34] 2022. State of Mobile 2022 – App Annie. https://www.appannie.com/en/go/state-of-mobile-2022.

[35] Kevin Allix, Tegawendé F. Bissyandé, Jacques Klein, and Yves Le Traon. 2016. AndroZoo: Collecting Millions of Android Apps for the Research Community. In *Proceedings of the 13th International Conference on Mining Software Repositories* (Austin, Texas) *(MSR '16)*. ACM, New York, NY, USA, 468–471. https://doi.org/10.1145/2901739.2903508

[36] Steven Arzt, Siegfried Rasthofer, Christian Fritz, Eric Bodden, Alexandre Bartel, Jacques Klein, Yves Le Traon, Damien Octeau, and Patrick McDaniel. 2014. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. *Acm Sigplan Notices* 49, 6 (2014), 259–269.

[37] William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon P Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N Sheth. 2014. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)* 32, 2 (2014), 1–29.

[38] Clint Gibler, Jonathan Crussell, Jeremy Erickson, and Hao Chen. 2012. Androidleaks: Automatically detecting potential privacy leaks in android applications on a large scale. In *International Conference on Trust and Trustworthy Computing*. Springer, 291–307.

[39] Catherine Han, Irwin Reyes, Amit Elazari Bar On, Joel Reardon, Álvaro Feal, Serge Egelman, Narseo Vallina-Rodriguez, et al. 2019. Do you get what you pay for? comparing the privacy behaviors of free vs. paid apps. In *Workshop on Technology and Consumer Protection (ConPro 2019), in conjunction with the 39th IEEE Symposium on Security and Privacy, 23 May 2019, San Francisco, CA, USA*.

[40] Yuta Ishii, Takuya Watanabe, Fumihiro Kanei, Yuta Takata, Eitaro Shioji, Mitsuaki Akiyama, Takeshi Yagi, Bo Sun, and Tatsuya Mori. 2017. Understanding the security management of global third-party android marketplaces. In *Proceedings of the 2nd ACM SIGSOFT International Workshop on App Market Analytics*. 12–18.

[41] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. 2021. Are iPhones Really Better for Privacy? Comparative Study of iOS and Android Apps. arXiv:2109.13722 [cs.CR]

[42] Martina Lindorfer, Matthias Neugschwandtner, Lukas Weichselbaum, Yanick Fratantonio, Victor Van Der Veen, and Christian Platzer. 2014. Andrubis–1,000,000 apps later: A view on current Android malware behaviors. In *2014 third international workshop on building analysis datasets and gathering experience returns for security (BADGERS)*. IEEE, 3–17.

[43] Abbas Razaghpanah, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, Phillipa Gill, et al. 2018. Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. In *The 25th Annual Network and Distributed System Security Symposium (NDSS 2018)*.

[44] Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 2019. 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 603–620. https://www.usenix.org/conference/usenixsecurity19/presentation/reardon

[45] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't somebody think of the children?" examining COPPA compliance at scale. *Proceedings on Privacy Enhancing Technologies* 2018, 3 (2018), 63–83.

[46] Suranga Seneviratne, Harini Kolamunna, and Aruna Seneviratne. 2015. A measurement study of tracking in paid mobile applications. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. 1–6.

[47] Ailie KY Tang. 2016. Mobile app monetization: app business models in the digital era. *International Journal of Innovation, Management and Technology* 7, 5 (2016), 224.

[48] Nicolas Viennot, Edward Garcia, and Jason Nieh. 2014. A measurement study of google play. In *The 2014 ACM international conference on Measurement and modeling of computer systems*. 221–233.

[49] Takuya WATANABE, Mitsuaki AKIYAMA, Fumihiro KANEI, Eitaro SHIOJI, Yuta TAKATA, Bo SUN, Yuta ISHII, Toshiki SHIBAHARA, Takeshi YAGI, and Tatsuya MORI. 2020. Study on the Vulnerabilities of Free and Paid Mobile Apps Associated with Software Library. *IEICE Transactions on Information and Systems* E103.D, 2 (2020), 276–291. https://doi.org/10.1587/transinf.2019INP0011

A PRICE OF GAMES AND IAP

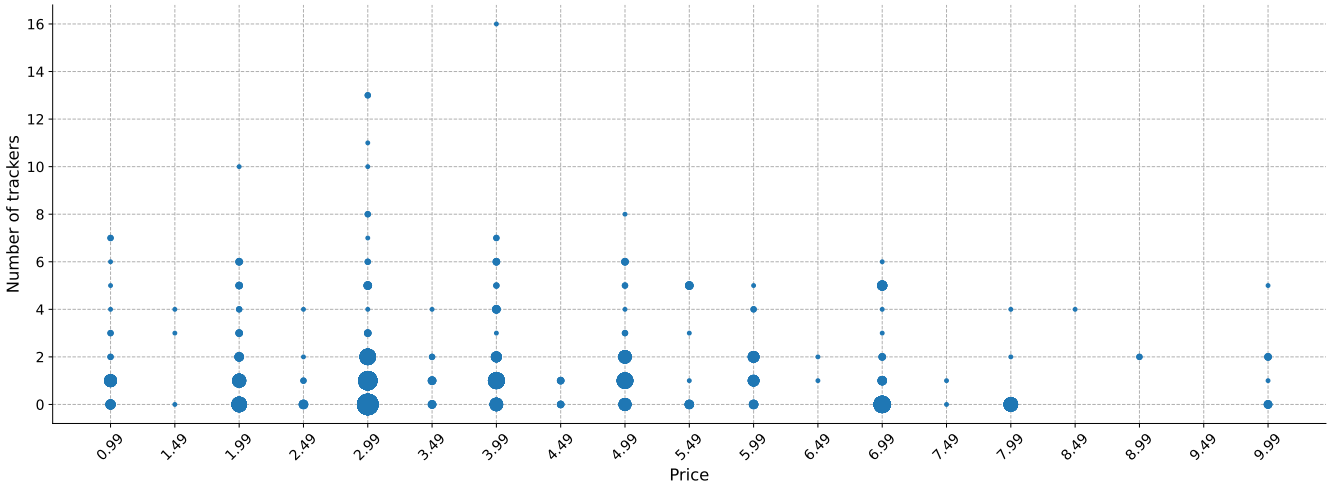


Figure 6: Number of trackers per game price.

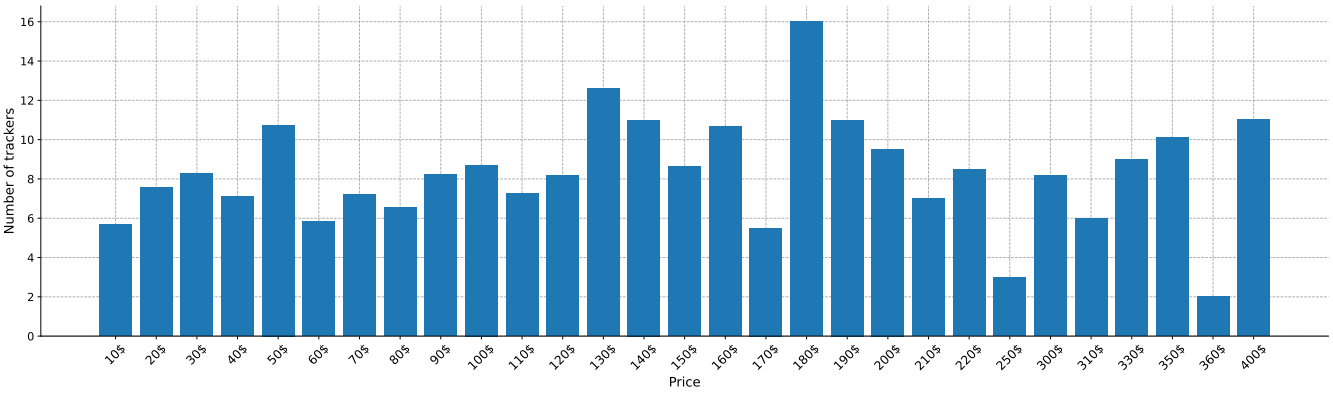


Figure 7: Number of trackers per maximum IAP price.