Can you buy privacy?

Seminarthesis

submitted to
Jun.-Prof. Dr. Miller,
Prof. Dr. Bernd Skiera
– Marketing Department –
Faculty of Business and Economics
Johann Wolfgang Goethe-University
Frankfurt am Main

by

Daniel Hinz Florian Hagen

Table of contents

Number of words: 5390

File: ONCO_CanYouBuyPrivacy_Hagen Hinz.doc

Table of figures

List of tables

Table of abbreviations

App	Application
WTP	Willingness to pay
GPS	Global Positioning System

1 Introduction

Currently, about 3 million Android applications (apps) can be downloaded using the Google Play Store [4]. About 96% of those can be downloaded free of charge, while 4% require the user to pay for the app [3]. While the latter can generate revenue solely with their purchase prices, monetization for free apps is more complicated.

Every app can ask for certain *permissions* when being installed and is theoretically able to collect different kinds of information from the device it is installed on – or “track” information over time – utilizing so-called *trackers*. The collected data can then be used in various ways by the publishers and developers, which will be discussed in detail further on. However, some of them lead to means of monetization and thus can generate revenue, even though the app might be free for the consumer to download, install, and use. This leads to a trade-off: either the purchase price of an app generates enough revenue, or the publishers have to rely on collected information from trackers or permissions, or both, thus creating a risk of privacy for the user, depending on how the data is used.

In our thesis, we will put this trade-off to the test and analyze statistically, whether the use of free apps actually compromises the consumer’s privacy more than the use of paid apps. This question appears more relevant over time, as app downloads from the Google Play Store increased by over 30% from Q3 2019 to Q3 2020, reaching more than three times the download rates of Apple’s App Store, the second largest source for mobile applications after the Play Store [7].

1.1 Trackers

Trackers mainly come in two varieties: the ones openly tracking the user’s behavior – e.g. those used in health-apps to create statistics for the user – and the ones implemented by the publisher or developer to collect background-data which are not necessarily crucial for the app’s performance [14]. The latter are the kind usually referred to when talking about “trackers”.

Said trackers are usually used to analyze user behavior and optimize individualized advertising. These again come in two varieties. The information collected can either be analyzed by the publishers or developers themselves, helping with advertising or other strategic choices, while not reaching third parties. Or they can be sold to advertising companies such as Google, who can then easier target the individual user with more personalized ads

(Google Ads) or services, such as better results when using their search engines. These and other monetization approaches will be discussed further below.

1.2 Permissions

When downloading an application from the Google Play Store, one usually has to agree to a variety of permissions needed for the app to function on one's device. Those permissions can range from obtaining access to the device's camera to sending its current location via GPS. Often, the required permissions are connected to the app's functionality: a photo-editor will most likely require access to the device's gallery as it otherwise will not be able to execute its task.

Permissions are also divided into several protection level categories by Android. The ones recognized by our source are mainly "normal" and "dangerous". Normal permissions, according to Android, "present very little risk to the user's privacy" [1], such as using an internet connection or modifying audio settings [2]. Dangerous permissions could grant the app "access to private user data", among other things [1]. Accessing the user's current location or answering phone calls are examples of dangerous permissions [2]. It is important, however, that dangerous permissions are required for certain functions. This does not immediately make an app dangerous but raises its potential to impair the user's privacy.

From the user's perspective, the main differences between permissions and trackers are transparency and functionality. While the collection of permissions can be viewed in the Google Play Store for every app separately, trackers are usually not listed and thus cannot be controlled as easily. Additionally, permissions can be individually denied on the user's device, which might prove more difficult to achieve with trackers.

1.3 How companies use personal data

While only a minority of app-developers earn money by a one-time payment from the consumer, the most commonly used monetization strategy is in-app advertising, often based on the user's interests. With a market size of 62 billion US dollars by 2018, leveraging third-party in-app advertising is an attractive business opportunity [17].

This development is fueled by the ability of companies to use tracking-technology that allows the collection of user data through aforementioned trackers and permissions. Aziz & Telang (2015) showed that targeted ads can lead to an increase in ad effectiveness by over 30% in comparison to random ads, by exploiting sensible private user information. The mobile advertising practice is handled as follows.

The developers partner with an advertising network, which provides an ad library that can be incorporated in the app [12]. This ad library is able to use permissions, given to the app during installation, to collect (sometimes private) data about the user's behavior. The collected data is then used by an ad network to build user profiles and match the most relevant ads to those profiles [8]. If, for example, the app has permissions to access the current location status, the ad network can provide location-based ads. Or if the app has access to the browsing history, customized ads based on the user's interests can be displayed [10]. Many ad networks provide different kinds of advertising, such as banner-, pop-up- and video-ads.

On the other side of the market are advertisers with the interest of reaching a respective target group. The value for the match of user and ad is then determined by the impressions of the user, such as the number of clicks on a banner-ad [8]. Through this mechanism, a strong incentive arises for all entities to collect as much data as possible.

If users "pay" for free apps with sensible information, it could be assumed that paying for an app monetarily keeps users safe from data gathering, as the collection of data is often associated with the purpose of ad targeting and monetization [11]. Additionally, the absence of ads in paid apps could lead to the same impression. From the point of view of a company, the handling of user data enables an additional source of income, for instance by selling a large amount of user information to third parties [20].

2 Literature

Prior to our thesis, research has already been done to some extent on the topic of price and privacy with Android- and iOS-apps. Articles range from the comparison of privacy in free and paid apps [11, 16, 22] to the consumer's views on privacy and their willingness to pay (WTP) [6, 18].

2.1 Privacy in free vs. paid apps

Research in the past has examined free Android apps and their paid counterparts to answer the question if paying for an app will guarantee more privacy in terms of data collection [11]. There is no clear evidence validating this thesis, as 48% of the paid version used the same third-party libraries as their counterpart free version and 56% those app pairs asked for the same permissions [11]. These numbers only account for free apps and their direct paid alternatives though, and do not look at a relation between different prices and privacy measures – or lack thereof.

A similar approach can be found in the work of Kummer & Schulte (2016). They investigated the money-for-privacy trade-off in the Android app market and found that lower priced apps use more privacy-sensitive permissions on data obtained between 2012 and 2014. The result firstly referred to the market's supply-side, i.e. app-publishers and developers, while our thesis focuses on the demand-side. We differentiate our research by using a more recent dataset and focusing on dangerous permissions.

Prior work has also investigated the amount of overhead traffic of free and paid apps [22]. Overhead traffic is defined as the portion of smartphone app traffic that is not required by the app to serve its initial purpose. Results have shown that the amount of overhead traffic of free apps is substantially higher than that of the paid version of the same app, considering that the measured overhead traffic mainly consists of advertisements and transmission of analytic data [22]. Even when apps were inactive, overhead traffic in the background has been observed [22].

2.2 Willingness to pay for privacy

As Beresford et al. (2012) showed in a small field experiment, although customers' dissatisfaction may rise, their WTP is often not significantly lowered by less privacy. Schreiner et al. (2013) attempted to calculate optimal monthly fees for freemium models of Google (1.52€/month) and Facebook (1.67€/month), but also suggested the selection bias to affect their results. Thus, the WTP might be lower than calculated, as users less interested in privacy probably did not participate in the study in the first place or dropped out along the way [6, 18].

These findings lead us to conclude that, although customers might generally care about their personal data, WTP is relatively low compared to other optional services such as Netflix (currently 12.99€/month).

3 Methodology

3.1 Data collection

The main goal of this work is to analyze the privacy-intrusiveness of free and paid apps and look for factors that influence the level of privacy. Therefore, we had to set certain requirements for our data to fulfill:

We are looking for a dataset with a sufficient **number** of Android apps and both **relevant** and **useful** information. Relevance in this case was determined by *how recently* the data was acquired and by the *popularity* of included apps, measured usually in download-numbers, which the Play Store itself provides to some extent. Usefulness can best be explained by our method of extracting trackers and permissions for each app: we utilize Exodus Privacy [9], a website dedicated to providing information about what and how many trackers and permissions each app requires respectively. This can best be achieved by taking an apps *app-id*, which is uniquely defined in the Play Store, and searching for its entry in the Exodus database. To answer our question, we would then need the price of each app and additionally had to make sure to have both enough free and paid apps in the dataset.

Overall, our requirements for the dataset are the following: the data has to include app-ids, be reasonably new, and if possible, include information about download-numbers and prices. Additionally, the absolute and relative amount of entries in the dataset for both free and paid apps is important to achieve useful results in our later analysis.

In the end, we opt for a dataset from Kaggle.com, a community-driven platform for data science and other projects. The original data encompasses over 1M Android apps with over 4% of them being paid apps, resembling the distribution of the Play Store itself almost exactly [3, 15]. The dataset was also last updated by its publisher in December 2020, making it most relevant for us and our thesis. Among other things, it contains information about an app’s app-id, install-numbers, and price, giving us a useful base to work with. Additionally, it provides each app’s category, ad-support, size and whether it contains in-app purchases, suggesting further points of exploration.

3.2 Data transformation

With our acquired dataset we perform several transformations: we first divide the apps into their two main distinctions, free and paid. Of each we take the most popular 3000 entries, sorting by “Maximum Installs”, to ensure relevance, and build a small web-scraper which extracts an app’s entry from Exodus Privacy, providing us with details about implemented trackers and permissions. We thus obtain the needed information: 2732 Exodus reports are received, 83.57% of which describing free apps. After processing through the Exodus database, our dataset now also contains the number, as well as the specific names, of implemented permissions and trackers for each app.

3.3 Measure of privacy: dangerous permissions

The aim of our research is to measure and compare privacy in paid and free Android-apps and thus help consumers to decide whether it is worth paying for an app in return for better privacy. Google provides 136 defined permissions of which 30 are classified as dangerous. From our view, the permissions classified as ‘dangerous’ by Google provide the best measure of privacy, as those types of permissions allow the developer access to sensible user information. Those dangerous permissions are defined by Android as follows: “A higher-risk permission that would give a requesting application access to *private* user data or control over the device that can negatively impact the user” [1]. Examples for those permissions are access to the camera, contact information and fine location [2]. In our view, this definition fits the general consumer’s understanding of privacy best, which is one reason why we proceed only with dangerous permissions in further analysis.

The other reason is that – without using tools such as Exodus privacy – the consumer has no direct information about trackers implemented in an app when installing it. Only information about the used permissions is provided, without a classification of dangerous ones. By concealing tracker information, the consumer cannot take the use of trackers into account when deciding whether to pay for an app or not.

3.4 Important variables

To measure privacy, we choose an app’s number of dangerous permissions as our main dependent variable. Therefore, we compare free and paid apps, each encoded with dummy variables ($\text{Status}_{\text{free}} = 0$ if the app is free), to test the influence of their app-status (free/paid) on the number of dangerous permissions implemented. For the analysis we use prices, provided by the Google Play Store, whereby we only differentiate between paid or free and ignore the actual amount of the price. Although a detailed analysis of different prices and privacy makes for an equally interesting topic, it exceeds the scope of our thesis and is thus not included. We do, however, encourage research in that direction as it can be equally or even more important to consumers than just the app-status. In addition to the app-status, we observe other possibly relevant variables which could have an effect on permission usage: Content.Rating as a measure for the potential target group, Ad.Supported if the app allows in-app advertising, In.App.Purchases if in-app purchases are allowed, and a classification for the app's category.

4 Descriptive Analysis

Since the majority of apps in the Google Play Store are free, this distribution is somewhat reflected in our dataset. Figure 1 shows that about 16.73% of all 2732 entries are paid apps.

As we see in Figure 2 the number of trackers and permissions is lower on average in paid apps, which supports the common understanding of data gathering mentioned in the literature research above: free apps on average demand more permissions and trackers than paid apps mainly because free apps utilize trackers to display in-app advertising for monetization. Therefore, user data is collected to increase ad-relevance based on the user's preferences.

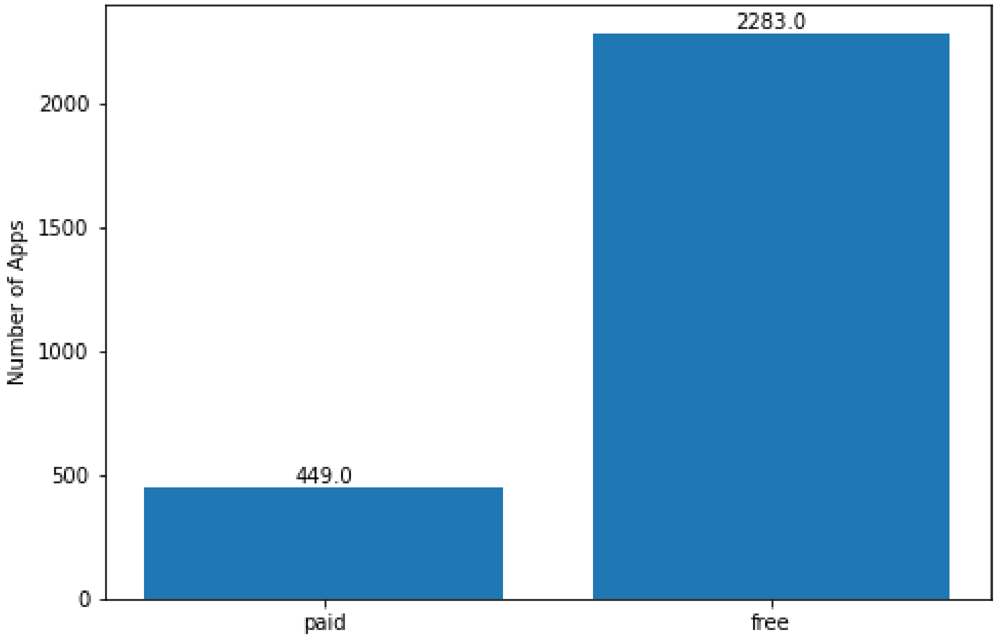


Figure 1: Number of free and paid apps

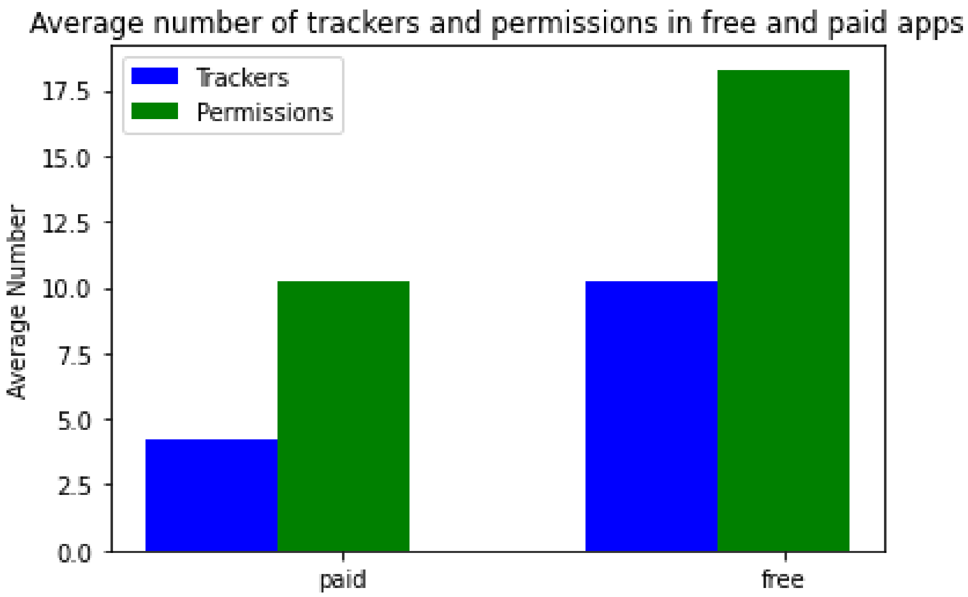


Figure 2: Average number of trackers and permissions in free and paid apps

4.1 Dangerous permissions

We observe a similar pattern comparing the relative amount of dangerous permissions (Figure 3). The consumer can expect that – on average – paid apps demand less privacy-intrusive permissions and that an average free app requires more dangerous permissions. Where paid apps use 1.6 dangerous permissions on average, free apps need 3.7, which is more than twice as much.

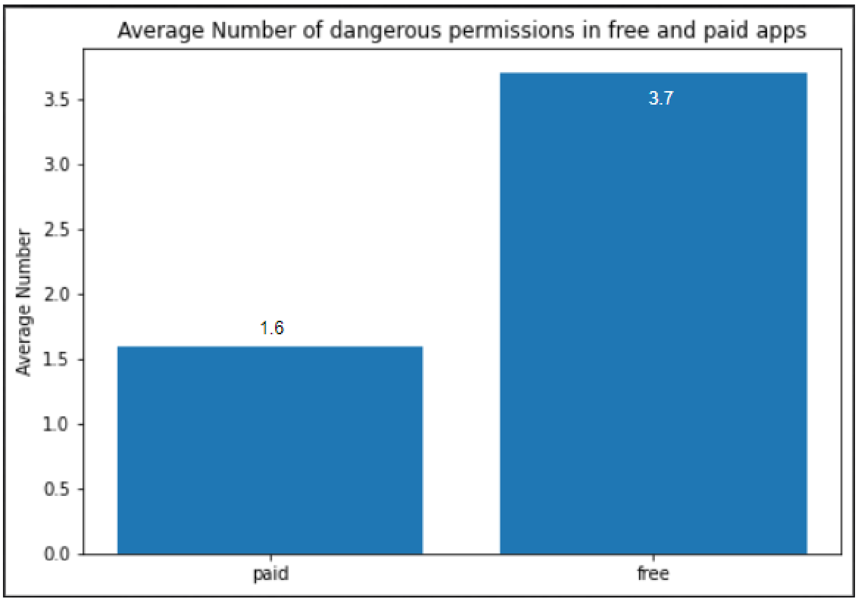


Figure 3: Average number of dangerous permissions in free and paid apps

A more detailed comparison of dangerous permission usage can be made in the form of a violin-boxplot. In Figure 4, the distribution of dangerous permissions in free and paid apps is depicted in further detail; the red dots represent the means which are visibly higher than the medians due to many outliers. As the violins show, a large number of paid apps demand none, or almost no, dangerous permissions and their median is quite low, compared to free apps. To take a closer look at the outliers in paid apps, we observe "Do Not Disturb" to have the highest demand of dangerous permissions (12). With it, users can block calls or messages from certain contacts or based on the current location to minimize disturbances. Since the number and distribution of outliers in free apps is relatively high, we examine those closer in the following.

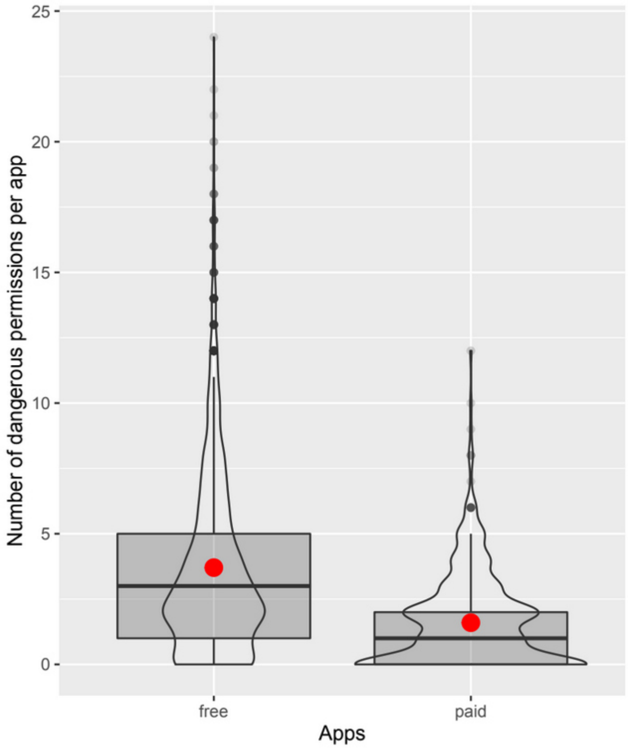


Figure 4: Distribution of dangerous permissions in free and paid apps

As seen in Figure 5, the app demanding the most dangerous permissions is the "Google Play services"-app. It is used as a central update management app for Google applications and comes preinstalled on most Android devices. To conveniently manage other Google-apps, it requires all their permissions from the start, explaining its high place in this list. However, we do not know whether there are apps with more dangerous permissions outside of our dataset. Considering there are only 30 dangerous permissions in the first place, 24 is a relatively high number already.

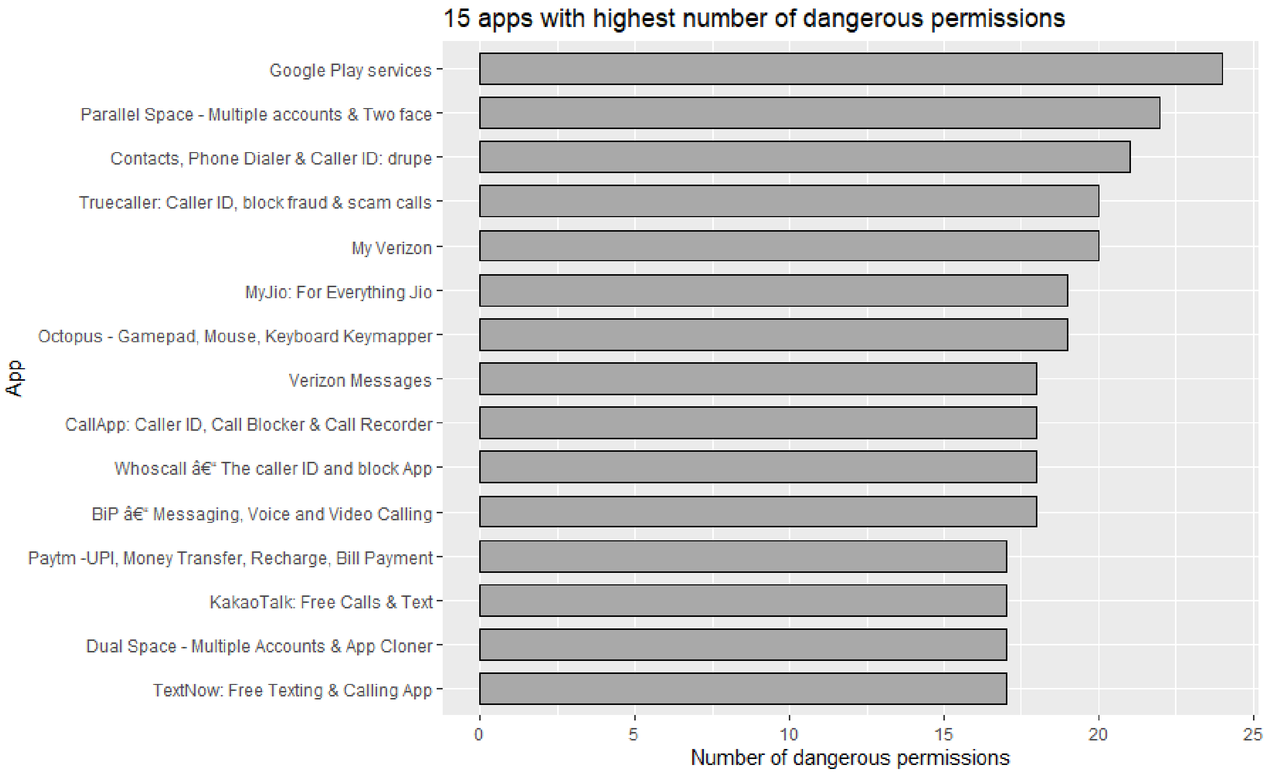


Figure 5: Top 15 apps with highest number of dangerous permissions

The second app on this list, “Parallel Space”, is a central account manager for social media, thus being structurally similar to Google’s services app in needing permissions for all managed apps. All other apps on this list are mostly free and in the communications category, as many dangerous permissions are required for communication between devices.

Figure 6 shows the 20 most often implemented dangerous permissions in both free and paid apps. The most common permission is “WRITE_EXTERNAL_STORAGE”, which allows the app to write to any file outside the directory where the app is installed. Our assumption would be that the app requires this permission to utilize trackers, since 74.5% of free apps use it but we were not able to find further evidence. “CAMERA” allows the app to take pictures and videos and “ACCESS_FINE_LOCATION” allows for accurate location tracking [2].

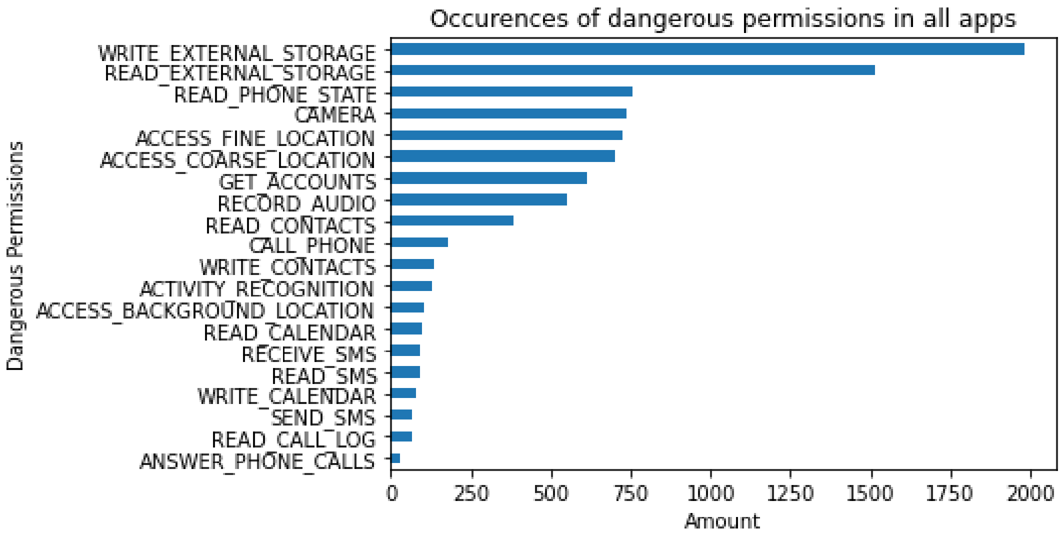


Figure 6: Top 20 dangerous permissions with most occurrences overall

4.2 App prices

As mentioned before, our dataset contains 449 paid apps sorted by popularity with a mean price of 2.81 $ per app. When we compare this average to the mean price of all android apps amounting to 4.92 $ (collected in December 2020), a difference arises. This can be explained by the fact that we extracted the most popular apps by number of installations. The consequence could be that users prefer cheaper apps, as the average price for the most popular apps is lower.

The most expensive app in our dataset with a price of 99.99 $ is “LockMyPix Pro”, which provides functions to encrypt photos and videos on the device. We could not find specific reasons which explain the extraordinarily high price. About 62.92% of paid apps cost less than 2 $ in our data.

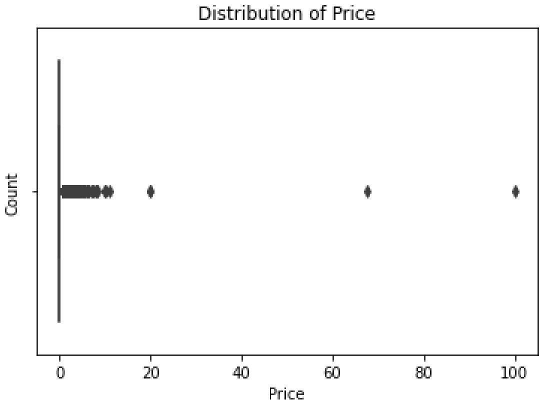


Figure 7: Distribution of app-prices

5 Analysis

5.1 Linear regressions

To analytically approach our question of whether one can pay for privacy or not, we conduct several different regressions. Categories with an insufficient number of entries were left out; thus, the dataset we use in the regressions includes only 17 categories and 2,534 apps, opposed to the original 2,732 entries and 29 categories. We also group similar categories into bigger ones [list in Appendix 1]. The largest example for this being "Games_Grouped", containing 15 categories linked to gaming such as "Puzzle", "Strategy", and "Arcade"-apps.

In total, we model 5 linear regressions and change the combination of independent variables each time, observing the changes taking place in the "Statuspaid"-estimate. Using the stargazer-library in R [13], we can compare the different results side by side in text-form [Appendix 2]. The results referenced here can be viewed in table 1. As the dependent variable, we always look at the number of dangerous permissions per app.

Firstly, we only examine one exogenous variable: the status of an app, describing whether it is free (0) or not (1). The model estimates a paid app to have about 1.98 dangerous permissions less than if it were free, with a standard error of only about 0.17 and very high significance ($p<0.01$), strongly supporting the assumption of higher privacy in paid apps. The adjusted R^2 of this model, however, only amounts to about 0.049, suggesting other influencing variables than only an app's status.

In the **second** regression we then include other possible factors provided in the original dataset, namely age-rating (Content.Rating), whether an app supports ads (Ad.Supported), and in-app-purchases (In.App.Purchases). Interestingly, the estimated absolute influence of app-status increases by almost 50% to almost three dangerous permissions less in paid apps. The adjusted R^2 also increased to 0.153.

However, the estimate further decreases in the **third** regression, giving an estimate of about -1.2 dangerous permissions for app-status. Additionally, it includes dummy-variables for all categories, resulting in a promising adjusted R^2 of 0.415.

The **fourth** model includes all variables from the previous ones. We then remove all estimates deemed insignificant, depicted in our fifth and final regression.

Variable:	(1)	(2)	(3)	(4)	(5)
Status (paid) (std. error)	-1.982*** (0.172)	-2.966*** (0.180)	-1.197*** (0.139)	-1.552*** (0.158)	-1.590*** (0.154)
Rating: Everyone 10+ (std. error)		-0.558** (0.242)		0.426** (0.206)	0.448** (0.205)
Ad-support (std. error)		-1.704*** (0.160)		-0.758*** (0.139)	-0.746*** (0.133)
In-app-purchases (std. error)		-1.124*** (0.144)		0.096 (0.130)	
Communication (std. error)			3.551*** (0.388)	3.663*** (0.387)	3.633*** (0.337)
Shopping (std. error)			0.797** (0.402)	0.607* (0.406)	0.602* (0.355)
Weather (std. error)			-1.758*** (0.596)	-1.398** (0.595)	-1.411** (0.563)
Games_Grouped (std. error)			-3.954*** (0.271)	-3.752*** (0.283)	-3.746*** (0.205)
Observations	2,534	2,534	2,534	2,534	2,534
Adjusted R²	0.049	0.153	0.415	0.423	0.424

Significance levels: * p<0.1 **p<0.05 ***p<0.01

Table 1: Excerpt from regression results found in Appendix 2

Our **final** model still shows a significant effect of app-status (-1.590) as well as an adjusted R² of 0.424 – almost ten times higher than in the first regression. While some independent variables show a weaker impact – such as 0.602 for the “Shopping”-category – others give higher absolute estimates like the “Communication” (3.633) and “Games_Grouped” (-3.746) categories. These results already suggest some variables to be bigger influencing factors than an app’s status; meaning that the difference of the number of dangerous permissions between a free app in “Games_Grouped” and a paid one in “Shopping” is affected more by them being in different categories rather than having a different app-status.

5.2 Comparison of example categories

As the results from the regression analysis suggests, the category of an app is an important factor for permission usage. Therefore, we observe two categories more carefully in a mean comparison (Figure 8):

On average, the number of dangerous permissions in the weather category (3.78) is more than double of that in gaming apps with an average of 1.5, which coincides with the regression results. The intuitive reason could be that some categories demand more dangerous permissions because their apps' functions require access to sensitive user data. Weather apps, for example, will usually need the user's current location in order to conveniently carry out its function. The black bars, describing standard errors, show a higher volatility in the weather category.

Furthermore, the free-paid-effect is relatively higher for games apps and lower for weather apps: in the weather category, free and paid apps almost request the same number of dangerous permissions whereas in the games category, free apps demand nearly twice as many dangerous permissions. To find specific examples, we look at app-pairs which contain a free and a paid version. Taking "Hangman" – a simple word game – as an example, we can observe that the free version demands two dangerous permissions more than the paid version for 2.99$, whereas both versions provide the same functions.

In the weather category, a smaller difference of permissions usage depending on the status can be explained by the fact that free apps demand a certain amount of permissions as well to deliver functionality. In this category, our example "Meteored" contains the same amount of permissions in both free and paid versions.

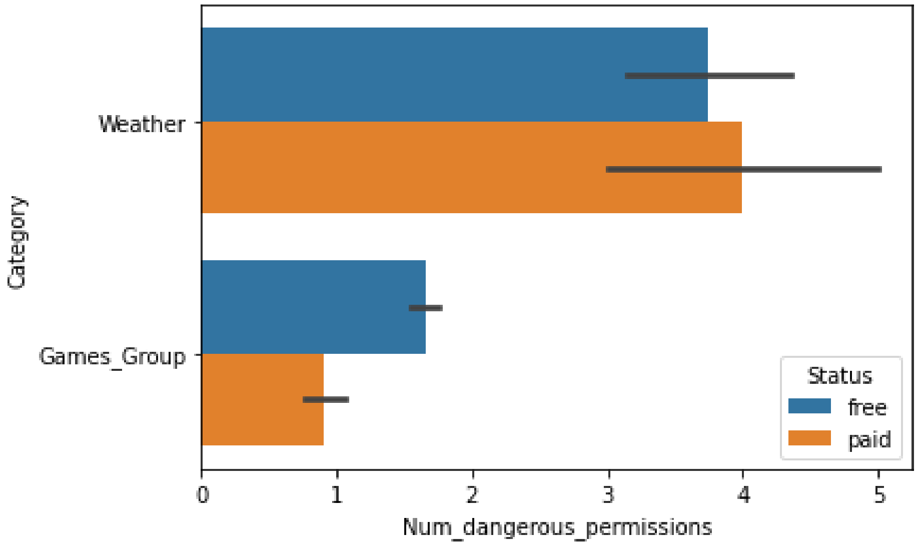


Figure 8: Mean comparison of dangerous permissions: weather vs. games

6 Conclusion

6.1 Analysis implications

From the results of our regressions and category-comparison, we conclude that privacy is often lower in free apps, measured by number of dangerous permissions. In our data, however, we found several more important factors: some categories have a higher or lower impact on the number of dangerous permissions. The direction of the impact – whether the estimate is positive or negative – also differs greatly. Gaming-apps for example seem to contain 3.746 *less* and communication-apps 3.633 *more* dangerous permissions; the absolute estimates are similarly strong but go into opposite directions. This can be explained by the general functionality of apps in a specific category and therefore the respective demand of permissions as communication apps, for example, provide functionality for which more dangerous permissions are needed. It is often possible to send photos and videos, inform others about one's current location or to send documents; all those functions demand dangerous permissions to be implemented [2]. Gaming apps are often monetized using the "freemium" strategy, where the user can play a basic version of a game and can omit in-app-advertising by upgrading to a paid version which, however, do not necessarily provide extended functions.

When comparing categories, we also observe the following: the free-paid-effect is very low for weather-apps, but relatively high in the gaming-category, where free apps have almost 100% more dangerous permissions than paid ones. We therefore conclude that the difference in numbers of dangerous permissions in free apps compared to paid apps depends on their categories. Our category-comparison suggests that the difference in privacy of free and paid apps is higher in categories which require less dangerous permissions in order to function (like games) and lower in categories where functionality is highly dependent on dangerous permissions (such as weather-apps).

The consumer implication whether it is worth paying for an app on a privacy perspective thus depends on the category. In certain categories (games) the consumer can increase privacy through paying while in other categories it is not possible (weather).

6.2 Further research ideas

For future research, we would recommend using bigger datasets. While this is generally a good idea, in order to increase accuracy, the sample size we used was relatively small, given the amount of all available data on the topic. This could not only improve the general quality of statistical tests, but also make data transformation, as we had to do it, obsolete, namely omitting categories due to insufficient information. It might also make a closer look at category-differences possible, as we had only a few categories with enough data to conduct a more in-depth analysis.

To increase the size of usable data, one should also look at Apple's App Store. While it is not as large as the Google Play Store, the distribution of free and paid apps is different (92.7% free [19]), suggesting a higher WTP of customers overall. Additionally, Apple is considered to keep stricter control over what apps are offered than Google, possibly keeping out apps with unnecessarily high privacy intrusion.

Studying the developers' motivations to implement privacy intruding elements in the first place should shed further light on possible causality chains. Additionally, causality in general was not considered in our thesis but could be worth looking at.

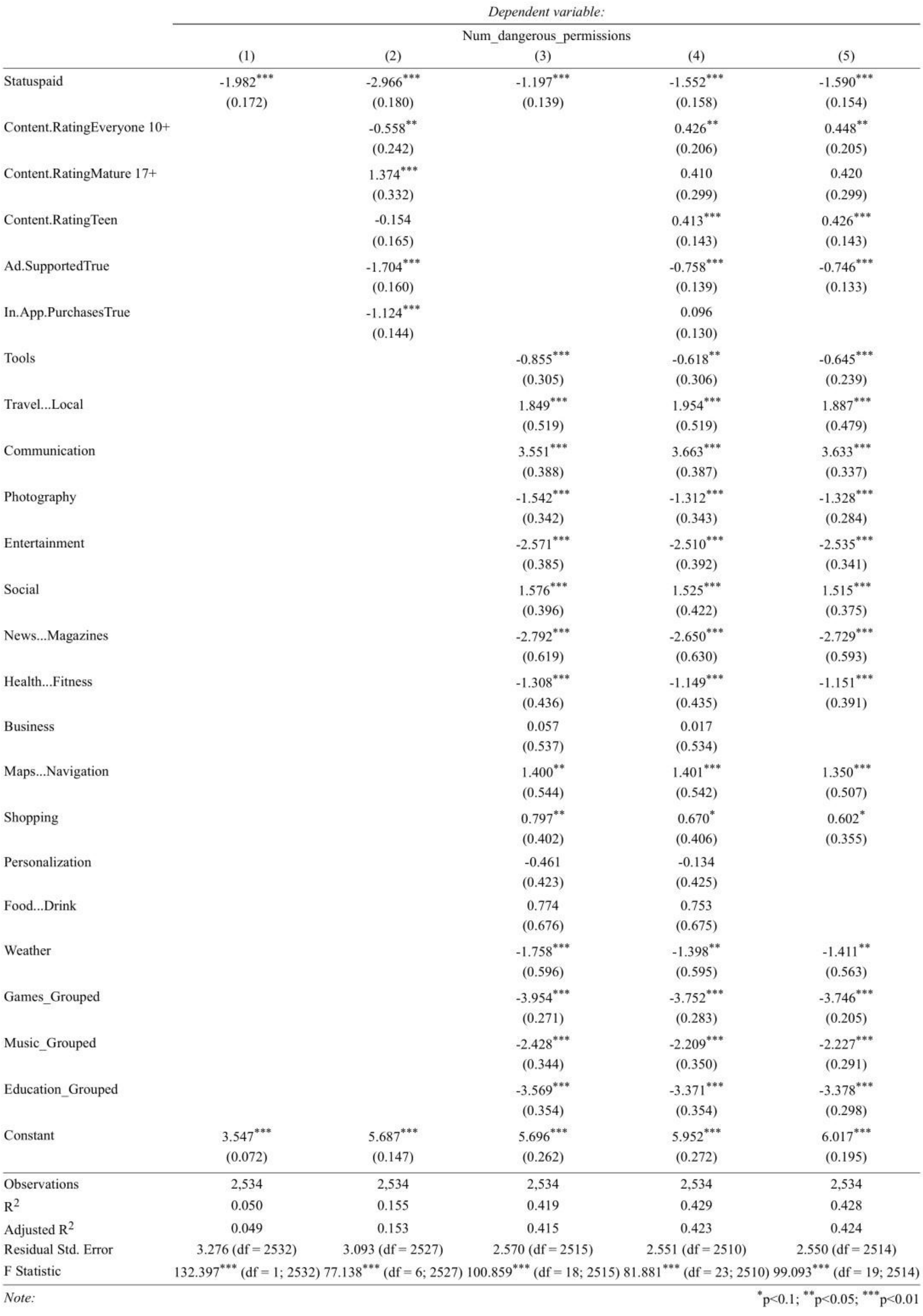
Finally, privacy can be measured in multiple different ways. We only analyzed dangerous permissions, but cases could be made for trackers instead, as well as wholly different factors such as server security or similar structural decisions made by the developers.

Appendix

Appendix 1: List of category groupings:

- Music_Grouped: Music & Audio, Music
- Books_Grouped: Books & Reference, Comics
- Games_Grouped: Action, Board, Arcade, Casino, Casual, Racing, Sports, Strategy, Adventure, Puzzle, Card, Role Playing, Word, Trivia, Simulation
- Education_Grouped: Education, Educational

Appendix 2: Entire result-set of 5 linear regressions, conducted with R and stargazer [13]:



	Dependent variable:				
	Num_dangerous_permissions				
	(1)	(2)	(3)	(4)	(5)
Statuspaid	-1.982***	-2.966***	-1.197***	-1.552***	-1.590***
	(0.172)	(0.180)	(0.139)	(0.158)	(0.154)
Content.RatingEveryone 10+		-0.558**		0.426**	0.448**
		(0.242)		(0.206)	(0.205)
Content.RatingMature 17+		1.374***		0.410	0.420
		(0.332)		(0.299)	(0.299)
Content.RatingTeen		-0.154		0.413***	0.426***
		(0.165)		(0.143)	(0.143)
Ad.SupportedTrue		-1.704***		-0.758***	-0.746***
		(0.160)		(0.139)	(0.133)
In.App.PurchasesTrue		-1.124***		0.096	
		(0.144)		(0.130)	
Tools			-0.855***	-0.618**	-0.645***
			(0.305)	(0.306)	(0.239)
Travel...Local			1.849***	1.954***	1.887***
			(0.519)	(0.519)	(0.479)
Communication			3.551***	3.663***	3.633***
			(0.388)	(0.387)	(0.337)
Photography			-1.542***	-1.312***	-1.328***
			(0.342)	(0.343)	(0.284)
Entertainment			-2.571***	-2.510***	-2.535***
			(0.385)	(0.392)	(0.341)
Social			1.576***	1.525***	1.515***
			(0.396)	(0.422)	(0.375)
News...Magazines			-2.792***	-2.650***	-2.729***
			(0.619)	(0.630)	(0.593)
Health...Fitness			-1.308***	-1.149***	-1.151***
			(0.436)	(0.435)	(0.391)
Business			0.057	0.017	
			(0.537)	(0.534)	
Maps...Navigation			1.400**	1.401***	1.350***
			(0.544)	(0.542)	(0.507)
Shopping			0.797**	0.670*	0.602*
			(0.402)	(0.406)	(0.355)
Personalization			-0.461	-0.134	
			(0.423)	(0.425)	
Food...Drink			0.774	0.753	
			(0.676)	(0.675)	
Weather			-1.758***	-1.398**	-1.411**
			(0.596)	(0.595)	(0.563)
Games_Grouped			-3.954***	-3.752***	-3.746***
			(0.271)	(0.283)	(0.205)
Music_Grouped			-2.428***	-2.209***	-2.227***
			(0.344)	(0.350)	(0.291)
Education_Grouped			-3.569***	-3.371***	-3.378***
			(0.354)	(0.354)	(0.298)
Constant	3.547***	5.687***	5.696***	5.952***	6.017***
	(0.072)	(0.147)	(0.262)	(0.272)	(0.195)
Observations	2,534	2,534	2,534	2,534	2,534
R^2	0.050	0.155	0.419	0.429	0.428
Adjusted R^2	0.049	0.153	0.415	0.423	0.424
Residual Std. Error	3.276 (df = 2532)	3.093 (df = 2527)	2.570 (df = 2515)	2.551 (df = 2510)	2.550 (df = 2514)
F Statistic	132.397*** (df = 1; 2532)	77.138*** (df = 6; 2527)	100.859*** (df = 18; 2515)	81.881*** (df = 23; 2510)	99.093*** (df = 19; 2514)
Note:					*p<0.1; **p<0.05; ***p<0.01

References

1. Android Developers. Documentation: Manifest.permission class. https://developer.android.com/reference/android/Manifest.permission (09.02.2021)
2. Android Developers. Documentation: permission file. https://developer.android.com/guide/topics/manifest/permission-element (09.02.2021)
3. AppBrain. Free vs. Paid Android apps. https://www.appbrain.com/stats/free-and-paid-android-applications (09.02.2021)
4. AppBrain. Number of Android apps on Google Play. https://www.appbrain.com/stats/number-of-android-apps (09.02.2021)
5. Aziz, A. / Telang, R. (2015). What is a Digital Cookie Worth? Available at *SSRN: https://ssrn.com/abstract=2757325* (09.02.2021)
6. Beresford, A. R. / Kübler, D. / Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. In: *Economics Letters, Vol. 117, pp. 25-27.*
7. BuildFire. Mobile App Download and Usage Statistics (2021). https://buildfire.com/app-statistics/ (09.02.2021)
8. Demetriou, S. / Merrill, W. / Yang, W. / Zhang, A. / Gunter, C. A. (2016). Free for All! Assessing User Data Exposure to Advertising Libraries on Android. From: *NDSS '16, 21-24 February 2016*
9. Exodus Privacy. https://reports.exodus-privacy.eu.org/en/ (09.02.2021)
10. Gao, X. / Liu, D. / Wang, H. / Sun, K. (2015). PmDroid: Permission Supervision for Android Advertising. In: *2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), pages 120–129, Sept 2015*
11. Han, C. / Reyes, I. / Feal, Á. / Reardon, J. / Wijesekera, P. / Vallina-Rodriguez, N. / Elazari, A. / Bamberger, K. A. / Egelman, S. (2020). The Price is (Not) Right: Comparing Privacy in Free and Paid Apps. In: *Proceedings on Privacy Enhancing Technologies 2020, Vol. 3, pp. 222-242*
12. He. B. / Xu, H. / Jin, L. / Guo, G. / Chen, Y. / Weng, G. (2018). An Investigation into Android In-App Ad Practice: Implications for App Developers. In: *IEEE INFOCOM 2018, pp. 2465-2473*
13. Hlavac, Marek (2018). stargazer: Well-Formatted Regression and Summary Statistics Tables. R package version 5.2.1. https://CRAN.R-project.org/package=stargazer (09.02.2021)

14. Hutton, L. / Price, B. A. / Kelly, R. / McCormick, C. / Bandara A. K. / Hatzakis T. / Meadows, M. / Nuseibeh B. (2018). Assessing the Privacy of mHealth Apps for Self-Tracking: Heuristic Evaluation Approach. In: *JMIR Mhealth Uhealth 2018, Vol. 6, No.10 (2018)*

15. Kaggle. Google Play Store App data of 1.1 Million applications. https://www.kaggle.com/gauthamp10/google-playstore-apps?select=Google-Playstore.csv (09.02.2021)

16. Kummer, M. / Schulte, P. (2019). When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications. In: *Management Science Vol. 65, Issue 8, pp. 3470-3469*

17. Market Research Future. In-App Advertising Market by Type, Trend, Growth and Overview. https://www.marketresearchfuture.com/reports/in-app-advertising-market-6005 (09.02.2021)

18. Schreiner, M. / Hess, T. / Fathianpour, F. (2013). On The Willingness To Pay For Privacy As A Freemium Model: First Empirical Evidence. In: *ECIS 2013 Research in Progress. 30.*

19. Statista. Distribution of free and paid iOS apps in the Apple App Store as of January 2021. https://www.statista.com/statistics/1020996/distribution-of-free-and-paid-ios-apps/ (09.02.2021)

20. The New York Times. Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data. https://www.nytimes.com/2017/04/24/technology/personal-data-firm-slice-unroll-me-backlash-uber.html (09.02.2021)

21. Wickham H (2016). ggplot2: Elegant Graphics for Data Analysis. Springer-Verlag New York. ISBN 978-3-319-24277-4, https://ggplot2.tidyverse.org. (09.02.2021)

22. Zhang, L. / Gupta, D. / Mohapatra, P. (2012). How Expensive are Free Smartphone Apps? In: *Mobile Computing and Communications Review, Vol. 16, No. 3*