Digital Marketing: Privacy Concerns of Consumers

Aysun Yesim Özköse

Haaga-Helia University of Applied Sciences

Bachelor's Thesis

2022

Bachelor of Business Administration

Abstract

Author(s)
Aysun Yesim Özköse

Degree
Bachelor of Business Administration

Report/thesis title
Online Marketing: Privacy Concerns of Consumers

Number of pages and appendix pages
24 + 1

This thesis is a research-oriented report and aims to identify privacy concerns of consumers in online marketing as its main research objective. Furthermore, it analyzes consumer views towards personalized advertisments and consumers' awareness of tools available to protect their privacy online as its sub-objectives.

Businesses in today's modern, technologically advanced world, collect huge amounts of data from consumers online to create and implement their marketing strategies. With data collection being conducted, companies have the responsiblilty to protect consumer's privacy and compile with laws and regulations. This does not come without consumer's concerns regarding their online privacy.

A theoretical framework is established as a basis of the research topic. The contents of which include online marketing, with specific regards to data collection and personalization, online privacy, specifically consumer privacy concerns and the privacy paradox and laws and regulations that help consumers protect their data online. In detail discussed are the European Union's General Data Protecton Act and specific tools available to consumers to protect their online privacy. In order to establish the theoretical framework, books and websites were as sources.

The research in the thesis is done with qualitative research methods, mainly personal interviewes with three chosen individuals from various age groups and gender representations to represent a wide range of European society. The research results are analysed, summarized and answer the research objectives.

Lastly, this thesis concludes with further research suggestions into the impact of the European Union's General Data Protection Regulation on its consumers and the implications for marketers the ever growing consumer privacy concerns will have. Furthermore the author evaulates the thesis process and their own development during it.

Keywords
Online Marketing, Data Privacy, Personalization, GDPR, Consumer

Table of contents

1 Introduction

Businesses are increasingly collecting and using data about current and potential customers to improve the effectiveness of their customer relationship management, sales, and service. By receiving information about their customers' transactions and behavior, as well as their socio-demographic profile, businesses can better understand their customers' preferences and desires. This enables them to build customer intelligence to improve strategic marketing decisions and improve customer relationships. (Kumar & Reinartz 2018, 279.) However, while companies have been increasingly collecting data on their customers, said customers have grown to become more reluctant with disclosing their personal information or allowing the tracking of their online behavior due to privacy concerns. Additionally, increasing legal restrictions on the collection and use of personal data are creating new obstacles for businesses (Kumar & Reinartz 2018, 279).

As consumers spend more time online, whether to play, work, shop or conduct business, privacy has become a major issue. What kind of data is collected online? Who oversees its collection? Who should be held accountable for safeguarding personal information? And how do we protect our privacy online?

1.1 Research objectives and questions

The main research objective is to identify the drivers of privacy concerns of consumers in the context of digital marketing and their respective implications for companies. Furthermore, consumers' views towards personalized advertisements in digital marketing will be analyzed as well as their awareness of privacy protection tools. This thesis is research-oriented with qualitative methods to understand concepts, thoughts, and experiences to gather in-depth insight by both conducting interviews and analysing precollected document data, such as the General Data Protection Regulation of the European Union.

1.2 Scope and delimitations

The following thesis aims to describe, understand, and interpret the phenomenon of growing customer privacy concerns in terms of online marketing and the implications it has on companies' digital marketing strategies. The focus will be on customers of the European Union, namely three selected persons representing various age groups and gender representation. While online marketing happens throughout the entire Internet, only the market of the European Union will be considered for this research.

The interviews conducted are structured by having all interviewees answer the same questions, although independently from each other. In the thesis it will be explained in detail how said interviews were planned and carried out.

1.3 Key concepts

Online Marketing is defined as applying the Internet and related digital technologies to achieve marketing goals. In practice, online marketing involves managing an online business presence in many forms, including the company's website and social media pages of the company related to online communication technology, including search engine marketing, social media marketing, online advertising, email marketing, and partnership agreements with other websites. These techniques are used to support the goals of attracting new customers and providing existing customers with services that help build customer relationships.

Data Privacy or information privacy, is the area of data protection that specifically concerns the proper handling of sensitive data, including not only personal data but also other sensitive data such as certain financial data and intellectual property data. (Storage Networking Industry Association 2022.)

Personalization is the process by which companies tailor experiences and communications based on information they learn about individuals. (Salesforce Inc. 2022.)

The General Data Protection Regulation (GDPR) is a legal framework that sets out guidelines for the collection and processing of personal data from individuals residing inside and outside the European Union (EU). (Proton AG 2022.)

A *consumer* is a person who purchases goods and services for their personal usage.

2 Theoretical framework

2.1 Online marketing

Before we can define online marketing, we must differentiate between digital and online marketing. Digital marketing means applying the Internet and related digital technologies in combination with traditional communication to achieve marketing goals. While that is a simple definition of an incredibly wide range topic, this thesis will be focusing on the sphere of online marketing, which is a subset of digital marketing.

Furthermore, there is a distinction to be made between direct and general marketing. Direct marketing is a marketing technique based on individual customer records stored in a database. These records form the basis for marketing analysis, planning, program execution and management of all these activities. Contrary to this, general marketing revolves around creating a brand for each product and gaining market share for that product. (Tapp, Whitten & Housden 2014, 4.) Online marketing is therefore a subset of digital marketing and direct marketing, for the most part.

2.1.1 Data collection

To tailor their marketing efforts towards their current and potential customers, companies need to have access to a wide range of data. This is often done by using a database that holds customer information, which is the used to help create marketing strategies (Tapp & al. 2014, 7). A marketing database can simply be defined by the following quote: “A marketing database is a list of customers’ and prospects’ records that enables strategic analysis, and individual selections for communication and customer service support. The data is organised around the customer” (Tapp & al. 2014, 34).

The following four types of data are what marketing departments of a company would want to store in their database:

- Primary data, such as names and addresses of customers, details of products and/or services your organisation offers, pricing details, campaign details and definitions of various channels of distribution
- Secondary data, which is data used to qualify primary data, such as demographics, lifestyle information, geographical profiles, or levels of penetration into markets
- Performance data to record how your customers have responded, what they bought, how much they spent, and to which campaigns they responded
- External data, covering everything rented or bought in lists to data from various agencies that can enhance your base data

(Tapp & al. 2014, 34.)

Specifically in online marketing, data collection is done by the following means.

The most straight forward way of collecting your data online is done by companies simply asking for it. When someone subscribes to a service, registers on a website, or make first time purchase online, they are usually required to fill out a form. In this form, the company requests at least their name and email address, but other demographic information is also collected. Then companies can later conduct customer surveys to ask direct questions commonly used to build customer profiles. As well as directly asking customers for their information, companies also have the technology online to pull customer data from a large number of online sources. Of course, the most obvious place is their own website, most of which are now equipped with cookies and web beacons. These technologies allow a company to track a visitor's browsing history even if the visitor leaves the company's website and moves around the internet. The cookies allow businesses to know where their customers are, what they browse, and where they go after visiting their website, so they can then retarget their customers with their ads. This is the reason why after looking at specific products on one website, consumers will find ads on the same product or product category on different platforms.
Social media is also an important data source. This is especially true, for example, if a customer uses their Facebook account to log into a third-party application provided by a company (such as Spotify). That said, the data that costumers share publicly on social media is accessible to anyone online.
Email tracking is another method. This allows businesses to know not only when a recipient has opened an email, but where and on what device. Similarly, apps embedded in third-party “trackers” are also sources of customer data. Some of this data is analyzed to better understand how the app is used, but much of it is also used for targeted advertising, behavioral analysis, and location tracking. According to research by Exodus Privacy and Yale Privacy Lab, more than three out of four of his Android apps contain at least one third-party his tracker.

With customer data, businesses can improve customer experiences, improve marketing strategies, drive targeted advertising, and (if enough is collected) generate new revenue streams by selling data to data companies. Of course, there are data protection regulations such as the EU General Data Protection Regulation (GDPR) that all companies that start collecting customer data must comply with. But for organizations that want to use customer data for business purposes, it all starts with collection. But collecting is just the beginning. The real challenge is to analyze everything and turn the gained insights into valuable marketing strategies and efforts.

Collecting customer data has become a key priority for businesses. As more sophisticated technologies are developed to collect and analyze customer data, organizations will be better able to contextualize it, extract insights from it, and monetize it. In the era of always-

on connectivity, smartphones, wearables, and the Internet of Things (IoT), customer data is collected 24/7. Computers can identify your voice through a microphone, recognize your face through the eyes of a camera, record your biometric details through portable devices, track your internet browsing history through cookie technology, locate your exact location with GPS tracking. And with all that data, computers can create a more accurate profile of a company's customers, predicting what they think, what they like, and most importantly, what they spend their money on. (William Goddard 2019.).

2.1.2 Personalisation

After companies have collected consumer's data throughout their online activities, they can then take the next step in using said data to personalize their marketing efforts towards the individual consumer, which is increasingly becoming a customer's expectation of marketing.

There are two key methods of personalization: user-defined and behavioral personalization. Simply put user-defined personalization means letting the consumer tell you what they want, while behavioral personalization means learning from the consumer what they want. (Kingsnorth 2016, 204.)

User-defined personalization requires that individuals are willing to provide data to allow marketers to tailor communications to them. This includes demographics, interests, routines, etc. which can be collected through any channel, such as an online form. This method of personalization comes with its own challenges. If a consumer does not want to provide their information to the marketer, their entire personalization model falls apart. This will result in some customers receiving personalized and some generic communications, which then may require a company to run two separate communication programs. Furthermore, this realization will have to be included into every marketing decision, which can lead to mistakes due to its complex nature. Additionally, user-defined personalization relies on the data being accurate. Not every user will always provide their real data, but fake ones – data such as birth dates, interests, gender, etc. could be false which can lead to embarrassing and brand damaging consequences if companies send for example an old man a voucher for a teenage clothing. Lastly, this personalization model assumes that consumers know themselves. Not always do people know what they really like, and memory is not always reliable, meaning, a consumer might give a genuine answer, but it might not be correct.
Summarized it can be said that while user-defined personalization comes with strong advantages, marketers will need to be completely sure of the reliability and accuracy of their received data.

As mentioned, behavioral personalization is the area of personalization where marketers can learn from their customer's behavior with the power of big data. Data is one of the greatest assets a business can have, and the sheer amount of data that can be gathered from web analytics, buying funnels, research, finance, and many other areas opens up an incredible number of possibilities for marketers.
Behavioral personalization obtains cues about a person's behavior from signals received through various data collection points, such as: visiting websites, opening emails, and interact with certain online content. This data can be fed into models that make real-time decisions. Behavioral personalization creates the opportunity for companies to tailor their marketing information so that the consumer only receives what is relevant to them. Things like spam emails will not bother the consumer anymore and marketing effectiveness will soar for businesses.
Just like with the user-defined personalization model, this one comes with its own challenges, too. As well as with the previous model, using the gathered data on consumer behavior correctly is key. The interpret behavioral data, marketers will need to draw certain assumptions and conclusions, which will then have to be the correct ones. Otherwise, the high-quality data gathered can become useless fast. Therefore, the made assumptions must be made in a very careful manner. Lastly, data privacy is an ever-relevant challenge in this area of personalization. Consumers are becoming more apprehensive about disclosing their data, and regulations continue to limit businesses' ability to obtain and use that data.

It's important to know that these methods of personalization aren't mutually exclusive. Both models have their time and place and it's up to the company which to use when and where. It's with the possibilities of modern technology that helps companies go far beyond simple personalization models and segmentation. (Kingsnorth 2016, 204-209.)

2.2 Online privacy

Internet privacy, also referred to as online privacy, refers to the right to personal privacy in relation to the reuse, storage, provision to third parties, and display of user information on the Internet. It also covers the privacy and security level of Personal Destiny posted on the Internet and is a broad term that refers to a range of techniques, factors and technologies used to protect personal and sensitive data, preferences, and communications.

As e-commerce continues to grow and gain popularity online, internet privacy has become extremely important for business owners and managed IT service providers. Businesses and users continue to be concerned about threats and privacy breaches as the risk of information ending up in the hands of cybercriminals is greater than ever.

Online privacy is a major concern for Internet users who plan to visit social networks, shop online or participate in online games because they want to protect their privacy. A victim's identity can be stolen or used fraudulently by cyber criminals who simply compromise the victim's password. (Dynamix Solutions Inc. 2017.)

2.2.1 Customer privacy concerns

Customer privacy concerns have increasingly grown over the last decade which can be attributed to a variety of internal company factors as well as external ones (Kumar & Reinartz 2018, 280).

Internal drivers of customer privacy concerns can be defined as the following: Collection, Control, Awareness, Errors, Improper Access, and Unauthorized Secondary Use (Kumar & Reinartz 2018, 280).
Collection refers to the way companies collect consumer's information. It can be defined as the extent to which an individual is concerned about the amount of personal-specific data held by others in relation to the value of benefits received. Collection summarizes consumer concerns about the amount and the way in which their private data is collected by companies.
Control of consumer's information is done by the consumer approving of the collection of their personal data, the modification of it and the right to opt-in or opt-out of the collection.
Awareness refers to the communication from companies of their data collection to the consumer. Is the consumer aware of a company collecting their personal information and are they aware to what extent this is being done?
Consumers' privacy concerns can additionally be driven by the fear that information is not correct, referring to the established category of *Errors* and *Improper Access*, the fear that information is accessible to parties that the consumer didn't consent to. Lastly, consumer concerns also stem from the worry that their personal data will be used in a way they didn't agree to – referred to as *Unauthorized Secondary Use.* (Kumar & Reinartz 2018, 281-282.)

In addition to these internal factors that can drive consumer privacy concerns there are several external drivers as well. The Internet, technological advances, public media coverage and governmental regulations, which all influence each other, foster fears and concerns in consumers. (Kumar & Reinartz 2018, 283.)

Customer privacy has always been an important issue in marketing, but it has become even more important with the advent of the Internet. The online environment also presents new and different conditions for organizations in their data collection and data processing

efforts. Businesses can develop customer profiles, behavioral profiles, and insights to target and differentiate their customers. In the online environment, there are several methods of collecting customer information. As such, a trade-off between the benefits of providing personal information (name, address, credit card number, etc.) versus the fear of threats associated with sharing such sensitive information is faced. It has even been argued that it is nearly impossible for customers to conduct online transactions without disclosing information about themselves. But what makes customer privacy even more of a concern is the approach companies are taking. One example is the use of behavioral advertising. This is a personalized advertising message based on the customer's previous surfing behavior and online purchasing patterns. But the rise of his social media sites online, including Facebook and Twitter, means that customers are voluntarily sharing personal information, giving advertisers detailed insights that can be used for customer segmentation and targeting. Additionally, there may be privacy concerns related to the potential exposure of sensitive customer information. In summary, the Internet often threatens privacy and can undermine a company's marketing performance in the long run. (Kumar & Reinartz 2018, 283-284).
With online privacy concerns, the ever-growing advancement of technology cannot be ignored. Various technological innovations have made it easier for businesses to collect, process and use customer data to gain a competitive advantage, but they have also raised concerns about customer privacy. The main innovations being mobile and smart phones as well as location-based services. Location-based services for example give companies the chance to tailor their online marketing to the consumer based on their location. (Kumar & Reinartz 2018, 284-285). These tailored advertisements can give consumers the feeling of “always being watched”, losing control over their personal information.

Furthermore, over the past decade public media has increased its coverage of privacy issues in both online and print media which shaped the concerns of consumers. The media coverage plays an important role in shaping perception of the public and can ultimately lead to increased privacy concerns among consumers. Especially social media platforms like Facebook and Twitter can help spread privacy issue news worldwide and in no time. Lastly, governmental regulations, or the lack of them, also have a powerful impact in shaping consumer privacy concerns. (Kumar & Reinartz 2018, 286).

Customer privacy concerns can in summary arise from various internal and external drivers and it’s up to online marketers to respond to said fears in order not to lose their consumers’ trust and willingness to purchase their goods and services.

2.2.2 Privacy paradox

The privacy paradox is a phenomenon describing the relationship between consumer's intention to disclose personal information and their actual personal information disclosure behavior. This phenomenon is based on experiments, research, or general behavioral observations. Before it received its name, early studies revealed that there is an inconsistency between the privacy concerns consumers have disclosed and their actual behavior. In 2007 an article called *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors* gave the phenomenon its name. Many studies have been conducted on the privacy paradox which reach different findings. One the one hand it has been concluded that people fail to take easy privacy protection measures, despite expressing privacy concerns. On the other hand, it has been found that people will share their personal data with third parties for incentives like small amounts of money even though they have expressed that they value their privacy highly. (Solove 2020, 5.)

Professor Daniel Solove of George Washington University Law School argues that the privacy paradox can be divided into two arguments: The behavior valuation and the behavior distortion argument. According to Professor Solove the behavior valuation argument states that consumer's behavior is a more accurate measurement of how they value their privacy than their expressed attitudes towards it. Meaning, the behavior valuation argument proposes that consumer's revealed preferences are a better indication of their views towards their privacy than their stated preferences. This argument claims that the privacy paradox demonstrates that consumers do not highly value their privacy and easily trade it away for goods and services. Therefore, privacy regulations should focus on consumer's behavior instead of their stated preferences because consumers revealed that they aren't as concerned about their privacy as they say they are.

The contrary argument Professor Solove proposes is the behavior distortion argument. This argument claims that consumer's behavior does not necessarily reflect their actual preferences towards their privacy. Consumer's behavior is distorted by several influences such as biases and heuristics, framing effects and behavioral manipulation and skewing. Biases and heuristics, so Solove, mean that consumers experience a certain degree of difficulty figuring out what to din in complex situations that involve cost, benefits, and risk. This also comes with the fact that consumers favor instant gratification, giving up their personal data without considering the long-term consequences and costs this can mean. Framing effects refer to the timing when privacy notices are presented which, according to Solove, significantly affect consumer's decisions to disclose their personal data. Things like the wording, the information they're given, and the range of choices are drivers for

consumer's data privacy decisions. Behavioral manipulation refers to the fact that consumer's behavior is being manipulated by businesses and skewed by technological design. But consumers aren't only manipulated directly but sometimes also by their environment. For example, consumers today expose their personal information on social media openly and freely because the Internet makes it easy to do so. People say things online that they normally wouldn't do so when faced with other people in real life.
At the end, Whether the design is intentionally created to manipulate consumers or unintentionally distorts their behavior, it leads to the same result. People share data in ways they might not otherwise share.
Lastly, Professor Solove points to the fact that consumers generally have inertia when it concerns the steps to be taken to protect their online privacy. Privacy notices are hardly read, and default privacy settings are rarely changed.

According to Professor Solove, the privacy paradox does not exist because privacy is not an all-or-nothing concept – it is about boundaries and controlling data flow. The author of the thesis agrees with Professor Solove; concepts and phenomenon are never a black and white issue but complex and need to be looked at from different angles and perspectives. Therefore, fact that consumers share their data does not mean they do not care about their privacy.
Additionally, it is to be mentioned, that privacy has many dimensions. Privacy laws and regulations make sure that even when consumers provide their personal information, organizations must keep that data secure. Thus, when consumers share their data, they aren't giving up all their privacy. They are allowing companies to use their data in certain ways but retain their various rights to their privacy of said data. By sharing data, consumers aren't sacrificing all their privacy but rather increasing privacy risks to certain extents. (Solove 2020, 8-24.)

2.3 Laws and regulations

Data protection standards are increasingly high, and companies are faced with the increasingly complex task of verifying the legal compliance of their data processing, especially in an international context. By its very nature, data can easily cross borders and plays a key role in the global digital economy. Data has become a precious commodity in recent years and is even called the currency of the future. The processing of personal data takes place in various spheres of economic and social activity, and advances in information technology greatly facilitate the processing and sharing of such data. In this context, the European Union has adopted the General Data Protection Regulation to further harmonize data protection rules within EU Member States and to raise the level of data

protection for persons concerned. Due to its wide cross-border reach, it will also affect many companies based outside the EU. (Voigt & von dem Bussche 2017, 1).

2.3.1 GDPR

The GDPR was adopted in 2016 to replace the 1995 Data Protection Directive. It is the result of a gruelling negotiation process that involved numerous changes to the legal text, which lasted 4 years before the adoption of the final regulation. The fragmentation of data protection in EU Member States and the resulting legal uncertainty have been seen as an obstacle to the conduct of economic activities at the EU level and as a distortion of competition. Unlike the Data Protection Directive, this regulation applies directly to recipients, without further enforcement measures imposed by EU member states. By coordinating data protection rules, the GDPR increases legal certainty and removes potential barriers to the free flow of personal data. The EU aimed to restore people's trust in the responsible processing of their personal data to revitalize the digital economy in the EU internal market. This required companies not only to strengthen their existing obligations under the GDPR, but also to meet the new data protection obligations. Considering the challenges of the global economy, new technologies and new business models, legislators have created a very broad field that affects many businesses. As data protection obligations as well as future fines increased significantly, companies had to carefully restructure their internal data protection procedures to comply with the GDPR. (Voigt & von dem Bussche 2017, 2).

After billions of people entrusted their personal information to online companies, their personal information was compromised and misused. The GDPR is the most ambitious regulatory effort yet to be implemented. Businesses have quietly harvested data for profit and influence. The Facebook Cambridge Analytica scandal is just one of the high-profile episodes that have unfolded over the years. Uber, Google, Apple, and other companies big and small are systematically violating the privacy of millions of people. Data protection has failed miserably, even though businesses are fair and transparent in their data management. Almost every large enterprise has had to deal with data breaches. Massive breaches make headlines, but small businesses are a favorite target for cybercriminals because of their weak defences.
Through the GDPR, the EU aims to restore some of the same basic security and privacy safeguards from the physical world to the digital world, such as door locks and liability for negligence. Online organizations that fail to protect the personal data of EU individuals can face fines of up to 20 million euro or 4% of global revenue, whichever is greater. The GDPR gives certain rights to technology users, including the right to control and access

data and request data deletion. Organizations must now use security tools such as encryption to minimize harm to users in the event of a data breach. Overall, the GDPR establishes a new way of thinking about personal data. Personal data belongs to people, not companies. The law gives millions of internet users in the EU more powers than ever to protect themselves. In the following, some of the most important ways will be listed.

End-to-end encryption: Ad-based companies like Google and Facebook don't need to read documents, searches, and emails, but they do anyway because it's part of their business model. With GDPR and clear references to encryption, many companies are adopting end-to-end and zero-access encryption technologies. These security tools ensure that no one other than the consumer, the data owner, can access their data.

Consent: The GDPR guarantees that companies will only be able to send consumers marketing emails or collect their personal information if the consumer explicitly agrees. Children under 13 cannot give consent without parental consent.

Accountability: The GDPR legislates that companies that fail to ensure their consumer's data privacy will be fined up to 20 million euro; one of the many reasons the GDPR is the harshest data privacy regulation in the world.

The core rights of consumers in the GDPR are summarized in the following list:

- The right to be informed how personal data are used
- The right of access to personal data organizations are holding
- The right to correct personal data that's inaccurate or incomplete
- The right to request the deletion of personal data under certain circumstances
- The right to restrict or pause the processing of data if there are irregularities
- The right to have an organization send personal data it holds to other companies
- The right to object to data processing
- The right to protection from harmful automated decision-making processes

(Proton AG 2022.)

2.3.2 Online privacy protection tools

As consumers use the internet in their daily lives, they're often asked to disclose their personal information that uniquely identifies them. This includes information on name, address, phone number, birth date, credit card and bank account numbers as well as their age, religious faith, marital status, and shopping history. All this information can and is being then combined by marketers to develop profiles on consumers. Websites often will also collect consumer information in the background with things like Internet cookies and mobile phone hardware identifiers (for example device IDs).

Sharing personal data with companies comes with many benefits, but if consumers aren't careful about what information they provide to which companies, unexpected or undesirable consequences, like unwanted marketing and intrusive advertising can follow.

To protect their online privacy and limit the information they share, consumers have a variety of tools available to them.

Firstly, consumers can make sure they know their options when using web browsers or signing up for online stores. The options, such as the privacy settings of browsers and websites, often allow the limitation of certain types of tracking cookies or the opportunity to opt-out of marketing emails after signing up in an online store. Not accepting default settings unless they represent the privacy level consumers desire is important.

Additionally, the usage of strong and secure passwords is an important tool to protect consumer privacy and information security online. Password managers can help to create such strong and secure passwords and can easily store them together in one place.
Next to strong and secure passwords, the usage of two factor authentication is recommended. Often, services such as online banks and social networking sites will offer their customers an opportunity to not only login with a password but with a code that is sent to their phone number or email to ensure only the consumer has access to their personal data.

In addition to only sharing personal information with companies and websites consumers trust, consumers should further only share their data with secure sites. Websites that start their web address with https (instead of http) can be recognized as secure and safe. (Maryland Attorney General's Office. 2022.)

The most known security measure amongst consumers is the usage of a VPN. VPN stands for Virtual Private Network and is a service that protects consumer internet connection and online privacy by redirecting the network through a specifically configured remote server managed by the VPN host. This means that when a VPN is used to browse online, the VPN server becomes the data source. Internet Service Providers (ISPs) and other third parties cannot see the websites consumers visit or the data they send or receive online. A VPN acts as a filter that turns all data into encrypted data. Meaning, even if someone has access to the data, it's useless because they can't read it. (AO Kaspersky Lab 2022.)

3 Research

3.1 Research methods

This chapter will introduce the research objectives of the thesis and the methodology used to answer the research objectives. It will furthermore describe the background and rationale for the methodology, explaining why it was chosen over other available research methods. In addition, this chapter will focus on the implementation of the chosen research method and the results of data collection. The following chapter will then outline the results of the data analysis.

The main research objective of this thesis is to answer the question of what consumer concerns are regarding their personal data in online marketing. The sub objectives that are going to be answered are consumer's views towards personalized advertisements in online marketing and their awareness of tools available to protect their privacy online. These objectives have been chosen to gain familiarity with the phenomenon of online privacy views of consumers and achieve new insights.

As this thesis is a research-oriented report, a choice between quantitative or qualitative research methods had to be made. Both methods collect different data; quantitative research is applicable to phenomena that can be expressed in numbers and graphs and to established generalized facts by confirming or denying theories, Qualitative research is concerned with qualitative phenomena, for example when examining human behaviour and their causes to understand concepts, thoughts, and experiences. (Kothari 2004, 3).

This thesis will be using qualitative methods, mainly personal interviews, to collect the data necessary to answer the research questions. Since the research objectives of this thesis aim to understand consumers' thought processes and their motivation for privacy concerns online, qualitative research is best suited. A mixed approach of both quantitative and qualitative research was also not appropriate for the nature of this thesis, because the phenomenon of online privacy concerns cannot be expressed through generation of quantitative data. The research objectives represent consumers' subjective feelings and worries, which are best investigated by personal interviews with said consumers.

Personal, structured interviews with three chosen individuals from the EU were conducted for this thesis. Structured interviews involve a set of predetermined questions by the interviewer; all interviewees were asked the same set of questions, independently from each other. Structured interviews were chosen so that the answers from all interviewees can be easily compared to each other to get a deeper understanding of consumers' concerns of

their online privacy as well as their awareness of tools to protect it. The opportunity with this kind of interview is the fact, that more information can be gathered in depth and there's greater flexibility with the ability to restructure questions in case of uncertainties or questions interviewees might have.

3.2 Implementation

To conduct successful interviews, the interviewer must plan the process in advance, such as preparing the interview questions to get an understanding and insights into the research objective. For this purpose, six well-crafted interview questions were prepared. The questions in interviews should not be easily answered with Yes or No but give the interviewees the opportunity to share all their thoughts and feelings they have regarding the research objectives. Additionally, the interview questions should be non-leading to avoid pushing interviewees down a certain path and therefore manipulate the answers given. The research questions can be found in Appendix 1.

To represent a wide range of European society, three people from various age groups and gender representations were chosen as interviewees to answer the prepared questions. They were then asked if they would feel comfortable being part of the research process of this thesis and invited to either in person interviews or over video chat, since not all interviewees live near the thesis author.

The interviews took approximately one hour each and were recorded with the consent of the interviewees, for later transcription and analysis of the given answers.

Lastly, the interviewees will not be mentioned by their full names but with initials, to keep their anonymity.

The following people were interviewed: Interviewee S.S., male, 20 years old and a university student. Interviewee I.Ö., female, 26 years old and a healthcare professional. And lastly interviewee J.S., male, 33 years old and a postal worker. In the following chapter the results of the transcribed interviews will be presented and summarized.

4 Results and Discussion

4.1 Interview results

The first question that was asked of each interviewee was “What does personal/private data mean to you in an online context?”. Interviewee S.S. answered that personal data in an online context means his physical location that is accessible to website or app runners, his search history on the internet and his IP address. The other two interviewees gave more in depth answers such as I.Ö. for whom personal data means sensitive personal information that can and will be collected about her person, like her IP address, her name, birth date, address, residence, search history and so on. She summarized it as every little detail that’s somehow connected to her personally. Postal worker J.S. indicated that personal data in an online context is anything that he wouldn’t want the public at large to know. This includes data such as his address, social security number and health status. He also suggested that for other people, personal data might also mean their full name, martial status, political leanings, employment status and sexual orientation, to name a full example. On the clarifying question asked by the interviewer if J.S. does not consider his full name his personal data, he answered that he considers that public data.

The next question interviewees were asked was why or why not would they share their data with companies online? Interviewee I.Ö. is vehemently against it, because she doesn’t want her data to be collected or even published – even if that was done anonymously. Her data should, according to her, only belong to her and nobody else should have access to anything related to her person. The internet, so the healthcare worker, should be a safe space without companies trying to collect data from innocent people. Contrary to I.Ö., interviewee S.S. shares a completely different opinion, in which he doesn’t mind if companies collect his data online, as long as it’s not shared publicly. He is aware that a lot of apps and programs online are free to use because of him giving away his data, and he appreciates paying with his data instead of real money. Similarly, interviewee J.S. would and does share his data with companies online to get access to their services; many free to use websites and apps such as Youtube, TikTok, Twitch and Twitter have their business models based around advertising to you based on the information you’ve given them with cookies and your usage habits.

The third question that was asked was “How much information and what kind of information do you think companies have of you online?”. While S.S and I.Ö. shared both that they think companies have their IP-address and location, S.S also specified that he thinks companies know his health information since he wears smart watches. On the other hand,

J.S. believes that companies know more about him at this point than he knows about himself. Especially Google has had many years to figure out who he is and what he likes, what his habits are etc. They know where he is at all times because of his phone, they know what he's searching online using their search engine – by that they know what political content he consumes and his political leanings, they know what video games he plays and what he does in his free time. They also know, so J.S. believes, where he works because of his location data, and they know who he has saved as his contacts since he uses a Google created Android phone.

In relation to the last question, the interviewer then asked what the interviewees views towards personalized advertisements were. I.Ö. shared that she does not like them at all and finds them creepy because in her believes, nobody should know what she's looking up online or what kind of clothes she likes or what she recently bought. She acknowledges that other people might find this useful to find items like their previous purchases but personally is not a fan. Contrary to this, S.S answered that he doesn't mind them if they don't appear instantly after he's talked about something. J.S. also has the opposite opinion of I.Ö., he enjoys personalized advertisements because he doesn't live under the illusion that advertisements don't influence him, so knowing that and knowing Google AdSense being the biggest ad platform in the world with some of the most sophisticated algorithms working on almost infinite data points, he is fully aware that personalized advertisements will show him exactly what he'd want in a product. J.S. also shared that it isn't always successful showing him advertisements he would be interested in, but he suspects it is because Finland isn't a huge ad market compared to the rest of the world and because he has relatively niche interests, making advertisements specifically tailored to him not available.

The following question that was asked was if the interviewees are concerned regarding their personal data that they've shared online or has been collected of them and if so, what their concerns are. All interviewees gave very differing answers. University student S.S is not concerned at all about the data he's shared or has been collected of him online, but he can imagine others being afraid that companies know almost everything about a person. While S.S. isn't concerned at all, I.Ö. shared that she is concerned about companies collecting her data online even though she says she is just another small person that companies don't specifically care about but collect her data to improve their websites, advertisements, and work in general. She would rather prefer if they could collect data without it being possible to be traced back to her person. She also shared that collecting data isn't always bad when speaking about the topic of online crime. Another different viewpoint is the one of J.S. who has, according to him, completely given up on the concept of online privacy. Terms of services are too hard and long to read for a normal person and

he shared that he has agreed to many of them without knowing what they entail. His major concern moreover is data leaks and his personal details getting into the hands of malicious actors because he has seen the huge amounts of damage that people can do with very little information. That being sad, he is at the same time not extremely paranoid because he understands that even if someone somehow got access to all his user data of companies like Google or Twitter, he would be a very low priority largely due to being not famous and not rich.

Lastly, all interviewees were asked if they are aware of tools that can protect their privacy online and if they would use them or not. S.S shared that he knows about VPNs and ad blockers that also block cookies. He sometimes uses VPNs but not for privacy reasons, more so for availability of content, that isn't possible to be viewed from his country. The same applies to ad blockers, so S.S. I.Ö. answered that VPNs seem like a really good way to keep her information private. Although the more advanced one's cost money, she still prefers to surf the internet with one. The health worker also shared that she is aware of being able to surf in incognito mode, but she still gets personalized advertisements even then, so she doesn't trust that it works its intended way. The first tools that come to mind for J.S. is the EUs GDPR data protection act that allows any person to request their data to be deleted by any company and that company must respond or they will get in very large financial and legal trouble. For him, there's also the option of using a VPN like surfshark and NordVPN to take a more proactive approach to protecting his data. Lastly, J.S. shared that there's also mass deletion tools for your old messages or posts on the internet which have helped him clean up his online post history in the past.

4.2 Views towards personalized advertisements

Personalized advertisements can shortly be defined as the delivery of customized content to consumers through data collection, its analysis and implementation. (Jen Murray 2017.) As previously established, consumers are becoming more apprehensive about disclosing their data, while at the same time expecting personalized marketing efforts towards them by companies. (Kingsnorth 2016, 204-205.) This seemingly paradox thinking of consumers is represented also in the results of the conducted interviews. While one person stated that they are apprehensive and even completely against personalized advertisements, others enjoy them and expect them to be tailored towards them. As one of the interviewees mentioned, sometimes consumers will get advertisements seemingly tailored towards something they've only said out loud and not searched online or bought online. While this can scare consumers into believing their phones or other electronical devices are listening and spying on them, it is mostly likely not the case. This belief would mean that companies are recording everyone, analysing those recordings, and storing them in their data

bases. Even though with technological advances the gathering and storing of data has become cheaper, the computing power requirements to process the amount of that being produced by billions of cell phones listening to conversations would be an unrealistically large amount. What is more likely happening is the fact that companies can predict what products and services consumers want to see advertised to them, through their analysis of consented data they provided online.
The desire by consumers to see advertisements that are personalized towards them, described by Kingsnorth, is also represented in the study findings.
It is not surprising to find both views towards personalized advertisements represented also in the target demographic displayed by the interviewees, as views on most things can be either positive or negative. Based on this, it is interesting to find that some consumers will not have a distinct positive or negative view on personalized advertisements, they let them happen and don't think too much about them. It can be assumed that they're still influenced by those advertisements, since they improve the selling of products or services of companies, otherwise those advertisements wouldn't be as widespread as they are nowadays.

4.3 Awareness of privacy protection tools

Consumers have a wide array of tools available to protect their privacy online. As previously established privacy can be protected by managing privacy settings in browsers and apps, using two factor authentication, strong and secure passwords and only sharing personal information with companies and websites that consumers trust. (Maryland Attorney General's Office. 2022.)

A more hands-on-tool to privacy protection is the usage of Virtual Private Networks, or in short, VPNs. The interview candidates were all aware of the existence of VPNs and shared that they all have been using them. Not always was this for the purpose of privacy but also to access content not available at their location, which is another feature VPNs offer. Only one interviewee mentioned the European Union's General Data Protection Regulation, the other two were asked if they too knew of this regulation, which they denied. Furthermore, the interviewee who mentioned the existence of the GDPR only knows one function of it – the request to have your data that companies store deleted.
None of the interviewees are aware of the core rights being issued to them as consumers by the GDPR. The author of the thesis concludes from these findings that most people are aware of some privacy protection tools, prominently the ones being advertised to them like VPNs or ad blockers but aren't aware that there are actual laws and regulations that protect their privacy as consumers online as well. Most consumers seem to care about their online privacy when asked, some using tools such as VPNs and ad blockers to escape

personalized advertisements, but often it appears to be the case that consumers don't necessarily know their rights regarding their personal information online – may that be the collection, distribution, or usage of it.

4.4 Summary

The thesis' main objective is the question if consumers have concerns regarding their personal data in digital marketing and if so, what those are. Established in the theoretical part of this thesis, consumer privacy concerns have increasingly grown over the last decade and can be attributed to a variety of internal company factors as well as external ones (Kumar & Reinartz 2018, 280).

Through the qualitative research, the author has gathered different views on the objective of the thesis, although most of the interviewees answered that they are concerned about their online privacy. The fear of the data of consumers ending up in data leaks is present, as well as the aversion of their data being collected at all by companies and their marketing teams in specific. Consumers are also concerned about what they agree to in companies' Terms of Service but still take the trade off to be able to access products and services. It is especially interesting to note that even while consumers are concerned for the privacy of their personal data, not all are aware of many privacy protection tools, laws and regulations.

In conclusion, consumers are concerned about their online privacy and with the advancement of technology and with that the advancement of marketing strategies, it can be concluded that consumers will also grow more concerned in the future. Consumers are, moreover, most concerned about not knowing what data is being shared with companies and what said companies are doing with their data. This outcome of the qualitative research matches the findings of chapter 2.2.1, where consumer privacy concerns and their reasons are discussed in detail.

5 Conclusion

5.1 Future research suggestions

As the thesis dived deep into the topic of privacy protection tools, mainly the European General Data Protection Act, further research on its impact on consumer privacy should be conducted. As many people are not fully aware of how the GDPR works and how it affects companies and businesses, the real impact of its regulations on consumers should be studied and evaluated. It is known how the GDPR has affected companies both in the EU itself but also worldwide. It would be interesting to gather information on its affects on the consumers themselves. Has their day to day lives been affected by the GDPR and how could that be measured? Why are many people not aware of the GDPR and its workings and implications? These questions validate a new research approach.

Moreover, the growing privacy concerns of consumers have implications for companies and especially their marketing departments. Further research into what those implications are and how they will be changing as consumer privacy concerns will keep growing as well as the advancement of modern-day technology. With the latter ever evolving, privacy laws might and will have to adapt and with that companies will have to follow. There might come a time where most consumers will no longer be comfortable with sharing a lot of their data which can be cause of marketing strategies having to change and adapt.

5.2 Evaluation of thesis process

The thesis process helped the author to learn and develop various existing and non-existing skills and knowledge. The topic chosen for the report let the author dive deeper into their major of Marketing and explore an important part of it – privacy and its protection. The author has been passionate about the topic of privacy and was able to relate it to their major in their degree field. Through this, the author gained a deeper understanding of the thought processes and feelings of consumers, since often the focus is on the company side during their studies.

Moreover, the author developed their communication skills by conducting three, one-hour long interviews with people they weren't close to. This enabled the author to get more confident and improve their social skills. With the interview process comes the knowledge gained about conducting qualitative research and its evaluation. The author developed their skills in academic writing and conducting research for the thesis through different kind of media.

Lastly, the author learned new methods and the importance of time management as both writing this thesis and doing the mandatory work placement have, for the majority, taken

place at the same time. This the author would not recommend for future students writing their thesis.

References

AO Kaspersky Lab 2022. What is VPN? How It Works, Types of VPN. URL: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn. Accessed: 28 October 2022.

Dynamix Solutions Inc. 2017. What Is Internet Privacy and What Does Privacy Mean to You? URL: https://dynamixsolutions.com/what-is-internet-privacy-and-what-does-privacy-mean-to-you/. Accessed: 23 September 2022.

Jen Murray 2017. What Is Personalized Marketing? Strategy, Examples & Trends. URL: https://emarsys.com/learn/blog/what-is-personalized-marketing/. Accessed: 15 August 2022.

Kingsnorth, S. 2016. Digital Marketing Strategy. An integrated approach to online marketing. Kogan Page. London.

Kothari, C. 2004. Research Methodology. Methods and Techniques. New Age International (P) Ltd. New Delhi.

Kumar, V. & Reinartz, W. 2018. Customer Relationship Management. Concept, Strategy, and Tools. Springer. Berlin Heidelberg.

Maryland Attorney General's Office. 2022. Consumer Guide to Protecting Privacy Online. Maryland. URL: https://www.marylandattorneygeneral.gov/CPD%20Documents/Tips-Publications/Consumer_Guide_to_Protecting_Privacy.pdf. Accessed: 25 October 2022.

Proton AG 2022. What is GDPR, the EU's new data protection law? URL: https://gdpr.eu/what-is-gdpr/. Accessed 24 October 2022.

Salesforce Inc. 2022. Personalization Defined: What is Personalization? URL: https://www.salesforce.com/resources/articles/personalization-definition/. Accessed 25 October 2022.

Solove, D. 2020. The Myth of the Privacy Paradox. GW Law Faculty Publications. Washington DC. URL: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2738&context=faculty_publications. Accessed: 22 October 2022.

Storage Networking Industry Association 2022. What is Data Privacy. URL: https://www.snia.org/education/what-is-data-privacy#_ftn1. Accessed: 20 September 2022.

Tapp, A., Whitten, I. & Housden, M. 2014. Principles of Direct, Database and Digital Marketing. Pearson. Edinburgh Gate.

Voigt, P. & von dem Bussche, A. 2017. The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer. Berlin Heidelberg.

William Goddard 2019. How Do Big Companies Collect Customer Data? URL: https://itchronicles.com/big-data/how-do-big-companies-collect-customer-data/. Accessed: 29 August 2022.

Appendices

Appendix 1. Interview questions

1. What does personal/private data mean to you in an online context?
2. Why would/wouldn't you share your data with companies online?
3. How much information/what kind of information do you think companies have of you online?
4. In relation, what are your views towards personalized advertisements you get online?
5. Are you concerned regarding your personal data you shared/has been collected of you online and if so, what are your concerns? (in-depth)
6. What are tools available to protect your privacy online – are you aware they exist? Would you use them and why/why not?