MOBILE GAME ADVERTISING: PLAYERS' VIEWS ON PRIVACY AND DATA GATHERING

Jyväskylän yliopisto
Kauppakorkeakoulu

Pro gradu -tutkielma

2020

Tekijä Veera Ranta
Oppiaine Markkinointi
Ohjaaja Juha Munnukka

JYVÄSKYLÄN YLIOPISTO

TIIVISTELMÄ

Tekijä
Veera Ranta

Työn nimi
Privacy in mobile games and player's views on data gathering

Oppiaine	Työn laji
Markkinointi	Pro gradu -tutkielma
Aika (pvm.)	Sivumäärä
6.6.2020	58 + liitteet

Tiivistelmä
Ihmisten käyttäessä enemmän aikaa puhelimiensa ääressä ja mobiilipelejä pelatessa on pelien ja applikaatioiden mainosten ympärille on kehittynyt liiketoimintaa. Applikaatiot ja mobiilipelit luovat valtavan määrän dataa käyttäjien ja pelaajien käyttäytymisestä. Tätä dataa voidaan hyödyntää ja myydä mainostajille, jotka käyttävät dataa kohdennettuun mainontaan. Tämän datan käyttö luo ongelmia yksityisyyden kanssa ja käyttäjät eivät välttämättä ole tietoisia, että heidän dataansa myydään ja käytetään kohdennetussa mainonnassa. Mainonnan kohdentamista tehdään usein ilman käyttäjien lupaa. Yksityisyyslait ovet yrittäneet hillitä henkilökohtaisen datan myymistä ja käyttämistä ja kasvattaa kuluttajan oikeutta hallita omaa dataansa. Uusimpia yksityisyyslakeja on toukokuussa 2018 toimeenpantu laki General Data Protection Plan (GDPR. Säännös pakotti yritykset arvioimaan ja muokkaamaan omia yksityisyyskäytäntöjään.

Tämän tutkimuksen tarkoitus oli saada lisää tietoa pelaajien käsityksistä yksityisyyttä ja kerätyn datan hyödyntämistä kohdennettua mainontaa kohtaan mobiilipeleissä. Lisäksi, onko GDPR:llä ollut jotain vaikutusta tätä käsitystä kohtaan. Tutkimuksessa tutkittiin myös käsityksestä johtuvaa käytöstä. Tutkimus tehtiin yhteistyössä Rovio Entertainment Corporationin kanssa. Tutkimus oli kvantitatiivinen ja aineisto kerättiin verkkokyselyn avulla. Kyselyn linkki jaettiin kahdessa Rovion pelissä ja kyselyyn vastasi 152 henkilöä. Data analysoitiin SPSS ja SmartPLS ohjelmia käyttäen.

Tutkimuksen tuloksista selviää, että aiemmat kokemukset ja henkilökohtaiset mieltymykset sekä mainosten määrä vaikuttavat eniten käsitykseen yksityisyydestä. Yksityisyyden käsityksellä on kaksi käyttäytymisen lopputulemaa, mainosten katsominen jatkossa tai niiden välttely. Pelaajat pitivät hyvin tärkeänä, että heillä on kontrolli omasta datastaan ja voivat päättää kenelle sitä jakavat. Tulosten perusteella pelikehittäjiä suositellaan panostavan mainospaikkojen suunnitteluun, jotta niiden katsominen olisi positiivinen asia. Mainokset ovat tärkeä osa ilmaisten mobiilipelien tulosta, joten on tärkeää saada pelaajat jatkossakin katsomaan mainoksia peleissä.

Asiasanat
Mobiilipelit, pelien sisäinen mainonta, yksityisyys, kohdennettu mainonta, GDPR

Säilytyspaikka
Jyväskylän yliopiston kirjasto

SUMMARY

Author
Veera Ranta

Title
Privacy in mobile games and player's views on data gathering

Subject
Marketing

Type of the degree
Master's thesis

Time of publication
6.6.2020

Number of pages
58 + appendices

Abstract

As people are spending more time on their phones and playing mobile games, an industry has formed around advertising in mobile applications. Applications and mobile games generate a huge amount of data of user and player behaviour. This data can be utilized and sold to advertisers to target their advertisements based on the information. Using this data creates a problem of privacy and whether people are aware of that their data is being sold and used to target ads to them. Often targeting is done without the permission of the user. Privacy laws have tried to limit the selling and usage of personal data and increase the user's right to submit or withhold their personal data. New addition to the privacy laws was the introduction of General Data Protection Plan (GDPR) in EU in May 2018. The regulation made businesses and organizations handling personal information re-evaluate their privacy policies.

Aim of this study was to gain understanding what perceptions players have towards data gathering and using that data in advertising in mobile games. And also did the introduction of (GDPR) have an effect on that perception. Also, the behavioural outcome of perception of privacy was studied. Study was done in cooperation with Rovio Entertainment Corporation. Study was done as a qualitative study and data was gathered via online survey. Survey link was shared in two of Rovio's games and got 152 complete answers. Data was analysed using SPSS statistical program and factor analysis was done by using SmartPLS program.

The results show that previous experiences and personal preferences along with the number of ads have the biggest impact on the perception of privacy. The perception of privacy then leads to two possible outcomes, users continue to watch advertisements in games or avoid them. Players find it very important to have control over their data and with whom to disclose it. Based on the findings in this study game developers are encouraged to carefully design advertising placements in their games to ensure a positive experience and keep players watching advertising. As ads are an important revenue stream in the free-to-play business model it is important to keep players engaging with advertisements in mobile games.

Keyword
Mobile games, in-game advertising, privacy, ad targeting, GDPR.

Storage
Jyväskylän yliopiston kirjasto

FIGURES

TABLES

APPENDICES

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Study background

Imagine a situation where you are browsing on the internet and decide to check if your favourite online retail store has any discount sales for new shoes. You found and tried on a good pair another day and now you hope to buy the shoes cheaper online. But you have no luck, the online store does not have any sale for those shoes, so you continue to look for them somewhere else. The next day you are reading a news article online and see an advertisement (ad) on the site for shoes you were just googling and checking on yesterday. Other ads show you a similar kind of shoes to the ones you were originally looking for and offer them with a discount. How the other retailers knew what you were looking for, if you had not even visited their websites?

When browsing through the internet your every movement is saved and tracked, from the ads you click, the videos you watch, the articles you read and products you watched (but did not buy) (Aqcuisti, et al., 2015). We are engaging in privacy related transactions all the time, whether we know it or not, and whether the trade-off is tangible or invisible, as is sharing our private information (Aqcuisti, et al., 2015). Based on the actions done online for example clicks, cookies collect and establish a profile of you and advertisers can target advertising to you based on the interests that suit to your profile more accurately than before (Tucker, 2012; Smit et al., 2014).

Cookies and other cross-site tracking methods enable to show the right ad for the right person and customize the content to those, who would potentially be interested in them. Ideally, people would only see ads that are interesting to them. From a marketer's point of view, targeting is important and profitable. Focusing on showing the right and interesting products to the right consumers, increases profits and revenues (Tucker, 2012).

Then imagine a moment you are playing your favourite mobile game. After failing a level you get an option to watch a short video to gain an extra life, and continue playing the level. The video you saw was a 30 second ad for a new puzzle game from a renowned game publisher. You like the puzzle genre a lot and decide to check out the new game. You click the ad and you are directed to the App Store and download the game immediately. You start playing the new game and enjoy it a lot.

In the original game you were playing, you could have also seen another product or game ad based on your previous click/downloading history in the game. If you have linked your Facebook profile to the game, the video could have shown you products or games based on the interests and actions in Facebook. If you are using many applications (apps) from the same developer, they know your interests and habits from those, and can target you new offers based on your previous interests (Zang et al., 2015).

There are some ways to target ads. Some networks target ads based on the behaviour of a consumer. Targeting can also be done based on the used app genre or category. The reason why some consumers might find behavioural ad targeting off putting is that online consumer profiles are created without awareness or agreement of the consumer (Turow et al., 2009). In many cases, consumers do not have a lot of knowledge of what information other people, companies and government have on them, and how that information is used (Aqcuisti, et al., 2015).

Turow et al. (2009) also found that a big share of consumers do not want marketers to tailor advertisements to their interests. Consumers had even bigger objections if advertising is targeted to them based on following their behaviour across websites. Consumers do not have an issue for the idea of tailored ads, but they want to have a control of the content they receive and more openness with advertisers. Personalized ads are a trade-off between disclosing personal data and receiving ads that have more content interesting to you. Some consumers reject tailored ads by declining to give out requested data or provide false information, this can lead to skewed customer databases and profiles (Beatrix Cleff, 2007).

Nowadays the selling and purchasing information of individual consumers has become a huge business. As the laws for this are different from country to country, in some areas it is prohibited to sell information without the consumers' consent (Turow et al., 2009). But more often companies do not have any limits to using data for business purposes without the knowledge or consent of their consumers. Thus, information about the consumer might be distributed to a vast number of operators, who will use the data in their advantage, and all this is done without the knowledge or consent of the consumer. In most of the cases, consumers do not read website privacy policies (Aqcuisti et al., 2015), and even if they did, the policies can be written in such a difficult law terms that a normal consumer would not understand them.

Data gathering and user privacy have become a big issues and topics of general discussion in 2018, along the news of Facebook sharing private data of their users improperly with Cambridge Analytica. The company took advantage of the private user data in the previous president elections in 2016 in the United States (Salinas, CNBC, 2018). The collected data included details of the users' identities, friend networks and "likes" in Facebook. The data was then used to target suitable audiences with ads about the presidential campaign. Cambridge Analytica believed that with the personal data of the users, they could find the audience most prone to the ads.

The issue was that Facebook prohibits user data to be sold for any kind of advertising purposes. News also arouse from other companies, who have access to huge amount of user data that also they had used that data in ways that the users did not know or allowed (Cuthbertson, 2018.). In general consumers are also unaware of who has access to the personal information collected of them, how persisted it is or how the data is integrated across other systems and databases (Beatrix Cleff, 2007).

App and game developers have taken some actions to prevent leaks of user privacy, but the privacy protection solutions currently are not as effective

as they could be (Leontiadis et al., 2012). One way of solving the issue of privacy and data gathering could be to give consumers more control over how their information is used (Tucker, 2012; Acquisti, et al., 2015). New data regulations have taken this into account and made it compulsory. General Data Protection Regulation (GDPR) was introduced in the European Union (EU) in May 2018. The regulation made it compulsory for businesses and organizations handling personal data of users residing in the EU region, regardless of location of the company, to re-evaluate their privacy policies and comply to the new regulations.

New regulation forced advertisers and networks collecting data to be more transparent and open about how they use that data. Consumers are now given the option to see what data has been collected of them, to whom it is shared with and have the data removed when requested. Also, a clear consent has to be asked now from the user to collect data (Corcoran & Costache, 2018). This has led to some side effects such as users not being able to access the site or game, if they did not consent on the privacy policy.

Existing privacy laws had to adapt to the new need for privacy and new privacy regulation has also been introduced to tackle the issues. Introduction of GDPR in May 2018 forced publishers and advertisers in the EU and outside to rewrite their privacy statements and comply with new regulation. The effect of GDPR is evident to consumers with the never ending agreeing to privacy policies when visiting new sites.

As the global mobile advertising spend is expected to increase in the following years and targeting is becoming more and more accurate and personal, it is important to study what effects privacy breaches have had on the players and consumers' views for data collecting and whether their views have had an effect on their behaviour in mobile apps.

1.2 Research problem and questions

The aim of this study is to gain better understanding on what perception players have of data gathering and utilizing that data in advertising in games. Another topic is to study if the introduction of GDPR has had an effect on that perception and to the willingness to watch advertisements in mobile games. Based on previous studies and theories, a number of research questions have been developed for this study:

1. How players perceive data gathering and privacy in mobile games?
2. How are these perceptions related with the players' willingness to watch advertisements in mobile games?
3. How did the GDPR- privacy regulation affect the players' perception and willingness to watch advertisements in mobile games?

This study was performed as quantitative study and the data was collected through a questionnaire distributed in pre-decided Rovio mobile games, Angry Birds 2 and Angry Birds Friends in Finland.

1.3 Key terms and concepts

Certain terms and concepts are used often in this study; hence it is important to clarify their meaning. Key terms and concepts include mobile games, mobile advertising, dynamic in-game advertising, targeted ads, privacy and data gathering and General Data Protection Regulation.

Mobile games

Games developed and played on mobile phones or other carry on devices, such as tablets (Ha, et al., 2007). With smartphones and the technology advancements that came with them, mobile games are capable of running high-quality picture, audio, multiple online players and matches (Soh & Tan, 2008). Typical game genres are arcade, role-play-games, puzzle, problem solving and shooting.

Mobile advertising

Advertising by sending electronic advertisements, mobile ads, to consumers with carry on mobile devices (Beatrix Cleff, 2007). Transmitting advertising messages to consumers via mobile medium using wireless media (Haghirian & Madlberger, 2005). Promotion of an offer between a firm and its customers using mobile medium, device or technology, using two-way or multiway communication (Shankar & Balasubramanian, 2009).

Dynamic in game advertising

Advertising slots included in games, that can be altered and filled flexibly by different advertisers. Marketers can buy these slots to promote their products and services (Terlutter & Capella, 2013). Game designers define the advertising slots in the games and can modify them to specific audiences or players. Internet connection enables ads to be served in real time via ad servers (Turner et al, 2011).

Targeted ads

Targeting personalized ads is showing customized promotional messages to individual consumers. Advertising is personalized using personal information

such as consumer's names, buying history, demographics, psychographics, location and lifestyle interests (Baek & Morimoto, 2012).

Privacy and data gathering

Privacy is control over the disclosure of personal information in order to ensure effective right for privacy (Beatrix Cleff, 2007). Privacy is also the claim of individuals, groups or institutions to determine for themselves, when, how and to what extent information about them is communicated to others (Westin, 1968). Privacy is a regulatory process that serves to selectively control access of external stimulation to one's self or the flow of information to others (Klopfer & Rubenstein, 1977). Informational privacy is privacy of personal data (Acquisti, et al., 2015).

General Data Protection Regulation (GDPR)

GDPR was introduced in the EU in May 2018. The regulation laid rules relating processing people's personal data and set rules relating to the free movement of personal data. Regulation claims to protect the rights and freedom of people and their right to the protection of personal data. The regulation is applied to any individual residing in Union, and applies to any company, regardless of their location, if processing personal information of an individual inside the EU (https://gdpr-info.eu, accessed 18.2.2020). New regulation aims to give citizens better control of their data, to access it and see how it is distributed (Beatrix Cleff, 2007).

1.4 Structure of the study

After the first part of the study, introduction, the focus moves to the main theories concerning the field of this study and to the background of this study. Main theories and recent studies are presented in the second section. After the theories comes methodology, where the methods of conducting the study are told, including chosen research method, data collecting and analyses. Methodology is followed by analysis of the results, describing used data and reporting main results of the analyses. These are followed by discussing the main findings and limitations of the study and topics for future research. Evaluation of the study's validity and reliability is also discussed in the conclusion chapter.

1.5 Rovio Entertainment Corporation

This study was done in cooperation with Rovio Entertainment Corporation, and the survey was conducted in its Angry Birds 2 and Angry Birds Friends games. Mobile games company Rovio Entertainment Corporation, later referred as Rovio, was established in 2003 (Business Information System, 2020). The company went public in 2017 and is listed on the main list of Nasdaq Helsinki.

Rovio became famous for its hit game Angry Birds Classic, launched in 2009. Rovio has launched over 20 games over the years under the Angry Birds franchise and along with other intellectual properties. Rovio's games have been downloaded over 4.5 billion times. Rovio launched first Angry Birds movie in 2016 and a sequel followed in 2019 (Rovio.com, 2020).

In 2019 Rovio's overall revenue was over 289 million euros, of which the games business unit was 265 million and brand licensing 24 million. At the end of the year 2019 the company had 466 employees. Rovio has game functions and studios in Espoo and Stockholm, and the headquarters is also located in Espoo (Rovio Investors, 2020).

Rovio has two main business lines, mobile games and brand licensing. The games business unit creates, develops and publishes mobile games. All the games are free-to-play, meaning that the games can be downloaded and played for and optional In-App Purchases can be made. Players can also choose to view advertising in exchange for in-game benefits. During the end of the year 2019, Rovio reports that around 86% of games revenue came from in-app purchases and 14% from advertising (Rovio Investors, 2020). The brand licensing business unit licences the Angry Birds brand to produce products such as plushies, toys, clothes and food. The Angry Birds animated content on YouTube and Netflix has been watched over 10 billion times (Rovio Investors, 2020).

2 ADVERTISING ON MOBILE PHONES AND PRIVACY

Advertising via mobile phones is not a new invention, but the targeting capabilities companies nowadays have provide a new challenge for consumers to stay on top of their information and have control of their data. What often happens is that consumers do not know how and who has access to their data, and how they are profiled in the eyes of the marketer (Beatrix Cleff, 2007). Mobile games offer another channel for marketers to advertise, and as people are more and more tied to their phones, they become a great source for ad targeting. Data collected through multiple apps from the same device can be used to advertise similar apps or games to the consumer (Zang et al., 2015). It is important to understand how privacy is handled in mobile advertising and advertising on mobile games.

2.1 Mobile advertising

Advertising spend in mobile is increasing every year and most of the apps on app stores have advertising embedded in them (Leontiadis et al., 2012). Marketers are able to reach their customers on a very personal level with mobile advertising without any time or geo constraints. Mobile advertising (m-advertising) is referred as sending electronic advertisements to consumers mobile devices. It is the set of marketing initiatives that use mobile devices and media (Shankar & Balasubramanian, 2009). As m-advertising is quite inexpensive, the customizability and ability to reach and target consumers makes it a novel marketing method (Beatrix Cleff, 2007).

M-advertising begun during the same time when first mobile phones were introduced. First marketing efforts were text messages and multimedia messages. Along with the developments of mobile phones, the advertising also became more elaborate and begun to utilize and collect phone usage and GPS location data from the customers (Turner et al, 2011). Websites install cookies on computers or mobile devices when browsing the internet to track online behaviour. Cookies are small text files that are placed on to user's devices to collect profile information to enable targeted ads. Website users should understand the mechanics of behavioural tracking and cookies before accepting the terms (Smit et al., 2014). Behavioural ad targeting will be discussed more deeply later in this study.

Two general methods can be identified in m-advertising, "push" and "pull". Push advertising is sending messages to the mobile user, and messages are often unwelcomed, since the user did not ask to receive them. Pull advertising is then again sent to the consumer upon their request. Consumers should be able to opt-out of the push advertising at any point and without cost. And then by opting in, a consumer is giving permission to receive marketing.

But since there are usually several parties involved in m-advertising, such as network operators, advertisers, content providers etc., question arise to whom the consumer should give the permission (Beatrix Cleff, 2007).

More and more m-advertising is being done via personalized ads that are targeted to individual consumers or groups. Personalized ads are defined as the process of using customer's information to deliver a targeted solution to that individual and as the ability to recognize and treat its customers as individuals through personal and targeted messages (Baek & Morimoto, 2012). Personalized advertising usually has the possibility for consumers to opt out from future messaging. With the option, consumers might feel more in control of their data and how it is used, thus, mitigating the feeling of reactance towards personalized advertising.

2.1.1 Privacy in mobile advertising

Privacy as defined by Westin (1968), is the individual's claim to determine when, how and to what extent information of oneself is communicated to others. Privacy concerns arise when consumers are worried about potential invasion of the right to prevent the disclosure of personal information to others (Baek & Morimoto, 2012). As mentioned before, the rising concerns among consumers about loss of privacy caused by e-marketers' data collection practises, has led to increasing research for privacy and need for regulators to take actions to address the concerns.

From the companies' perspective, possible privacy breaches can lead to negative reputation and have an impact on the stock market valuation of the company. Companies are also confronted with expensive fines or settlements, and consumers not buying their products because of privacy issues. (Spiekermann & Cranor, 2008)

Often problems arise when commercial practises maximising advertising revenues via mobile clashes with the regulation of data protection (Beatrix Cleff, 2007). A typical example of the practices clashing, is when entering websites with mobile devices, small pop ups notify of the cookie and privacy policy of the site. Often the "Agree" button is highlighted and the pop-up can be closed even without pressing the button. However, closing the pop-up means that the policy is agreed. If consumers wish to know more about the policy, they can click on the policy statement. But reading pages and pages of privacy notice on mobile phone is not practical and this will have an effect on understanding the content of the policy (Beatrix Cleff, 2007).

Many of the personalized advertisements are considered unwelcome, and thus evoking advertising avoidance (Baek & Morimoto, 2012). Lack of knowledge on how private information of us is collected, is reflected in people's concerns about the misuse of personal data and possible violations of their privacy. However only one third of consumers avoid data collection for advertising targeting purposes by not accepting cookies for any type of website (Smit et al., 2014).

As marketers are able to approach their prospects on such a personal level, it is important to understand what kind of data our devices emit of us. As the

same technologies bring a lot of benefits to mobile marketing and advertising, they also raise a lot of privacy and data protection issues due to their capability to collect, store and use personal information. To assess the issues, it is important to review what data our mobile devices collect of us.

2.1.2 Privacy in different operating systems

Two biggest operating systems for smartphones and other mobile devices are Apple's iOS and Google's Android. These companies have different approaches when it comes towards gathering data and privacy with their applications. Almost all of the developed applications are in Apple's and Google's application stores. When a new mobile application is developed, it first goes through an approval process before it can enter the market. Apple and Google also require their developers to follow their data programs, before they allow the application to enter the app stores. (Newman et. al., 2014.)

In iOS's approval process, all new applications will go through their own closed process, where Apple acts as a trusted party that gives certificates, that the application can retrieve information from a phone. After the application is released, no information is given about the type of information the application has access to on the phone. (Leontiadis et al., 2012.)

With Android, being the trusted party is not considered necessary and discussion of privacy takes place directly between the app developer and the end user. On Android when a new application is downloaded, the application presents the user a list of all the permissions that the application requires to run. These permissions include for example location and access to phone's address book. So, the installation of a new application performs as the check-up point, after which the application has the access to the requested information on the phone. (Leontiadis et al., 2012.)

Leontiadis et al. (2012) also discovered that on average free applications on Android request 2-3 additional permissions compared to paid applications. Games were found to request frequently access to 's text messages, contacts and phone calls. Users are expected to make the decision of what information they want to share with the application. (Leontiadis et al., 2012.)

On Android's own site (https://www.android.com/security-center/,2019) above findings by Leontiadis et al. (2012) are confirmed. Android's site states that they believe in "openness and transparency" when making changes and keep the users informed of them. They also state that their users are in control if an app tries to access sensitive data on the phone. The app is required to request permission from the user first.

When a new app is downloaded, the app developers get access to unique ID's for that device, such as Device ID. Developers get data from that ID from the actions done in the app and can form profiles of the users and their interests. And when other apps are downloaded to that same Device ID, advertisers can target content based on their previous behaviour in other apps. (Zang et al., 2015.)

2.2 Mobile games

Modern mobile games came to app stores during the same time as first smartphones and apps were invented, around 2007. Games had naturally existed also earlier on mobile phones, but they were quite simple and already embedded in to the phones (Feijoo et al., 2012). When first smartphones arrived, especially the iPhone in late 2007, the new platform offered new features such as touch screen, motion sensor, precise location system enabling new types of mobile games (Feijoo et al., 2012). Distribution and downloading new games came easier and faster from the app stores.

There are two general business models on how mobile games make profit (Feijoo et al., 2012). When mobile games were first launched, app stores had a small price for them and players had to make a one-time purchase to buy and play the games. The apps and games themselves did not have any transaction possibilities. In this premium model game companies get money from every download. As the games had only a one-time paying option, soon In-App Purchases came into games to offer players more possibilities to spend money for more content. (Feijoo et al., 2012.)

In-app purchases, IAPs, are micro-transactions in the game, that require spending real world money (Newman et. al., 2014). With the in-app purchases players can buy additional game content, like new levels, VIP-packages, new gear, faster progression to advance in the game faster than other players. Games usually also have their own currencies, called soft currency, what you receive without spending real money. Some items can also be bought with soft currencies, but often progression is slower and advancing in the game takes more time. Thus, players are encouraged to spend real money in the games to gain advantage. (Newman et. al., 2014.)

Some people are not willing to spend money and buy a game, without playing it first and knowing whether they like. To appeal to a wider audience and getting more players, games started to shift from the premium business model to a freemium model. In the freemium model, or free-to-play games, players can download and play games for free. The games then offer additional possibilities for in-app purchases to make profit. (Newman et. al., 2014.)

Most of the mobile game players are non-spenders, which means that they are not spending any real money in the games (Sifa et al., 2015). To get benefit from the huge number of players who are not spending money, game developers needed another source of revenue. Advertising came into mobile games, to offer choices for players to receive additional resources for the game by watching ads. With ads players can get extra moves, lives, gear, boosters etc. In the freemium model players can also have the possibility to get rid of ads, if they make any in-app purchase. (Sifa et al., 2015.)

2.2.1 Mobile game advertising industry

In the recent years the time spent in mobile apps and games have increased significantly, and it makes sense for marketers to target their audience in the

places they spend a lot of time. Nowadays most mobile games are Free-to-Play, as they are free to download and play, but the games include ads in order to create revenues within the game on top of the in-app purchases (Sifa et al., 2015). Most of the free applications in app stores are ad-supported and higher advertising revenues are usually achieved with targeted ads. Thus, the party advertising on those applications, have strong incentives to collect as much data as possible about the user to offer them as efficient advertising as possible (Leontiadis et al., 2012).

Mobile games are a growing industry. In the year 2019 the worldwide revenue was $86 billion and is expected to grow over $100 billion in 2020. In 2019 mobile game downloads increased by 45% to 204 billion, compared to three years ago in 2016. Mobile games generate 72% of the total revenue when comparing non-game apps and game apps revenues. The overall spend in mobile apps was $120 billion in 2019 (Takashi, 2020).

Advertising revenue and spend in mobile platform is also growing year by year. In year 2017 the global advertising revenue for mobile was $107 billion dollars. (Dogtiev, 2019.) In 2016 it was $88 billion (Dogtiev, 2018). It is harder to estimate how big portion of the total digital m-advertising revenue is accumulated in mobile games. According to Newzoo (Wijman, 2018) mobile games generated over $70 billion in revenues in 2018. According to one study conducted for game developers found that around 30% of total revenue from games, is coming from in-game advertising.

Games have shifted from being standalone products, to evolving online services, where new features, events, characters and content are being updated constantly. Games collect and create huge amounts of data and information about their players from almost every input made in the game. (Sifa et al., 2018.) Games as a service are data driven and can offer more of a unique experience, when the player data is utilized in the game creating process through optimization and better monetization (Newman et al., 2014). Mobiles are also the most popular device for gaming among children (Russell et al., 2018), thus it is important to take note of the privacy issues associated with data collecting and how the data is used.

2.2.2 Methods to advertise on mobile games

Nowadays people are always on their phone and carry them anywhere with them. Phones usually are also personal as they are often owned and used by one person only. This offers marketers a chance to advertise on an individual level and personalizing the marketing measures. M-advertising has natural attributes of personalization: ubiquity and localization (Bauer et al., 2005). As modern phones also offer GPS tracking, advertisers can target marketing efforts also to specific regions, countries and cities.

Same features apply to advertising on mobile games as well. Based on the players' demographics, game genre they play, day of the week, previous click and downloading behaviour, different ads can be shown to different players (Turner et al, 2011). Advertising companies can use the collected "real world"

data of the players, such as age and geographic location to show the most suitable ad for a specific player (Newman et. al., 2014).

While playing mobile games, players might see video clips and banners with advertisements in different touch points of the games. Advertising in games is called dynamic in-game advertising (Terlutter & Capella, 2013). In video games advertising placements can be billboards, posters and banners situated in natural places suitable to the game environment. Whereas in mobile games advertising slots are included in various touch points in the game, e.g. player runs out of lives or moves, and the game offers a chance to get more lives by watching a short video ad. When clicking the ad, the player is guided to the advertiser's website, or to an app store, if the advertisements was for another game. (Terlutter & Capella, 2013.)

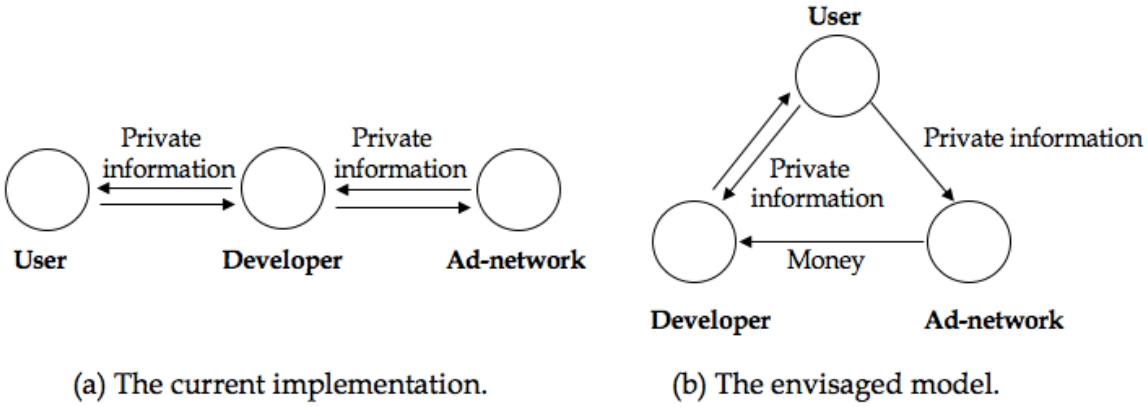
Ad slots are usually alongside in-app purchases and player can choose to spend real money or watch an ad. Dynamic advertising slots can be modified and altered by the game designers. (Terlutter & Capella, 2013.) Optimizing the frequency and specific ads the players see is the key to successful advertising (Turner et al, 2011).

Devices are nowadays almost always connected to the internet and use the vast amount of online services available. Some games also require a working network connection in order to work. Advertising on mobile applications and on mobile games is often done via advertising network (Leontiadis et al., 2012). This requires three parties, where the first is the user, who is using the mobile application. The second is the developer, who are expecting an income for creating and providing the application. And the third party is the advertising network, or ad-network that pays the developer for showing targeted ads to the user and creating interest among them. (Leontiadis et al., 2012.)

Ad-networks pay the developers in line with the number of impressions, views, a certain advertisement has in an application, and they pay more, when the impression generates a click/download from the user (Leontiadis et al., 2012). This urges the ad-networks to generate as many clicks as possible and to minimize the costs of paying the developer for impressions that did not generate a click or download. Because of this monetization model, ad-networks are trying to target and profile those users, who are most likely interested in their ads. (Leontiadis et al., 2012.)

2.2.3 Privacy in mobile game advertising

There are many ways of targeting ads to consumers, one of them is behavioural targeting (Turow et al., 2009). Behavioural targeting is based on the tracking the consumers activities on the internet over time and then utilizing that data to choose the best ads to show. As mentioned before, advertisers believe this helps them to display the most suitable and interesting content to the consumer. In general, advertising networks want to keep their profiling algorithms used to target ads as a secret, but demographic information, location, online behaviour and social networks are expected to provide data used in those algorithms. (Leontiadis et al., 2012.)



(a) The current implementation. (b) The envisaged model.

FIGURE 1: Mobile advertisement models by Leontiadis et al., (2012)

Companies use behavioural tracking differently. Turow et al. (2009) list three different parties and how they do behavioural targeting. First type are websites, and they follow the consumer's actions on their site, articles they have accessed, what kind ads they click and products they started to buy but didn't purchase. The websites can serve ads to the consumer based on their actions on the site, suitable products for the topics they are searching for and the sites can also save these records of the actions by placing cookies on the consumer's computer. And then if the consumer comes back to the site after a while, relevant ads can be served based on their previous visit's actions. (Turow et al., 2009.)

The second party listed (Turow et al., 2009), are advertising networks that track site visitors and save their actions. They do this across thousands and tens of thousands of websites that accept advertisements from those firms. The ads served to the site are owned by Google, ValueClick, Facebook and other big networks. Networks serve ads to the same visitor on other sites as well, if the site is part of the advertising network.

Third party listed by Turow et al. (2009) doing behavioural based advertising are retailers. They track visitors often through frequent shopper cards. Based on the purchases, product categories and shopping behaviour, targeted ads can be served. Special prices can also be offered and other services. All of these companies usually have huge databases and they rely on them to perform behavioural targeting as sophisticated as possible.

Not all mobile game advertising is done through advertising networks. Often game companies try push the players to play other games in their portfolio as well and have them playing and paying in as many games as possible. As buying completely new players can be expensive, in addition to showing players ads from the ad networks, sometimes it is better to show an ad of your own games and thus encouraging players to try those as well. (Sifa et al., 2018.)

Modern video games and mobile games collect and generate data from within the game environment and also from the outside of it. Newman et. al. (2014) studied what data can be collected within the games and outside the game world. Within the games, almost every input can be tracked. From all the

buttons pushed, levels won or lost, purchases made, to ads watched and clicked.

Data that can be collected from "real world" are biometric and physical characteristics. Especially with game consoles that require players movement, like Nintendo Wii, can collect data about the player's face, body movement and voice. Game platforms can also track social interactions, through sharing activities and friend lists. When linked to large social networks, such as Facebook and Twitter, games can learn a lot about the player outside the game environment. (Newman et. al., 2014.)

2.3 Privacy laws, policies and GDPR

Several privacy laws and policies regulate what kind of advertising can be done and what information can be collected from games. As children are a huge audience for games, there are rules regulating and protecting their privacy. In the United States the Children's Online Privacy and Protection Act (COPPA) limits the collection of personal information from children under the age of 13. (Newman et. al., 2014.) The law applies mainly towards commercial websites, but also any application that is either directed to children or services that are known to collect information and using the data for commercial purposes, such as in-game advertising. (Federal Trade Commission.)

In the EU-region privacy laws are implemented by the EU, but every member country also has their own set of privacy laws, as each country has their own law system. Compliance rules can differ depending on the local culture. The GDPR has many opening clauses, which means that the member states can modify the provisions (Privacy Europe, 2020).

Gaming platforms offer different privacy challenges than other platforms, such as social media. In games, the player's interactions are constrained within the game technology, provided by the game company, who have access to the personal information and online activity (Corcoran & Costache, 2018). Access to this information can be done without the equivalent regulatory controls enforced in the financial or medical sectors.

For the growing need of control and security, regulators have made efforts to give the control back to the consumers, on how their data is collected and used (Corcoran & Costache, 2018). The new regulations are aiming to give better control of their data to the EU citizens, and also to increase accountability for businesses and organizations. New regulation also answered to the need of the ability to control access and distribution of personal data, as without it, privacy cannot be protected (Beatrix Cleff, 2007).

Advertisers and networks who are collecting date, are forced to be more transparent and open on how they use that data. With the introduction of the new regulation, consumers are now given the option to see what data have been collected of them, which parties have access to it and importantly, consumers can now ask their data to be removed (Corcoran & Costache, 2018).

GDPR was not the first law for data protection, but it was notable because of the sanctions it imposes for the possible violators. If a company is non GDPR compliant, the fine is up to 20 million euros, or 4% of the company's annual turnover. Privacy policies have been already well established prior to GDRP, such as EU Data Protection Directive DPD (94/46/EC), which is protecting individual information privacy. Also, Privacy and Electronic Communications Directive (2002/58/EC) regulating privacy and data protection issues as a result of new online marketing practices by requiring permission-based advertising. Directives aim to guarantee, that the users are informed about the information practises and the possibility to choose to opt out of disclosing personal data and not to receive m-advertising (Beatrix Cleff, 2007).

In their study the Corcoran and Costache's (2018) identify four main rights of users and five responsibilities for companies from GDPR regulation. They studied these in the context of games and interactive media. Main rights are breach notification, right to access, right to erasure or right to be forgotten and data portability. Breach notification refers to that data controller, companies etc., is obligated to notify the user in case of any data breach, that might risk their rights. Consumers also have the right to know what personal data of them is being processed by the data controller and for what purpose, consumers also have a right to receive a copy of the data controller has collected of them.

The third user's right is right to erasure or right to be forgotten. This means that the user can request the company to delete their personal data, by withdrawing consent or if the data is no longer relevant for the original reason of collecting. Fourth right is data portability, users can ask their personal data to be transferred to another controller (Corcoran & Costache, 2018).

Corcoran & Costache's study (2018) identified five main responsibilities for data controllers, as in companies collecting the data. First is data protection by design and data minimization. Controllers have the obligation to develop and implement applicable technical measures to protect data, starting from the development stage of the applications, services and products. Also, to make sure that the processing of personal data is minimal. Companies should also designate a DPO, data protection officer responsible for data protection, if the business process data on a large scale. Third responsibility is impact assessment of data protection, if data processing may result in a high risk for the rights of the users. (Corcoran & Costache, 2018.)

Fourth responsibility mentioned by Corcoran and Costache (2018) is obtaining clear consent from the user. Consent should be given, with a clear indication of the data subject's, the user, agreement to the processing of personal data related to them. Fifth and final responsibility is that the processing of personal data should be lawful and fair. Communication and information about the processing personal data should be understandable and easily accessible, also written in a language that can be understood without knowledge of legal terms. (Corcoran & Costache, 2018.)

3 PRIVACY BEHAVIOUR

As mentioned before, our devices and smartphones alone can collect and share huge amount of data from us, but that is nothing compared to the digital footprint we leave from our day to day browsing in the internet. When a post is shared, or a photo uploaded to Facebook, they leave a permanent mark on the web and are stored, sort of a digital skeleton (Acquisti, et al., 2015). Technology has become a big part of our everyday tasks in personal and professional lives, thus it's important to distinguish a line of what data is private and cannot be collected, and what data can be collected and used without concern for privacy issue.

3.1 Factors of privacy behaviour

Research on privacy behaviour has previously focused on the context of internet and m-advertising (see Tucker, 2014; Beatrix Cleff, 2007) but more research is needed on privacy and advertising on mobile games. As stated by Beatrix Cleff (2007), issues with data protection and privacy arise when regulation of data protection clashes together with commercial practices done to take advantage of advertising via mobile. As mobile games are a part of other social apps and need to follow the same privacy guidelines, the findings in other apps and online websites, mobile game apps can be expected to follow the same trends.

3.1.1 Privacy uncertainties and concerns

Aqcuisti et al. (2015) review existing research in their article on privacy behaviour. They identify three main themes to connect different research streams. First theme is uncertainty about the nature of trade-offs, when giving consent to privacy policies in websites and such and what are people's preferences for them. Second theme is the power of context-dependency on privacy preferences and third is the malleability of privacy preferences, which means that there are many ways to manipulate factors, that enhance or suppress privacy concerns of individuals.

First theme is uncertainty about the consequences of behaviour related to privacy and people's own preferences to those consequences (Aqcuisti et al., 2015). There are many ways of how individuals manage the boundaries between their private and public surroundings, in example anonymity, protecting personal information and deception. People have the need to establish boundaries, to feel a sense of intimacy and desire for protection from social influence and control. When people feel that their privacy has been intruded, e.g. someone eavesdrops on your conversation or reads your email,

they experience uncertainty of if they should, or on what degree they should be concerned about their privacy. (Aqcuisti et al., 2015.)

First source of uncertainty is the lack of knowledge of what information other parties know about us and what they do with the information. Two factors make it harder to foretell the behavioural outcome of privacy concerns (Aqcuisti et al., 2015). Whether the privacy harms are tangible, such as financial losses, and the trade-off what usually comes with privacy. In example, making sure that customer's purchases are kept under privacy, can protect the customer from price discrimination, but it can deny potential benefits of targeted offers and advertising. (Aqcuisti et al., 2015.)

Consumers differ in the tolerance they have for unsolicited marketing efforts, they feel more positive towards advertising of products and services in which they are interested, opposed to advertising content they are not interested in (Beatrix Cleff, 2007). If advertising messages are perceived too personal, consumers are likely to experience a reactance state. Consumers suspect that the right of autonomous choice they have about disclosing their private information is threatened by unknown advertisers or third parties. (Baek & Morimoto, 2012.)

Second source of privacy uncertainty is related to preferences. There is a discrepancy between the need and care people have for privacy in general, and the actions to seek privacy protection, which is depending greatly on the costs and benefits of seeking it. In the age of social media, the need to share and be public about your life, is having a strong counteract for the need for privacy (Aqcuisti et al., 2015). Some individuals are more open to share details about their personal lifestyles, like political beliefs and religion. In these cases, the lines between private and what is public become harder to distinguish. Society can also have a strong influence on how much sharing one's personal lifestyle is valued (Corcoran & Costache, 2018).

The second theme Aqcuisti et al. (2015) propose was the context dependence of concern for privacy. This means that depending on the situation, individuals can display a very strong concern for privacy or worry next to nothing. The guidelines people follow for managing privacy vary from situation to situation, are learned over time and are based on cultural, motivational and situational criteria. What we regard as private and what is public, are based on social expectations and those vary between contexts.

People use cues to judge the importance of privacy, which can sometimes lead to a sensible behaviour. Cues encouraging the feel of trust and certainty, can be presence of government regulation or other trusted party. But then again, some cues may make people give out rather personal information, even illegal and sensitive one, if they know that other people are sharing the information out too. With the technologies used today, we cannot be sure who is following our social media and the boundaries between public and private, are becoming more intertwined and harder to separate. (Aqcuisti et al., 2015.)

Final theme of the article is malleability of our privacy concerns (Aqcuisti et al., 2015). This means that often individuals are not aware of the factors that determine their concerns about privacy, but parties who are dependent on the usage of personal data have developed ways to diminish the feeling of concern

for privacy. Peoples concerns can be easily influenced in what and how much they share. Parties such as online social networks and behavioural advertising, are relying on individual's propensity to share their private information. Efforts to promote sharing information play on the malleability of privacy preferences and those in turn affect behaviour.

3.1.2 Overcoming privacy concerns

Aqcuisti et al. (2015) mention in their article few strategies used to activate or suppress privacy concerns, such as default settings on sites, which are often taught as the best option and recommendations. Other strategies are in example malicious interface design, which can frustrate or confuse users into giving personal information. Trust in the party receiving information soothes concerns for privacy. But this can be misleading, people can mistakenly believe, that if a site has privacy policy, it would not share their private information. This implies, that letting consumers know that you have a privacy policy, may lead to false feelings of protection.

It is often thought, that if users had control over their data, people would feel more protected and reduce privacy concerns. But research has shown, that if people have explicit control over their personal information and could choose where and how much to share, they ended up sharing more sensitive information than others. (Xu, et al., 2009.)

Even though of the concerns people have about the misuse of personal data, only third of customers avoid data collection by not accepting cookies or other tracking technologies for ad targeting purposes (Smit et al., 2014). This finding is also supported by Spiekermann and Cranor (2008). They found in their study, that privacy was an issue, even though people did engage with services that use their data heavily and people do not protect their data sufficiently.

Acquisti et al. (2015) suggest that policies which rely heavily on approaches on informing and empowering the individual about their data, are unlikely to offer proper protection from recent information technologies. Transparency and control over own data can also backfire, as stated before. In order to have policies properly protecting privacy, they need to require minimal information of prior knowledge and decision making from the individuals. (Aqcuisti et al., 2015.)

3.2 Consumers' control over privacy

With the huge amount of data companies have on their users, they can tailor and personalize the ads shown to users across the web and on mobile. This might lead to a positive perception and ads are found more appealing, but personalized ads can also make the user feel that their privacy has been compromised (Tucker, 2014: Turow et al., 2009). The risen privacy concerns might lead to the opposite behaviour towards the personalized ad. If the

companies address the privacy concerns but continues to user consumer data to personalize ads, may make the users even less likely to respond to those ads.

Tucker (2014) studied how strengthening privacy controls affect advertising performance. The study found that personalized advertising on Facebook was twice as effective at attracting users after Facebook changed its privacy policies in 2010 to give users more control over their personal information. However, the study also found that consumers were concerned, if the personalized information in the ads was too personal to be used in an ad without equivalent sense of control over their data.

Study by Tucker (2014) supports the previous findings mentioned by Aqcuisti et al., (2015) and Turow (2009) in the sense that perceptual control over privacy can affect responsiveness to advertising. If websites and companies can successfully convince consumers that they are in control of their privacy, companies can use personalization of ads to generate higher number of clicks and engagement rate.

3.2.1 Granting permissions

In their research Krafft et al. (2017) studied the drivers related to consumers granting permissions to be contacted via personalized communication. In order for companies to do direct marketing, they need a permission or consent from the consumer. Permission based marketing also adhere with the privacy laws set in the EU. Getting permission from a consumer is important for marketing activities and for competitive advantage, but as the consumers are unlikely to give permission to multiple companies, companies left without are reduced to passive by-standers. Study found that consumers face a cost-benefit trade-off when deciding to do actions that disclose personal data.

In order to get more consumers to give consent, authors recognized determinants of the decision to grant permission to companies to send personalized advertising (Krafft et al., 2017). Study distinguishes between drivers related to benefits and cost to the consumers. Benefits and costs can be economical or psychological.

There are five types of benefits, economic benefits relate to monetary gains and psychological to the personal perception of the received benefits. Economic benefits are personal relevance, entertainment, incentives and lottery and information control is a psychological value. (Krafft et al., 2017.) Personal relevance means that consumers have a need for personally relevant information in order to interact with a company. Meaning that consumers are willing to give their data to the company if the marketing is relevant to the consumer and if they receive personal offers and information. Relevance affects positively to the consumers' willingness to give permission.

According to Krafft et al (2017) the second benefit is entertainment, consumers are looking for the factors that enhance the expected value of direct communication with the company. Krafft et al (2017) found that the higher the entertainment value of the direct marketing efforts, the more likely consumers grant permission for marketing activities.

The third and fourth benefit are incentive and lottery. When consumers a disclosing personal information, they might be looking for financial benefits like discounts or chance to take part in a lottery. Receiving monetary compensation with a relevant message was expected to raise consumer's interest in permission marketing. However, the study found that monetary compensation did not affect the willingness to give permission. (Krafft et al., 2017.)

Fifth and final benefit is psychological, information control. This refers to consumer's awareness of whether they are in control of the data they share and if they have control over the volume marketing messages they receive (Krafft et al., 2017). If consumers felt to have control over their data, they were more likely to give permission to marketers (Krafft et al., 2017). This supports Tucker's (2014) findings in the sense that giving users control of their private information can benefit media supported by advertising.

3.2.2 Costs of granting permissions

Krafft et al. (2017) found three cost related factors when consumers are engaging in data exchange with companies. Economic costs include the efforts customers may have to take to grant permission and psychological relate to loss of privacy and intrusiveness of personalized advertising. First economic cost is registration cost, where consumers have to go through sign-up steps in order to receive permission-based marketing. The registration process might take time and effort, and this can be perceived as too much effort and consumers might drop out in the middle of the process. (Krafft et al., 2017.)

The second cost is intrusiveness, where consumers perceive the incoming marketing efforts as irritating and annoying (Krafft et al., 2017). This might even lead to consumers trying to avoid the marketer. Advertising avoidance will be discussed further in the next chapter. The perceived annoyance has a negative effect on the consumers' attitudes towards m-advertising.

Final cost is a psychological, privacy concerns. When consumers decide to take part in marketing communication with a company, they need to provide their personal information. Disclosing personal information is seen as a loss, and privacy concerns may occur, if the consumer perceives the value of the information to be high. (Krafft et al., 2017.)

Krafft et al. (2017) argue that all cost related drives, have highly significant negative effects on the probability of granting permissions. Out of the three privacy concerns have the highest negative impact on the probability of giving permission. Privacy costs were found to decrease the positive effects of perceived benefits. Consumer were found to prefer communication, that matches their interests and provides relevant and tailored content, entertaining content was found efficient too (Krafft et al., 2017). Their study encourages companies to use transparent privacy policies, to diminish privacy concerns.

3.3 Advertising avoidance

Baek and Morimoto (2012) studied the key factors influencing advertising avoidance on the context of personalized or customized advertising. They found, that privacy concerns lead to an increase in scepticism towards advertising and advertising avoidance. This contradicts the findings mentioned before by Krafft et al. (2017), where personalized ads were found to positively affect the consumers. Advertising avoidance is one form of negative responses towards advertising and said to be of the greatest obstacles for advertisers. Advertising avoidance can also be function of prior negative experience and avoidance is the actions done to reduce exposure to ad content. With the similarities of using the internet, social apps and games, findings in the studies can be expected to be similar in mobile games as well.

Ad avoidance has three components of responses: cognitive, affect and behaviour (Cho et al., 2004). Cognitive component refers to a consumer's belief about and object. The affective represents consumer's feeling or emotional reaction to an object. Then behavioural component refers to a consumer's actions to avoid an object.

There are three main constructs that lead to three components of consumers responses mentioned before. Firs one is perceived goal impediment (Cho et al., 2004). When using the internet or mobile games, consumers are more likely to be goal-directed, they are searching for something or want to play five levels. The ads seen on the internet or in games are perceived more intrusive than other media ads because these ads interrupt the consumer's goal. Interruption may result to aggravation, negative attitude and ad avoidance.

The second construct is the perceived ad clutter. The number of ads seen is closely related to the perceived advertising clutter and the consumer sees the number too excessive (Cho et al., 2004). The ad clutter refers to all different kind of advertising: advertising on websites including banner ads, pop-ups and on mobile games such as forced ads, banners and video ads. If the consumer is feeling irritated with the number of ads or feel that the used site/game is only used as an advertising medium, the perceived ad clutter might lead to negative attitudes and thus to ad avoidance.

The third and final construct leading to components of consumer behaviour are prior negative experiences (Cho et al., 2004). Information learned from past experiences, is known to have a strong and direct impact on attitudes and behaviour. Prior knowledge and negative experience with ads can indicate annoyance and make the consumer less likely to click the ad or do actions towards them. The negative experience might lead them to avoid the source of the negative experience, like ad avoidance.

The mentioned three components have an effect on the behavioural outcome of ad avoidance, which are: cognitive, affect and behaviour (Cho et al., 2004). The subsequent components prior to behaviour, may lead consumers to intentionally ignore any personalized ads, which is cognitive ad avoidance, if they have negative feelings towards ads or do not like ads, as in affective ad avoidance. Consumers may also discard any personalized ads if seen on the

internet or mobile games by closing the site or closing the game app, which is behavioural ad avoidance. (Cho et al., 2004.)

Consumers are also sceptical for the strategies advertisers use to persuade consumers to buy/click/download ad content. More sceptical consumers evaluate advertisements more negatively and tend to avoid it more often. Thus, consumers may perceive customized ads as attempts to persuade and manipulate them, which then leads to higher probability of advertising avoidance (Cho et al., 2004). Tucker (2012) found that privacy concerns appear to be the leading behavioural driver in successful advertising. In cases of more privacy-sensitive services, like healthcare and financial, using targeted and obtrusive ads can diminish their effectiveness. The same issues effect mostly those consumers who show privacy-sensitive behaviour.

The results from tracking user behaviour and using that data for targeted and personalized ads vary between researches. Cho et al. (2004) found that by delivering targeted and customized ad messages through consumer profiling and behavioural tracking may reduce perceived goal impediment. This can lessen avoidance of ad messages. So, by delivering the right message at the right time might make the consumer feel that the ads support their goals and tasks, and not feel disrupted. On the other hand, Tucker (2014) found that consumers were concerned if the personalized ads are too personal and their privacy had been breached. In their studies Aqcuisti et al., (2015) and Turow (2009) found that if the consumers perceived to have control over their privacy, personalized ads were not seen too intrusive.

3.4 Research model

In the case of playing mobile games and whether watching ads in the game, the perception of privacy affects the behavioural outcome to keep on watching or advertising avoidance. Based on the previous studies six different factors were identified to have an affect to the perception of privacy. These factors are personal preferences and prior experiences, targeted ads, perceived control of data, number of ads, data collected and knowledge of the GDPR. Below the eight hypotheses for this study are presented and explained.

The first hypothesis states that people's personal preferences for privacy hold the previous experiences and information learned from them. Prior information affects the attitudes and behaviour towards advertising (Cho et al., 2004). It is proposed that:

H1: Personal preferences have a positive effect on the perceived privacy.

Targeted or personalized ads refer to person's personal view towards personalized ads (Tucker, 2014). Some researchers Cho et al., 2004) found that targeted ads help consumers reach their goals easier and if the perceived

personal relevance is high, the more likely it is that consumers have good perception towards advertising. Therefore:

> *H2: If the user perceives the ads as targeted and too personal, it has a negative effect on perception of privacy.*

Perceived control over data makes people more favourable towards personalized ads and privacy (Aqcuisti et al., 2015; Turow, 2009). Thus:

> *H3: The perceived control of data has a positive effect on the perception of privacy.*

Number of ads relate to the times ads are shown in the game, and if that amount is perceived to be too much. If consumers feel irritated because of too many ads, it might have a negative impact on the attitude towards advertising and result to ad avoidance (Cho et al., 2004). On this basis:

> *H4: If the number of ads shown is perceived too high, it has a negative effect on the perception of privacy.*

Users might not always be aware of what data is collected of them and if they are aware of the data collection, they might not know how that data is used. Loss of privacy might lead to tangible losses such as price discrimination (Aqcuisti et al., 2015). Users might suspect that their right to disclose personal information is threatened by advertisers or third parties (Baek & Morimoto, 2012). On this basis it is proposed that:

> *H5: If the user is unaware of what data is collected of her/him, it has a negative effect on perception of privacy.*

New privacy law GDPR covers all companies that process personal data of people residing in the EU region. Privacy became the topic of the discussion and was discussed widely in the media. The new regulation aims to give EU citizens better control of their data (Beatrix Cleff, 2007). Therefore, it's suggested that:

> *H6: GDPR has a positive effect on the perception of privacy.*

The perception of privacy has behavioural outcomes. If the perception of privacy is positive, it can lead to users engaging with the advertising in games (Aqcuisti et al., 2015). Thus:

> *H7: Positive perception of privacy leads user to watching ads in games.*

Whereas if the perception of privacy is negative, the behavioural outcome might be advertising avoidance, and not to engage and watch ads in games (Baek and Morimoto, 2012). On this basis:

H8: Negative perception of privacy leads to advertising avoidance

From these hypotheses the research model is constructed. Research model explains the relationship between each factor effecting privacy and the behavioural outcome. Please see below for Figure 2.

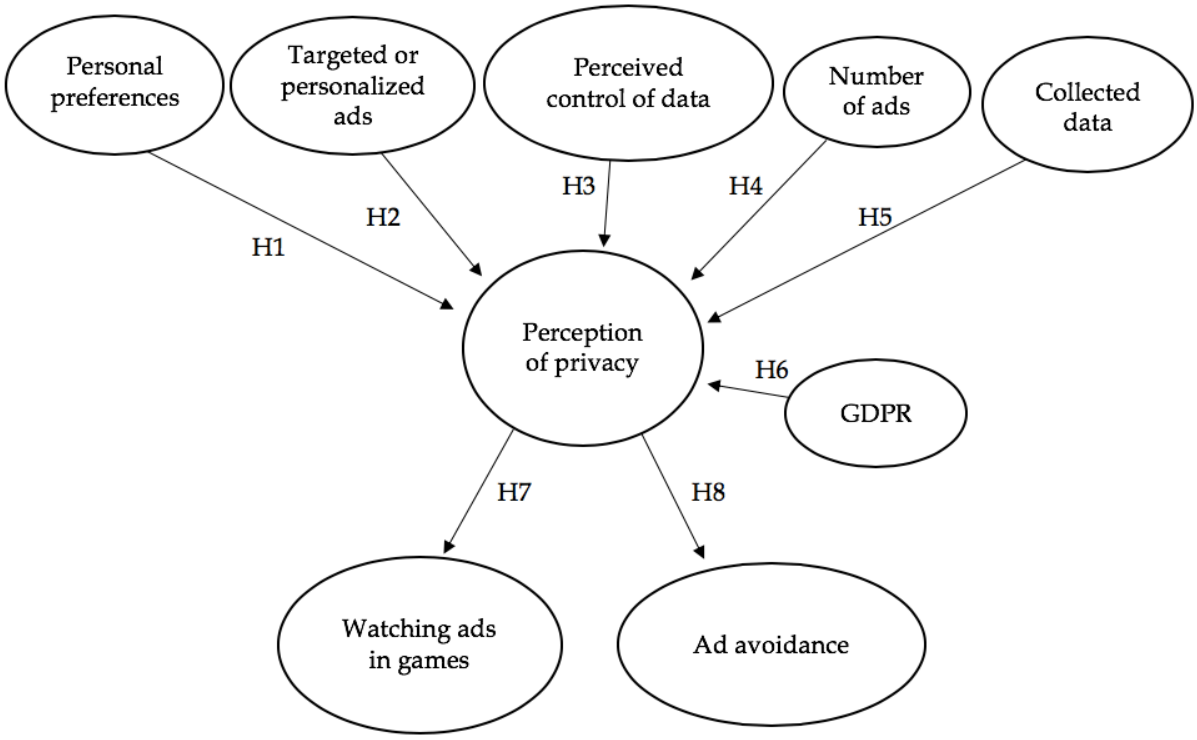


FIGURE 2: Research model

4 METHODOLOGY

This study tries to provide answers to what perceptions mobile game players have about data gathering and how it affects their behaviour when playing games. This study has a quantitative survey study research approach. Quantitative study suits well for the purposes of the study, because the aim of the study is to gain understanding on the phenomenon and be able to generalize the results to a wider audience. (Hirsjärvi et al., 2009.)

In this chapter, the chosen research method is presented and explained, along with the design process of the questionnaire and how the data for this study was collected. The practical implementation presents the chosen games where the survey was run and the determinants of the chosen player group. The final section describes how the data was analysed using the IBM SPSS Statistics v.26.

4.1 Research method

For this study data was needed for understanding what perceptions mobile game players have towards privacy and how that effected their behaviour in the games. The aim was to collect data that could be generalized to be accurate for users of Rovio's other games and outside Rovio's games as well. For this purpose, quantitative survey and questionnaire was chosen as the research method. Questionnaire is a structured method of research, as the researcher designs the questions that will enable data to be collected to answer specific research questions. Quantitative method is often used to test prior theories and explain phenomenon. (Bell et al., 2018.)

In quantitative studies data is often collected via questionnaire or structured interviews and the data is used to help define and compare phenomenon. Information is gathered in a standardized form from a defined group of respondents. The questionnaire is standardized, meaning that all the respondents answer to the same questions in the same order. Also, with using a questionnaire, the impact of the interviewer is minimized, and large data set can be gathered rather quickly. (Hirsjärvi et al., 2009.)

Using quantitative research method and questionnaire have some challenges, the answers might not be completed, and the researcher is unable to know whether the respondents answered truthfully. Also, it is hard to estimate how much prior knowledge the respondents have about the studied subject. When designing the questionnaire, the researcher must take note to minimize the possible misunderstandings when respondents answer to the survey. Sometimes those are hard to prevent, especially when the survey is done in a web environment. (Hirsjärvi et al., 2009.)

4.2 Study implementation

4.2.1 Questionnaire

With the help of a questionnaire it is possible to collect data about facts, attitudes, behaviour and perception. Using a questionnaire survey a relatively large data set can be collected quickly with little expenses (Hirsjärvi et al., 2009). Thus, it is argued to use survey as the chosen research method for this study, as the research question is to understand players perception on privacy in mobile games.

When designing a questionnaire, it is important to make the questions easy to answer and to complete the questionnaire (Hirsjärvi et al., 2009). This was taken into consideration when designing the questionnaire to minimize the drop outs. When answering to the questionnaire on a mobile device, a percentage bar at the bottom of the page indicated the progress. With a careful design of the questionnaire researcher can improve the success of the study (Hirsjärvi et al., 2009). The questionnaire was designed to fit for the purpose and goals of this study.

TABLE 1: Measuring instruments

Personal preferences and previous experiences.	Cho et al., 2004
Personalized ads	Swaid and Wigand, 2009
Control of data	Merisavo et al., 2007
Number of ads	Cho et al., 2004
Collected data	Merisavo et al., 2007
GDPR	Flynn and Goldsmith, 1999
Watching ads	Merisavo et al., 2007
Avoiding ads	Cho et al., 2004

Questions for the questionnaire were designed based on the theory presented before in this study (please see Appendix). The questionnaire was conducted in Finland in Finnish to suit the audience best and avoid misunderstanding. Thus, the measuring instruments were translated from the original language English to Finnish. The original meanings were tried to keep as similar as possible, but some compromises were made in this phase.

Personal preferences and previous experiences were measured using a scale made by Cho et al. (2004) measuring the experience of engaging with ads and had three items in the questionnaire. Personalized ads were measured using Swaid and Wigand's (2009) scale for personalization, this construct had three items. The scale for control of data included three items from the study of Merisavo et al. (2007) and three items. Number of ads was measured using two items adapted from Cho et al. (2004).

Questions for data collection and intention to watch ads were derived from the scale created by Merisavo et al. (2007). To measure players' awareness and knowledge about GDPR, two items were made by following the scale created by Flynn and Goldsmith (1999). Cho et al. (2004) provided also the outline for questions to measure advertising avoidance and this construct was measured with three items. Additionally, four questions were added as background variables, these were days players play games in a week, how many other mobile games they play, age and gender.

All questions had a 5-point Liker scale ranging from "strongly disagree" to "strongly agree". Players chose the most suitable option from the scale for each question. The questionnaire was created in a SurveyGizmo online tool and then the survey was shown in two games. A total of 22 constructs and four background factors were included in the questionnaire. The questionnaire was tested beforehand with 13 respondents to figure out possible issues.

4.2.2 Practical implementation

The survey was shown in two of Rovio's games, Angry Birds 2 and Angry Birds Friends for four days in Finland. These games were chosen as they have a similar core game play mechanic, slingshot. Thus, it is argued that the survey answers from both games can be used simultaneously. The questionnaire was shown in an interstitial ad placement, which appears in between levels after several minutes into the play session. This mechanic applied to both games where the questionnaire was shown. The placement showed a picture encouraging players to answer a survey and to help improve the game. The interstitial placement can be closed after a few seconds, so players were not forced to answer in the survey. If they chose to click on the survey image, they had a chance to return to the game at any point and were not forced to complete the survey.

The questionnaire was shown only to players who had played the game for more than three days. This was done to make sure that players had had time to get to know the game and they would be more familiar with the mechanics and advertising done in the game. Survey was shown only once to a player, and after this the survey was no longer shown to the same player. This applied between games, if a player saw the questionnaire in Angry Birds Friends, they no longer saw it in Angry Birds 2. Rovio conducts other surveys in their games to improve the user experience (Rovio privacy policy, 6.4.2020).

4.3 Data analysis

The survey data was transferred from SurveyGizmo to IBM SPSS statistics v.26 program for statistical analysis. All the questions in the questionnaire were obligatory, so completed answers had no missing values. The questionnaire had a total of 152 complete answers. The analysis of the study should be done based on the theory and theoretical framework (Karjaluoto, 2007).

The data was first analysed in SPSS statistics program and to test the research model analysed in SmartPLS 3.2. Analysing methods are presented in the Results section of this study.

5 RESULTS

In this section of the study the results are presented. First the demographic factors are presented along with the background factors. This will be followed by presenting the descriptive study constructs and mean comparison. Factor analysis was done by creating factors based on theory and started in SPSS and then analysed in SmartPLS 3.2 to assess the research model and test the hypotheses. Lastly, a comparison between the King and Rovio privacy and advertising policies is presented.

5.1 Describing the data

The questionnaire for this study got a total of 152 completed answers and 65 incomplete answers. Incomplete answers were left out when analysing the data. As expected by the usual player demographics of mobile games, over 68% respondents were male, and 28% were females. Most of the respondents were over 30 years of age, between 30 and 50+ years. Biggest age group was players over 50 years (36.2%), second biggest group was players between 41-50 years (28.9%) and third biggest was 31-40 years (23.7%). This result is not unusual for games that are targeted towards older players as Angry Birds 2 and Angry Birds Friends are.

TABLE 2: Demographic profile of the respondents

Demographic factors	Frequency	Valid percent %
Gender		
Female	43	28.3
Male	104	68.4
Other	5	3.3
Total	152	100
Age		
13-19	6	3.9
20-25	4	2.6
26-30	7	4.6
31-40	36	23.7
41-50	44	28.9
50+	55	36.2
Total	152	100

Majority of the respondents (N=107, 70.4%) reported to play on 6-7 days a week. Second active group of players reported to play on 4-5 days a week (17.1%) and close to 10% reported to play on 2-3 days a week. The least active group had only 4 respondents (2.6%), they reported to play on one day or less in a week. It can be said the respondents are quite active players and play on consecutive days a week.

Final background factor in this study was the amount of other mobile games respondents play, other than the one they are currently playing (Angry Birds 2 or Angry Birds Friends). The players were expected to play at least one game, as they would not have been able to answer to the questionnaire in other platform. Almost 15% of the players claimed that this was the only mobile game they played, but 56% of the respondents reported to play 1-2 other games than the one currently played. Those players who reported to play games claimed to play 4-5 other games (27%) and only four people (2.6%) claimed to play more than seven games. Thus, it can be said that players of the test games are quite devoted to few games and they play those games many times a week.

TABLE 3: Background factors

Background factors	Frequency	Valid percent %
Days play games in a week		
One day or less	4	2.6
2-3 days	15	9.9
4-5 days	26	17.1
6-7 days	107	70.4
Total	152	100
Number of other games played		
I don't play other games	22	14.5
1-2 games	85	55.9
3-4 games	41	27.0
5-6 games	0	0
7+ games	4	2.6
Total	152	100

5.2 Describing measuring constructs

In this section of the study descriptive analysis are done to data. Descriptive statistics are presented in five different groups based on the research model's eight constructs. Constructs effecting the perception of privacy were personal preferences/prior experiences, targeted ads, perceived control of data, number of ads, collected data and the effect of the introduction GDPR. Then the behavioural outcome constructs, watching ads in games and ad avoidance, are also presented. Each construct is presented in their own chapter.

5.2.1 Personal preferences and prior experiences

Personal preferences and prior experiences were measured using three measures. Respondents were asked to value the below statements (see Table 4) when they are playing mobile games. The mean for the items ranged from 2.28 to 3.13 (standard deviation between 1.081 and 1.360), where players felt most positive about advancing in the game with the help of advertising.

Interestingly in the final question about gaining some benefit by watching advertising has two modes: 1 (strongly disagree) and 4 (somewhat agree). This divides players into two groups; the ones who feel that they are not gaining anything by watching ads and the others who feel quite positive about the benefits of watching ads in mobile games. In the EXP3 item largest group after the modes was for "somewhat disagree", thus explaining why the mean is below 3. Based on these results it can be argued that players have quite neutral preferences for ads, but somewhat negative experience with ads, even though they feel that they are receiving benefits.

TABLE 4: Descriptive statistics for personal preferences and prior experiences

Item	Mean	Mode	SD
EXP1: I feel that my experience with watching advertising has been good	2.28	2	1.081
EXP2: I can advance in the game with the help of advertising	3.13	4	1.360
EXP3: I gain some benefit by watching advertising	2.62	1,4	1.345

5.2.2 Targeted or personalized ads

Questions were trying to explain, whether players felt that the ads seen in games feel targeted or personalized for them. Means are ranging between 1.72 and 2.03 (standard deviation between .866 and 1.079), so quite on the negative side of the scale. Players didn't feel that the ads shown in games are personally interesting to them or that the shown ads fit their needs. They did feel most positively about the ads enabling them to find other products or games, but then again most of the answers fell under the neutral scale.

TABLE 5: Descriptive statistics for targeted or personalized ads

Item	Mean	Mode	SD
PER1: The game gives me personally interesting advertising	1.84	1	.997
PER2: The game shows me ads that fit my needs	1.72	1	.866
PER3: The ads enable me to find other products or games that meet my needs	2.03	1	1.079

5.2.3 Perceived control over data

Third item measured the player's perceived control over data. Item means for this scale varied from 3.91 and 4.51 (standard deviation between .853 and 1.312), which means that players agreed very strongly for the questions. All the measures were well above the neutral, and the mode for all questions was 5, (strongly agree).

Players agreed especially strongly towards that it is important to be able to refuse to receive targeted advertising (4.51). Also, they want to receive targeted messaging (3.91) only if they had given their permission for that. This might explain the strong negative results in the previous scale, where players felt that the ads were not personally interesting to them.

TABLE 6: Descriptive statistics for perceived control of data

Item	Mean	Mode	SD
CON1: I would only be prepared to receive targeted advertising in mobile games if I had provided my permission	3.91	5	1.312
CON2: It is important for me that I can control the permission to receive targeted advertising in mobile games.	4.22	5	1.024
CON3: It is important to me that I can refuse to receive targeted advertising.	4.51	5	.853

5.2.4 Number of ads

Fourth construct in the research model was number of ads. This item had two questions, which measured the players feelings towards the number of ads seen when playing mobile games. The values were reverse coded when preparing for the analysis because of the negative wording in both questions. Means are 1.7 and 1.95 and for both questions the mode is 1 (standard deviations of .866 and .975). Players have quite strong feeling towards ads, as they feel that there are both too many ads and that the ads are found irritating in mobile games. Then again, players find ads to be annoying when at the same time they feel they are advancing in the game by watching ads, as mentioned previously.

TABLE 7: Descriptive statistics for number of ads

Item	Mean	Mode	SD
NUM1: The amount of advertising in mobile games is excessive	1.70	1	.866
NUM2: The amount of advertising in mobile games is irritating	1.95	1	.975

5.2.5 Data collecting and usage

Fifth construct is the unsureness of what data is collected of the players and how it is used and whether players believe that their data is used properly. Means are ranging between 2.53 and 3.33 (standard deviation between 1.156 and 1.250). Both DAT1 and DAT2 are nearly the neutral, so players are unsure that data holders use their data as they have approved. Game companies seem to enjoy a bit more trust (2.78) compared to marketers (2.53). Despite the distrust to data holders, players are leaning towards trusting that the privacy laws protect consumers (3.33).

TABLE 8: Descriptive statistics for collected data and how it is used

Item	Mean	Mode	SD
DAT1: I believe that game companies use my data only for a purpose that I have approved	2.78	2	1.156
DAT2: I believe that marketers would use my data only for a purpose that I have approved	2.53	2	1.250
DAT3: I believe that the consumer is protected by laws related to data privacy	3.33	4	1.189

5.2.6 General Data Protection Regulation (GDPR)

Knowledge of GDPR was measured in the sixth construct. Item means were 2.96 and 2.80 (standard deviations of 1.356 and 1.236), so close to neutral values. Interestingly mode for both questions was 4 (somewhat agree), which explains the bigger standard deviations. Players are a bit more aware of what the GDRP contains than how it actually affects the data collection. Both questions are close to neutral, so players know something about the GDPR and have heard about it.

TABLE 9: Descriptive statistics for the knowledge of the GDPR

Item	Mean	Mode	SD
GDP1: I know pretty much about GDPR (General Data Protection Regulation)	2.96	4	1.356
GDP2: I can judge the effects GDPR has to companies' data collection	2.80	4	1.236

5.2.7 Watching ads

The two final constructs in the research model were the behavioural outcomes on perception of privacy. The first of these measured the players feeling about advertising and intention to keep on watching ads in mobile games in the future. These were measured using three items and questions were done based on the study by Merisavo et al., (2007). Means for the questions range between 2.10 and 2.59 (standard deviations between 1.091 and 1.247), so towards the negative side of the scale. Modes were 2 and 1 for the two latter questions.

These results indicate that players do not feel very positively about advertising in mobile games, confirming the results of the first and fourth construct. However, the final question WAT3 had the biggest standard deviation, which means that the values ranged most out of the three. It could be stated, that players have close to neutral stance for watching ads in the future.

TABLE 10: Descriptive statistics for watching ads

Item	Mean	Mode	SD
WAT1: I feel positively about advertising in mobile games	2.34	2	1.091
WAT2: I am willing to receive advertising in mobile games in the future	2.10	1	1.108
WAT3: I would see advertising messages I receive in mobile games in the future	2.59	1	1.247

5.2.8 Ad avoidance

Eight and final construct of the research model and the second construct of the behavioural outcome is ad avoidance. Values of the questions were reverse coded in the preparation for the analysis, as all the questions are negatively phrased.

Means for the questions vary between 2.07 and 2.53 (standard deviation between 1.096 and 1.352). Mode was 1 for all the questions. Based on the results it can be stated that players do not have a good perception towards advertising in mobile games and would rather have games without them. This result again collides with the mentioned findings that players feel that they gain benefits and advance in the games with the help of advertising.

TABLE 11: Descriptive statistics for ad avoidance

Item	Mean	Mode	SD
AVO1: I avoid advertising in mobile games	2.35	1	1.246
AVO2: It would be better, if mobile games didn't have advertising	2.07	1	1.096
AVO3: I do not click or watch ads in mobile games	2.53	1	1.352

5.3 Mean comparison

When analysing the variables, some differences were found between the demographic and background factors. While doing analysing the correlations, some factors were found to correlate stronger with some variables and thus tests analysing mean were done. Tests were done for all the demographic and background factors. Tests were done using One-Way variance analysis, ANOVA, and also Independent Samples T-test on some variables. Tukey's test was done to further analyse the results of the One-way variance analysis (Karjaluoto, 2007).

Using One-Way variance analysis, no statistical significance was found when analysing variables by gender, other than for the whole DAT item, collected data and how it's used. Variables were only analysed using Female and Male values, as the third option had very small response amount (N=5). For each variable, females had higher values then males and results had the statistical significance. For DAT1 women had a mean of 3.26 and standard deviation of 1.157, whereas men had a mean of 2.64 and standard deviation of 1.079. For DAT2 mean was 3.14 for women (SD=1.246) and 2.35 for men (SD=1.164). In item DAT3 women had a mean of 3.79 (SD= .989) and men had 3.22 (SD=1.165).

TABLE 12: Collected data and how it's used

Item	F	*p*	Means	SD
DAT1: I believe that game companies use my data only for a purpose that I have approved	7.568	.001	Female: 3.26 Male: 2.64	Female: 1.157 Male: 1.079
DAT2: I believe that marketers would use my data only for a purpose that I have approved	11.353	.000	Female: 3.14 Male: 2.35	Female: 1.246 Male: 1.164
DAT3: I believe that the consumer is protected by laws related to data privacy	10.023	.000	Female: 3.79 Male: 3.22	Female: .989 Male: 1.165

Thus, it can be argued that women believe that game companies and marketers use the collected data as the player has approved. However, the means for all the answers are on the neutral scale, where the DAT3 had the highest mean of 3.79 for women. So even though the perception is on the positive side, it is not very high.

After gender comparison the same tests were done by using player's age as a factor. There were significant differences with CON2 variable with the youngest age group 13-19 to other age groups. However, the sample was so small for the youngest group (N=6), so these results are disregarded. When analysing the age groups with biggest samples 31-40 (N=36), 41-50 (N=44) and 50+ (N=55), no statistical significance was found with any variable.

Variance analysis was also conducted using days played in a week as the factor. All the variables were analysed, even though the biggest sample group by far was those who played 6-7 days (N=107), so that was only compared

between the second biggest sample, 4-5 days (N=26). No significance was found between these groups for any variable.

Lastly variance analysis was done by using the amount of other games as the factor. This was done by comparing the values of larger samples, ignoring those groups of players who played more than 4 games (5-6 games, 7+ games) as the sample sizes were so small. Only statistically significant find was with DAT3 variable with F=5.079 (p= .002, where $p < 0.05$, mean=3.33, SD=1.291). Differences were found between those who did not play any other game and those who played 1-2 games (p= .049, where $p < 0.05$), however there were no statistical differences. Differences were found also with those who played 1-2 games and 3-4 games (p=0.013, where $p < 0.05$).

When analysing deeper the means between the groups, those who do not play other games (mean=3.77, SD=1.066) and those who play 3-4 other games (mean=3.73, SD= .949) have more positive stance towards that privacy laws protect the consumers. Although the biggest sample group was those who play 1-2 other games (N=85) and they had a neutral stance towards privacy laws (mean=3.06, SD=1.238). Thus, no conclusion can be drawn that playing more games would increase the trust for privacy laws protecting consumers.

5.4 Factor analysis

When doing factor analysis, some preconditions are important to take into consideration before the data is suitable for factor analysis. Explorative factor analysis was done to the data as preparatory analysis. This was conducted in SPSS program.

5.4.1 Measurement model

Continuing the factor analysis was done by using SmartPLS 3.2 and confirmatory factor analysis, please see table 13. Exploratory factor analysis done in SPSS revealed six factors, as mentioned in the previous chapter, and those factors were used in the confirmatory factor analysis. Seven items were deleted because their communalities were not strong enough, thus leaving 15 items for the analysis. Factors were divided into groups to better follow and fit the research model and theory. The final factor structure in SmartPLS 3.2 consisted of intention to watch ads (WAT3, WAT2), targeted ads (PER1, PER2, PER3), amount of ads (NUM2, NUM1), collected data (DAT2, DAT1, DAT3), control of data (CON2, CON1, CON3) and GDPR (GDP1, GDP2). Factor loadings can be seen below in table 13.

TABLE 13: Factor loadings

Factor	Item	Outer loadings
Intention to watch ads (WAT)	WAT1	0.938
	WAT2	0.898
Targeted ads (PER)	PER1	0.895
	PER2	0.894
	TAR3	0.833
Amount of ads (NUM)	NUM1	0.957
	NUM2	0.966
Collected data (COL)	COL1	0.914
	COL2	0.919
	COL3	0.792
Control of data (CON)	CON1	0.646
	CON2	0.901
	CON3	0.891
GDPR (GDP)	GDP1	0.636
	GDP2	0.989

To evaluate the validity of the measurement model Average Variance Extracted (AVE) test was done to measure factor correlations and square roots of AVE. AVE values should be above 0.5 (Karjaluoto, 2016), which was the case for all the factors in this study. Also, the square root of AVE should be bigger than the value of correlation between factors. This also applies for this study thus it can be stated that discriminant validity is achieved. Values can be seen below in table 14.

TABLE 14: Composite reliability, AVE and correlation between factors

Factor	CR	AVE	PER	CON	NUM	COL	GDP	WAT
Targeted ads (PER)	0.907	0.765	0.875					
Control of data (CON)	0.859	0.674	-0.814	0.821				
Amount of ads (NUM)	0.961	0.924	0.364	-0.428	0.961			
Collected data (COL)	0.909	0.770	0.215	-0.163	0.257	0.877		
GDPR (GDP)	0.811	0.691	0.034	0.158	-0.048	-0.131	0.832	
Intention to watch ads (WAT)	0.915	0.844	0.490	-0.262	0.446	0.321	-0.072	0.918

5.4.2 Structural model

Using structural model evaluation, the research hypotheses were tested. This study had eight hypotheses, and each will be discussed in their own section. Path coefficients (β) and R^2 values were used to measure relationships between factors (Karjaluoto, 2016). The results and significance of these values are presented in Table 15. Bootstrapping was used to evaluate the statistical significance of path coefficients. R^2 values indicate the percentage that variables together cause of the dependent latent variable. The results show that the variables accounting for perception of privacy explain 69% of it. Also, that the perception of privacy explains 59% of watching ads and 45% of ad avoidance.

TABLE 15: Structural model results

	β	R^2	T-values	P-values
H1: Personal preferences -> Perception of privacy	.538**		9.512	0.00
H2: Targeted ads -> Perception of privacy	0.75		1.260	0.208
H3: Perceived control of data -> Perception of privacy	-0.76		1.545	0.123
H4: Number of ads -> Perception of privacy	.299**		4.552	0.00
H5: Collected data -> Perception of privacy	0.93		1.743	0.082
H6: GDPR -> Perception of privacy	-.106		1.826	0.068
H7: Perception of privacy -> Ad avoidance	0.668**		12.623	0.00
H8: Perception of privacy -> Watch ads	0.768**		21.510	0.00
Perception of privacy		0.686		
Watch ads		0.590		
Ad avoidance		0.446		

** $p \leq 0.05$; (one-sided test)

Out of the factors creating the perception of privacy, personal preferences (p=0.00, t=9.512) and number of ads (p=0.00, t=4.552) had the biggest impact and they are statistically significant (where p<0.05). These two can be said to be the biggest factors affecting the perception privacy. When analysing the effect on perception of privacy to behavioural intention, it has statistical significance (where $p < 0.05$) as mentioned in table 15. The t-values were pretty high for both variables, but the watching ads had a higher value (t=21.533), when ad avoidance had lower (t=12.623).

For the first hypothesis the path coefficient between personal preferences and perception of privacy is .538 and t-value was 9.391 (p=0.00), which is also the highest value of factors effecting the perception privacy. With this result it can be stated that personal preferences have a significant effect on the perception of privacy. Thus, hypothesis 1 is supported. The second hypothesis has a path coefficient of 0.075 and t-value 1.263 (p=0.208). The patch coefficient had some effect on the perception of privacy, even though not very strong. When studying descriptive statistic for this construct, the means for the

questions were more on the negative side, so players didn't find the advertising to be very targeted or interesting. With these results H2 is rejected.

For the third hypothesis the path coefficient was -.076 and t-value 1.507 (p=0.123). When studying the descriptive statistic for this construct, the values were very high, meaning that players thought it very important to have control of one's data. The weak result for this hypothesis could be explained by the question items, which didn't ask whether players felt they were in control of their data, rather than is it important to them. Hypothesis 3 is rejected based on these results. Fourth hypothesis studied the number of ads shown in games. Path coefficient was .299 and t-value 4.429 (p=0.00). This was the second strongest factor effecting the perception of privacy in the model. Hypothesis four is supported.

The fifth hypothesis has a path coefficient of 0.093 and t-value 1.670 (p=0.082), which does have some effect on the perception of privacy. The descriptive statistics for the question items were on the negative side, except for the stance on privacy laws protecting customers, which were more on the positive side. Hypothesis 5 is supported, even though not very strongly. For the sixth hypothesis the path coefficient was -.106 and t-value 1.820, and some of the low values could be explained by that the players didn't have a lot of knowledge of the GDPR. The statistical significance was 0.069, so close to being significant ($p<0.05$). When analysing the descriptive statistics, the values were more on the negative side, but pretty close to neutral. Even though players believe that privacy laws protect customers, H6 "*GDPR has a positive effect on the perception of privacy*" hypothesis does not get support in this study.

For the seventh hypothesis the path coefficient was 0.768 and t-value 21.533 (p=0.00) and of statistical significance ($p<0.05$). Thus, the relationship between the perception privacy and watching ads is quite strong. But as the descriptive statics showed, players had a neutral stance towards watching ads. This could be explained by the overall attitude towards ads, as measured in the personal preferences. As the values are quite high, this hypothesis is supported. The final eight hypothesis studied advertising avoidance. The path coefficient was 0.668 and t-value 13.499 (p=0.00), which are also quite high. The mean values for all three question items were on the negative side, which again follows the overall attitude towards advertising, which is more on the negative side. With these results this hypothesis is also supported.

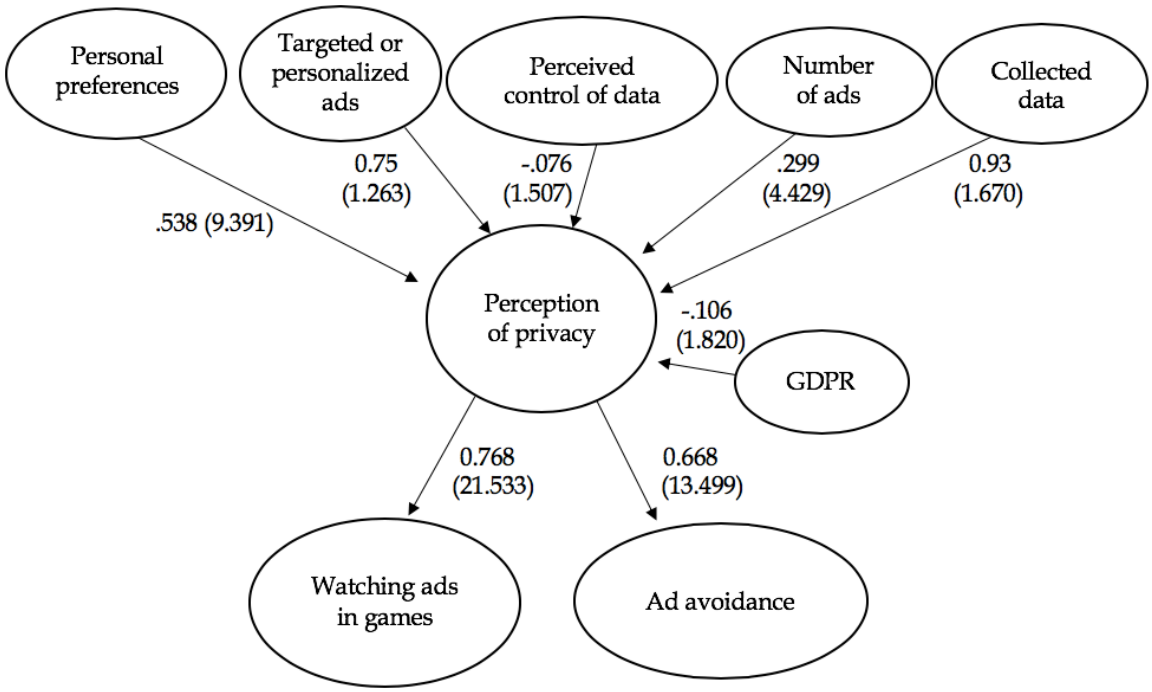


FIGURE 3: Empirical model (t-values in parentheses)

5.5 Privacy policies in game companies

Last section of the results section is the comparison done between two game companies, King.com and Rovio. Privacy and advertising policies were accessed and read in the companies' websites and the key differences are highlighted and presented in this section.

Due to the new regulations from the introduction of GDPR, all companies who process private data of people residing in the EU, thus also game companies, had to revisit and revise their privacy statements. In this section of the study two different privacy policies from two game companies are reviewed. The chosen game companies are King.com Limited, referred later as King, and Rovio Entertainment Corporation, referred later as Rovio.

King was established 2003 in and was acquired by Activision Blizzard Inc. in February 2016 and operates as an independent unit of the company. King reports to have developed over 200 games, such as Candy Crush, Farm Heroes and Bubble Witch Saga (King.com, accessed in 2.3.2020). Rovio Entertainment Corporation was already introduced in the introduction section of this study. These two companies were chosen for the comparison in this study because they both are well-established game companies, are over 10 years old and have published multiple successful games.

5.5.1 Privacy policy comparison

The comparison between the privacy policies of King (King privacy policy, accessed 2.3.2020) and Rovio (Rovio privacy policy and Rovio terms of service, accessed 2.3.2020) was done based on the key rights for users' data privacy and responsibilities for businesses mentioned in Corcoran and Costache's (2018) study. Data protection impact is not included in the comparison, as the assessment of the risks is not comparable and will be done inside the companies. In the table below, it is explained how both privacy policies align with the study and whether they include the points mentioned. Advertising privacy policies are also valued as another meaningful factor for this study.

King and Rovio's privacy policies had some differences in them, please see Table 1. First being one of the user's rights. In King's privacy policy there was no mention of the procedure or processes in case of data breaches and how that would be informed to the users. Both policies mention the player's right to access and receive data what has been collected of them, if requested. Data portability was also discussed in both policies, players have the right to receive their data and transform that to another provider.

TABLE 16: Privacy policies compared with Corcoran and Costache's (2018) framework

	Company	
	Rovio	**King**
User's Main Rights		
Breach notification	Can send service-related communications (e.g. technical notices, security alerts, or administrative messages).	Not mentioned.
Right to access	Included.	Included.
Right to erasure or Right to be forgotten	Included. Automated tools in the game to do that.	Included, has multiple steps and depends on the player's location. The games must be deleted from devices.
Data portability	Included.	Included.
Company's Main Responsibilities		
Data protection by design and data minimization	Data protection mentioned and described. Data collected to improve the game experience.	Data protection mentioned and described. Data collected to improve the game experience.
Designation of a data protection officer	Have an appointed DPO	Not mentioned. Mentioned an email to contact.
Obtain clear consent from user	By playing the games, player approves the terms of the service and agrees with the privacy notice	By playing the games, player approves the terms of the service and agrees with the privacy notice
Processing of personal data should be lawful and fair	Right to collect data is based on legitimate interests	Right to collect data is based on legitimate interests

The second difference between the policies is in the player's right to ask their data to be deleted. In Rovio's policy it's stated, that players can request this by using the automated tools in each game. In King's policy the process of data deletion had multiple steps and the process is not so straight forward. The deletion process is different for marketing, such as email, but if the player wishes to their data to be deleted from games, they have to delete the game completely. This right will also be discussed further later in advertising policies.

Then the company's main responsibilities were compared according to Corcoran and Costache's (2018) framework. The first company's responsibility is data protection and minimization, both policies explain why personal and behavioural data is collected. Also, both mention security measures, but it's hard to evaluate and compare those in this study. Rovio also had disclaimer, that they do not collect or process any special categories of data such as genetic, ethnic origin or political opinions. Third difference is found on the designation of a data protection officer. Rovio mentions to have a designated DPO, but King has no mention of this. They do mention a way to contact them about any privacy related matter.

Both companies handle consent also same way. In policies is stated, that by downloading and playing the games, players approve the terms of service and agree with the privacy policies. Both company's games have a pop up about the privacy and terms of service, and explained that by continuing to play, players agree with those. Also, in Rovio's terms of service, it is said that by playing the games players accept the terms and that they are 13 of age or older.

As mentioned before, in the United States the Children's Online Privacy and Protection Act (COPPA), limits the data collected online of personal information from children under the age of 13 (Newman et. al., 2014). King mentions country specific age restrictions to play, all of those are above 13. Fourth and final responsibility for the company was processing of personal data should be lawful and fair. Both privacy policies claim that the right to collect data is based on legitimate interests.

5.5.2 Advertising policy comparison

As mentioned before, by playing the games, players agree with the privacy policies. For advertising purposes, the advertising ID is collected, which is a non-personal alphanumeric string of digits provided by the operating system of a device and uniquely associated with certain devices (Rovio privacy policy, accessed 5.3). Also based on the IP address of the device companies can see the country, region or city of origin of the player. Below in Table 2 the advertising privacy policies of the companies are compared.

From the advertising ID's, the companies can track players interactions, e.g. clicks and downloads, with ads and use that to show them more relevant ads. The data also enables companies to inform players of new content, in-game offers and optimize the number of ads shown. An interesting mentioning in King's policy is that they state to show in their games only ads of their own or Blizzard's games. Rovio, however states to show ads of its own games along

with third party network ads. King states to use the data collected from its games, to place its ads in third party services to promote its games.

Both policies mention, that the advertising trackers can be reset from devices own settings. They also mention, that even if reset, ads will be shown in games, but they might be less relevant to the player. The fourth and final item discusses with whom the collected data is shared with. Rovio states to share data with companies who provide them services and with advertising partners, who process data independently from Rovio. King also mentions suppliers used to help provide game services, third parties for marketing purposes and if necessary legal authorities.

In its policy Rovio claims to have 14 advertising partners, who advertise in its games, whereas King has 74 advertising partners. Both companies claim to share data with these companies. This difference might be explained by the fact, that King considers as partner sites and apps in which sites and apps they advertise their own products and services, while Rovio considers as partners those companies who advertise in its games.

TABLE 17: Rovio's and King's advertising privacy policies

	Company	
Advertising privacy policy:	**Rovio**	**King**
What data is collected	Advertising ID, IP address, interactions with ads (clicks and downloads) in the game.	Advertising ID, IP address, interactions with ads (clicks and downloads) in the game.
How that data is used?	Show more relevant ads, inform players about new content and offers, limit the number of ads seen, ad networks serve more interesting ads	Optimization, customizing in-game offers, interest-based ads, limit the number of ads, show other King or Activision Blizzard ads, place ads on 3rd party services
Can the ads tracker be reset?	Yes, from the device's settings. Player would still receive advertising, but less relevant	Yes, from the device's settings. Player would still receive advertising, but less relevant
With whom the data is shared?	Companies that provide services for Rovio, advertising partners who process data	Transfer data to affiliated entities or 3rd parties. If necessary to legal authorities

6 DISCUSSION

This final chapter presents the relationship between the main empirical findings and earlier studies discussed in the theory section. This chapter will answer to the proposed research questions mentioned in the introduction. Theoretical contributions along with managerial implications are also discussed. Finally, the evaluation of the research will be discussed and alternative research lines and future directions of the research are suggested.

6.1 Theoretical contributions of the study

The aim of the study was to clarify what perception mobile game players have about privacy and what is its effect on their behaviour in the games while playing. The major interest was whether players intend to watch advertising in games or are they trying to avoid them. Relevant previous research and theories related to advertising in mobile games and privacy behaviour were used as the base of this study.

First research question of this study was about players' views on data gathering and privacy in mobile games. The second question inquire how these perceptions affect players behaviour in mobile games, will they watch advertising, or will they try to avoid it. Third research question analysed the effect of GDPR on perceptions and willingness to watch the ads. Based on these questions eight research hypotheses were presented and a questionnaire survey was conducted to answer in these questions. This study was done in cooperation with Rovio Entertainment Corporation and questionnaire was shown in two of Rovio's games, Angry Birds 2 and Angry Birds Friends.

These questions were first studied on the basis of relevant theories and previous research. As mobile games and other media platforms players use collect a lot of information about them, questions arise whether that data is used as promised and if players know what data is collected about them (Beatrix Cleff, 2007). Consumers find it very important to have control over the data collected of them (Tucker, 2014) and this was also shown in this study, as players reported it to be very important to them that they can control the permissions to receive targeted advertising. This result was not supported by this study, as the effect of perceived control of data did not have a significant effect on perceived privacy.

Using behavioural tracking for targeting the ads can be seen more favourable, as it leads to interest-based advertising which suits better to the consumers' needs (Turow et al., 2009). However, if the advertising is considered to be too personal, it might lead to advertising avoidance (Cho et al., 2004). Players in this study reported that they did not perceive the ads seen in mobile games too targeted, or that they showed personally interesting content to them. This might be one of the reasons of why results indicated that the intention to

watch ads was higher than advertising avoidance. When asked if game companies and marketers use the collected data as promised when giving permission, players trusted gaming companies more than marketers. The trust was close to neutral level, but suggested players might have some doubts on how data owners use that data. However, the players trusted more that the privacy laws are able to protect consumers.

The perception of privacy and using data for targeted advertising had divided results in earlier studies, Cho et al. (2004) found that targeted advertisements may decrease avoidance, and Tucker (2014) showed that specifically targeted ads breached consumers privacy. Aqcuisti et al., (2015) found in their study, that if consumers feel to be in control of their own data, personalized are not considered too intrusive. This was also seen in this study by the varying results of the structural model. The results showed, in line with studies of Cho et al. (2004), that personal preferences and prior experiences were the strongest factor affecting the perception of privacy as found by.

The biggest factor decreasing the perception of privacy in this study was found to be the number of ads. Players reported that if there are too many ads in mobile games, and they are found to be somewhat irritating. This supports the finding of Cho et al. (2004), showing that perceived ad clutter leads to advertising avoidance. Cho et al. (2004) also mentioned, that different factors affecting the perceived ad clutter included number of ads, timing of ads, their size or duration. These support the finding in this study that players experience advertising to help them advance in games and that they received some benefit from them.

This study was also trying to find out if the introduction of GDPR has affected the players perception of privacy. Beatrix Cleff (2007) mentioned that GDPR was the first notable privacy regulation, as it was the first to impose sanctions to possible violators. As already mentioned before, players did trust that privacy laws are protecting consumers and most of the players reported to know something about GDPR, as presented in the descriptive statistics. The values of analysis were on the neutral level, indicating that players were aware of the GDPR but did not find it to have a significant effect on personal data protection. It remains unknown whether players know about their rights concerning the protection of their personal data and specifically what are the details of policies as mentioned and compared in the game company privacy policy comparison in this study.

When comparing the privacy policies of Rovio and King.com with Corcoran and Costache's (2018) framework some differences were found. First finding was that Rovio had more clearly stated in their policy the main rights of the users as described in the GDPR. The second difference was on executing the players' right to have their data to be deleted. King had multiple steps in this process was not straight forward, and the player would need to delete all their games from their mobile devices. With privacy policies like this, the result of this study, that players did not trust the gaming companies to process their data as promised, is understandable.

Advertising policies of Rovio and King.com were also compared. Both policies explain what data is collected through advertising and how it is used,

mainly to show the players more relevant ads. As already mentioned, players in this study did not find the ads to be too personalized or targeted, thus not raising privacy issues. However, players might have difficulties when evaluating how their data is actually used and with whom it is shared. These are explained in the advertising policies, but they can be difficult to evaluate as a player. Also, most of the consumers do not study privacy policies (Aqcuisti, et al., 2015), so it is hard to estimate their effect on the trust toward game companies or marketers.

6.2 Managerial implications

As advertising is a significant part of mobile game companies' revenue and embedded in the game and its economy, it is important to study how players perceive advertising. Big portion of players will never spend money in mobile games, leaving a lot of players unmonetized. Advertising offers a great way for players to earn in-game bonuses by watching short ads and game companies to earn from this huge segment of players. Players might also find other interesting games and services, to play and use along with the game.

As found in this study previous experiences have a great effect on how ads are seen. Another important factor found was the number of ads seen in games, as too many players might find too many ads irritating. Ad clutter might decrease the overall experience when playing games. So, with careful designing and testing advertising placements new possibilities to advertise in mobile games can be found, without causing too much headache to players. It is also important for players to feel that the reward received from watching ads is meaningful and that they can advance in the game with the help of advertising. As of now, players did not consider the ads to be too personal, but as stated earlier on some degree behavioural targeting ads would make them more successful. However, advertising related to personal healthcare and finances might be seen as breach of privacy.

When addressing the privacy concerns of players, it is important to make information about policies easily accessible. In case of Rovio, this has been achieved as all the major topics are discussed in their privacy and advertising policy. Erasure of data can be done easily, and players have the access to their data. King and other game companies should take this into consideration as a way to lessen their players privacy concerns. Also, it would be important that the privacy policies would be written with understandable language to make easier to read, and maybe have more players read the policies. As mentioned, players believe that privacy laws protect consumers, it would be important to mention all the key points in privacy policies, as Rovio has mentioned.

Players found it very important that their data is used as they have agreed. Women were found to be more trusting towards marketers and game companies. This might be something to take into consideration, as by getting more women into playing games would increase the overall trust towards privacy. Rovio also have very dedicated players among their players, as most of

them play almost every day of the week and play only one or two games other games than what they were currently playing.

6.3 Evaluation of the research

The purpose of this research is to give as accurate and reliable information as possible. This is most often described with terms reliability and validity. Reliability refers to the reproducing of the same results, if the study would be done with the same scale by a different researcher (Metsämuuronen, 2011). If the scale is reliable, the results would be the same time after time. In this study this was considered as all the phases of the study were described and explained in their sections. Inner reliability was studied using by Composite Reliability value, which ranged between 0.811 and 0.961, and was on an acceptable level (Karjaluoto, 2016). Thus, reliability for this study should be on a good level.

Validity measures accuracy, meaning that does the research measure right things. Validity can be viewed as internal and external validity. External validity refers to whether the results of the study can be generalized. Internal validity can be divided into content, construct and criterion validity. Content validity studies if the used scale, terms and concepts are consistent with the theory and correctly operationalized, also if they cover the described phenomenon broadly enough. (Metsämuuronen, 2011.)

Validity was taken into consideration in this study as all the measures used were derived from research questions and hypotheses, drawn from theory. When analysing the survey data, some tests require the sample to be over 100 (Karjaluoto, 2007), which was the case for this study (N=152). Questionnaire was also tested with 14 people before launching it, to find any possible confusion or issues. Measuring instruments used in this study were also designed for this study based on previous studies and theories and were proven to be valid. When evaluating the validity of the measurement model Average Variance Extracted (AVE) test was conducted. The AVE values should be above 0.5 (Karjaluoto, 2016), and for this study the values ranged between 0.674 and 0.924, which are above the cut-off value thus confirming discrimiant validity.

When designing the questionnaire, it is important to note, that because Rovio terms of service state, that by playing games all players accept the terms and confirm to be over 13 of age or older, the age scale starts from 13 upwards (Rovio terms of service, accessed 6.4.2020). Nevertheless, it is possible that some respondent's might actually be under 13 of age.

6.4 Limitations of the study and suggestions for further research

Aim of this section is to discuss the limitations of the study and items which could be improved and thus improve the study. Further research topics are also

discussed in this section. One practical improvement would be an increase in the amount of responses. This study got 152 responses, which is a relatively small number. Also, the gender and age distribution are quite skewed, as most of the respondents were male and above 40 years of age. In the questionnaire the age scale started only from 13 up, as it is mentioned in Rovio's Terms of Service (Rovio terms of service, accessed 2.3.2020) that all players claim they are over 13 to play and to agree with the terms. However, some of the respondent's might in reality have been under the age of 13.

As all the instruments used in the questionnaire were originally in English, they were first translated to Finnish to make answering easier and more understandable to recipients. When translating the questionnaire, the aim was to retain the original meanings of the questions, but some small details might have changed a bit due to the translation. Also, some words in English do not translate directly to Finnish, so some of the original meanings of the instruments might have been lost.

The questionnaire was executed in mobile games Angry Birds 2 and Angry Birds Friends and those games receive new players every day. Due to this, the survey was shown only to players who had played more than three days, so they would be more aware of how the game mechanics, economy and advertising works. But still playing only more than three days might not be long enough time for players to get familiar with the game. But as this study is more than of general nature, rather than studying behaviour specifically in these games, this might not be a big down side.

The study was conducted only in Finland, which is under the GDPR regulation as a European Union member country. This excludes results from other member countries, where the results might be different as each member state also has their own set of privacy laws and the trust to institutions might be different. The questionnaire was answered with mobile device, most likely with a mobile phone or a tablet. As a phone screen is pretty small, this might have caused some participants to drop out in the middle of filling the questionnaire.

Mobile games are growing bigger and bigger and gaining more audience every year. This leads to huge amounts of data available for developers and advertisers. It would be interesting to study, if the results would be similar in other member countries of the EU, as in this research. Overall, the research around GDPR's role in consumers' privacy perception is quite limited, as the law was introduced only a few years ago. A similar study to this could also be done in the United States, where California was the first state to introduce new privacy laws. In California, the California Consumer Privacy Act, CCPA, has been effective since beginning the of January 2020. The act makes it harder for companies to sell their consumers data forward (State of California Department of Justice, accessed 25.3.2020).

The CCPA has many similarities with GDPR in Europe, but one of the main differences is that the consumers have the right to know to whom their data is sold and forbid the sale of personal data (State of California Department of Justice, accessed 25.3.2020). It would important to study whether the results would be similar in the United States as well, or if the players perceive privacy differently there. The current direction of privacy regulation is going to

direction of consumers gaining more power over their own data, and this offers new challenges to marketers and personalized advertising.

REFERENCES

Acquisti, A., Brandimarte, L., Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science, 347(6221), 509-514.

Android Security Center, https://www.android.com/security-center/, accessed 25.1.2019

Bauer, H.H., Reichardt, T., Barnes, S.J., Neumann, M.M., 2005. Driving consumer acceptance of mobile marketing: A theoretical framework and empirical study. *Journal of electronic commerce research*, *6*(3).

Baek, T.H., Morimoto, M., 2012. Stay away from me. *Journal of advertising*, *41*(1), 59-76.

Beatrix Cleff, E., 2007. Privacy issues in mobile advertising. *International Review of Law Computers and Technology*, *21*(3), 225-236.

Bell, E., Bryman, A., Harley, B., 2018. *Business research methods*. Oxford university press.

Cho, C.H., 2004. Why do people avoid advertising on the internet?. *Journal of advertising*, *33*(4), 89-97.

Corcoran, P. M., Costache, C. (2018, August). A Privacy Framework for Games & Interactive Media. In 2018 IEEE Games, Entertainment, Media Conference (GEM) (pp. 1-9). IEEE.

Cuthbertson, Google admits giving hundreds of firms access to your gmail inbox, Independent, 21.9.2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-gmail-data-sharing-email-inbox-privacy-scandal-a8548941.html, accessed 25.1.2019

Dogtiev, App revenues (2017), BusinessofApps 11.5.2018, http://www.businessofapps.com/data/app-revenues/ accessed 22.3.2019

Dogtiev, Mobile App Advertising Rates (2018), BusinessofApps 18.1.2019, http://www.businessofapps.com/ads/research/mobile-app-advertising-cpm-rates/#1, accessed 22.3.2019

European Federal Trade Comission, accessed 15.2.2019 https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Feijoo, C., Gómez-Barroso, J.L., Aguado, J.M., Ramos, S., 2012. Mobile gaming: Industry challenges and policy implications. *Telecommunications Policy*, *36*(3), 212-221.

Flynn, L.R., Goldsmith, R.E., 1999. A short, reliable measure of subjective knowledge. Journal of business research, 46(1), 57-66.

General Data Protection Regulation, GDPR https://gdpr-info.eu, accessed 18.2.2020

Granville, Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, The New York Times, 19.3.2018 https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html accessed 25.1.2019

Ha, I., Yoon, Y., Choi, M., 2007. Determinants of adoption of mobile games under mobile broadband wireless access environment. *Information & management*, *44*(3), 276-286.

Haghirian, P., Madlberger, M., 2005. Consumer attitude toward advertising via mobile devices-An empirical investigation among Austrian users. ECIS 2005 Proceedings

Hirsjärvi, S., Remes, P., Sajavaara, P. 2009. Tutki ja kirjoita. (15. uudistettu painos) Helsinki: Tammi.

Karjaluoto, H. 2007. SPSS opas markkinatutkijoille. Jyväskylä: Jyväskylän yliopisto. Working paper / University of Jyväskylä, School of Business and Economics.

Karjaluoto, H., Munnukka, J. 2016. AMOS (SPSS)-ohjelman käyttöohje (versio SPSS AMOS 22.0). Working paper/Jyväskylä University. School of Business and Economics 382.

King.com, https://king.com, accessed 2.3.2020

King.com Privacy policy, https://king.com/privacyPolicy#section11, accessed 2.3.2020

Krafft, M., Arden, C.M., Verhoef, P.C., 2017. Permission marketing and privacy concerns—Why do customers (not) grant permissions?. *Journal of interactive marketing*, *39*, 39-54.

Klopfer, P.H., Rubenstein, D.I., 1977. The concept privacy and its biological basis. *Journal of social Issues*, *33*(3), 52-65.

Leontiadis, I., Efstratiou, C., Picone, M., Mascolo, C., 2012, February. Don't kill my ads!: balancing privacy in an ad-supported mobile application market. In Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications (p. 2). ACM.

Merisavo, M., Kajalo, S., Karjaluoto, H., Virtanen, V., Salmenkivi, S., Raulas, M., Leppäniemi, M., 2007. An empirical study of the drivers of consumer acceptance of mobile advertising. Journal of interactive advertising, 7(2), 41-50

Metsämuuronen, J. 2011. Tutkimuksen tekemisen perusteet ihmistieteissä: E-kirja opiskelijalaitos. Helsinki: International Methelp, Booky.fi.

Newman, J., Jerome, J., Hazard, C. (2014). Press Start to Track? / Privacy and the New Questions Posed by Modern Videogame Technology.

Privacy Europe, European Privacy Framework, https://www.privacy-europe.com/european-privacy-framework.html, accessed 3.3.2020

Robinson, In-Game Advertising Study 2017, DeltaDNA, 27.11.2917. https://deltadna.com/blog/game-advertising-study-2017-developers-now-see-ads-important-monetization-opportunity/, accessed 22.3.2019

Rovio About Us, https://www.rovio.com/about-us, accessed 18.3.2020

Rovio Investors, https://investors.rovio.com/en, accessed 18.3.2020

Rovio Privacy Policy, https://www.rovio.com/privacy, accessed 2.3.2020

Rovio Terms of service, https://www.rovio.com/terms-of-service, accessed 2.3.2020

Russell, N. C., Reidenberg, J. R., Moon, S. (2018). Privacy in Gaming

Salinas, Facebook says the number of users affected by Cambridge Analytica data leak is 87 million, 4.4.2018, https://www.cnbc.com/2018/04/04/facebook-updates-the-number-of-users-impacted-by-cambridge-analytica-leak-to-87-million-.html, accessed 25.1.2019

Seufert, How large is the mobile gaming advertising market?, Mobile Dev Demo, 25.2.2019, https://mobiledevmemo.com/how-large-is-the-mobile-gaming-advertising-market/, accessed 22.3.2019

Shankar, V., Balasubramanian, S., 2009. Mobile marketing: a synthesis and prognosis. *Journal of interactive marketing*, *23*(2), 118-129.

Sifa, R., Drachen, A., Bauckhage, C., 2018. Profiling in Games: Understanding Behavior from Telemetry. Social Interactions in Virtual Worlds: An Interdisciplinary Perspective.

Sifa, R., Hadiji, F., Runge, J., Drachen, A., Kersting, K., Bauckhage, C., 2015, September. Predicting purchase decisions in mobile free-to-play games. In *Eleventh Artificial Intelligence and Interactive Digital Entertainment Conference*.

Smit, E.G., Van Noort, G., Voorveld, H.A., 2014. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, pp.15-22.

Soh, J.O. and Tan, B.C., 2008. Mobile gaming. *Communications of the ACM*, *51*(3), 35.

Spiekermann, S., Cranor, L. F. (2008). Engineering privacy. *IEEE Transactions on software engineering*, *35*(1), 67-82.

State of California Department of Justice, California Consumer Privacy Act, https://oag.ca.gov/privacy/ccpa, accessed 25.3.2020

Swaid, S.I., Wigand, R.T., 2009. Measuring the quality of e-service Scale development and initial validation. Journal of Electronic Commerce Research, 10(1), 13-28.

Takashi, D., App Annie: Mobile game spending will top $100 billion in 2020, 15.1.2020. https://venturebeat.com/2020/01/15/app-annie-mobile-game-spending-is-expected-to-top-100-billion-in-2020/, accessed 10.9.2020

Terlutter, R., Capella, M.L., 2013. The gamification of advertising: analysis and research directions of in-game advertising, advergames, and advertising in social network games. *Journal of advertising*, *42*(2-3), 95-112.

Tucker, C. E. (2012). The economics of advertising and privacy. International journal of Industrial organization, 30(3), 326-329.

Tucker, C.E., 2014. Social networks, personalized advertising, and privacy controls. *Journal of marketing research*, *51*(5), 546-562.

Turner, J., Scheller-Wolf, A., Tayur, S., 2011. OR PRACTICE—Scheduling of Dynamic In-Game Advertising. *Operations research*, *59*(1), 1-16.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., Hennessy, M. (2009). Americans reject tailored advertising and three activities that enable it

Wagner, Here's how Facebook allowed Cambridge Analytica to get data for 50 million users, 17.3.2018 https://www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data, accessed 26.8.2018

Westin, A.F., 1968. Privacy and freedom. *Washington and Lee Law Review*, *25*(1)

Wijman, Mobile Revenues Account for More Than 50% of the Global Games Market as It Reaches $137.9 Billion in 2018, 30.4.2018, https://newzoo.com/insights/articles/global-games-market-reaches-137-9-billion-in-2018-mobile-games-take-half/, accessed 22.3.2019

Xu, H., Teo, H.H., Tan, B.C., Agarwal, R., 2009. The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of management information systems*, *26*(3), pp.135-174.

Yritys- ja yhteisötietojärjestelmä, YTJ, https://tietopalvelu.ytj.fi/yritystiedot.aspx?yavain=1831717&tarkiste=D7991B326865E861B5526406845003604500 8A1B, accessed 18.3.2020

Zang, J., Dummit, K., Graves, J., Lisker, P., Sweeney, L. (2015). Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. *Technology Science*, *30*.

APPENDIX 1

LIST OF SURVEY ITEMS IN ENGLISH

Experiences / preferences

EXP1: My experience with watching advertising has been good
EXP2: With the help of advertising I can advance in the game
EXP3: I gain some benefit by watching advertising

Targeted and personalized ads

PER1: The game gives me personally interesting advertising
PER2: The game shows me ads that fit my needs
PER3: The ads enable me to find other products or games that meet my needs

Control of data

CON1: I would only be prepared to receive targeted advertising in mobile games if I had provided my permission.
CON2: It is important for me that I can control the permission to receive targeted advertising in mobile games.
CON3: It is important to me that I can refuse to receive targeted advertising.

Number of ads

NUM1: The amount of advertising in mobile games is excessive
NUM2: The amount of advertising in mobile games is irritating

Collected data

DAT1: I believe that game companies use my data only for a purpose that I have approved
DAT2: I believe that marketers would use my data only for a purpose that I have approved
DAT3: I believe that the consumer is protected by laws related to data privacy

Knowledge of the GDPR

GDP1: I know pretty much about GDPR (General Data Protection Regulation)
GDP2: I can judge the effects of GDPR to companies' data collection

Watching ads

WAT1: I feel positively about advertising in mobile games
WAT2: I am willing to receive advertising in mobile games in the future
WAT3: I would see advertising messages I receive in mobile games in the future

Advertising avoidance

AVO1: I avoid advertising in mobile games
AVO2: It would be better, if mobile games didn't have advertising
AVO3: I do not click or watch ads in mobile games

Demographic and background factors

Gender
Female
Male
Other

Age
13-19 years
20-25 years
26-30 years
31-40 years
41-50 years
50+ years

Days played in a week
One day or less
2-3 days
4-5 days
6-7 days

Other mobile games played
I don't play other games
1-2 games
3-4 games
5-6 games
7+ games

APPENDIX 2

LIST OF SURVEY ITEMS IN FINNISH

Aiemmat kokemukset / mieltymykset

EXP1: Kokemukseni mainosten katsomisesta on ollut hyvä.
EXP2: Pääsen pelissä eteenpäin mainoksien avulla.
EXP3: Saan mainosten katsomisesta jotain hyötyä.

Kohdennetut mainokset

PER1: Peli tarjoaa minulle henkilökohtaisesti kiinnostavia mainoksia.
PER2: Pelissä esiintyvät mainokset sopivat tarpeisiini.
PER3: Pelin mainosten avulla löydän muita tarpeitani vastaavia tuotteita ja pelejä

Datakontrolli

CON1: Haluaisin saada kohdennettuja mainoksia peleissä vain, jos olen antanut sille suostumuksen.
CON2: Minulle on tärkeää, että voin kontrolloida suostumustani kohdennettujen mainosten saamiseen.
CON3: Minulle on tärkeää, että voin kieltäytyä kohdennetusta mainonnasta.

Mainosten määrä

NUM1**:** Mobiilipeleissä on liikaa mainoksia.
NUM2**:** Mainoksien määrä ärsyttää minua.

Kerätty data

DAT1: Uskon, että peliyhtiöt käyttävät dataani vain siihen tarkoitukseen, minkä olen hyväksynyt
DAT2: Uskon, että mainostajat käyttävät dataani vain siihen tarkoitukseen, minkä olen hyväksynyt
DAT3: Uskon, että yksityisyyteen liittyvät lait suojelevat kuluttajia

Tietämys GDPR:stä

GDP1: Tiedän GDPR:stä (General Data Protection Regulation) melko paljon.
GDP2: Osaan arvioida GDPR:n vaikutuksia yritysten datan keruuseen

Mainosten katsominen

WAT1: Pidän mobiilipeleissä olevia mainoksia positiivisena asiana.
WAT2: Haluaisin jatkossakin saada mainoksia mobiilipeleissä.
WAT3: Aion tulevaisuudessa katsoa mainoksia mobiilipeleissä

Mainosten vältteleminen

AVO1: Välttelen mobiilipeleissä olevia mainoksia
AVO2: Mielestäni olisi parempi, jos mobiilipeleissä ei olisi mainoksia
AVO3: En klikkaa tai katso mainoksia mobiilipeleissä

Demografia- ja taustamuuttujat

Sukupuoli

Nainen
Mies
Muu

Ikä

13-19 vuotta
20-25 vuotta
26-30 vuotta
31-40 vuotta
41-50 vuotta
50+ vuotta

Monenako päivänä viikossa pelaa

Yhtenä päivänä tai vähemmän
2-3 päivänä
4-5 päivänä
6-7 päivänä

Muiden pelattujen pelien määrä

En pelaa muita mobiilipelejä
3-4 peliä
5-6 peliä
7+ peliä