Data privacy on digital platforms – EU citizens' protective behaviour and privacy concerns

Master thesis

15th May 2020

Authored by:

Mette Bjerring Petersen (92962)

Sofia Boskovic (50287)

Copenhagen Business School

MA International Business Communication – Intercultural Marketing

Supervisor: Manuele Citi

Number of pages: 117 pages

Number of characters: 229,136 characters

Abstract

In the wave of increasing global scandals of data misuse by big data companies, the debate about data privacy has received enormous public attention. As a result, consumers demand more control over their data for the sake of staying private online. This thesis sought to explain how EU citizens' demand for strengthened data privacy correlates to their behaviour of protecting their data on digital platforms. Theories point towards trust, risk and convenience as having crucial impact on the degree to which consumers protect their privacy. The research approach for this study included Mixed Methods consisting of semi-structured expert interviews and a quantitative consumer survey regarding digital platforms and privacy concerns, for the purpose of uncovering the parameters and their influence on consumers' behaviour.

From the findings of the survey, we were able to confirm that the parameters of trust, risk and convenience influence the consumers' data protection behaviour. Additionally, the findings pointed towards a fourth influencer namely the consumers' level of awareness. However, as awareness plays a key role in understanding the complexity around data and how to stay private, we found it important to discuss whether or not consumers are equipped for the responsibility that has been placed upon them. This lead to specific recommendations for altering the GDPR and the current initiatives for data privacy, in order to meet the consumers' wish for more control.

Tabels of Content

1. Introduction

With the birth of the world wide web, otherwise known as the internet, consumers found that they had access to a whole new world of information. Information-sharing and connectivity between people became unlimited and just at hand. As of 2019, 57 percent of the global population had access to the internet due to the advancement of mobile technology and continuous modernization of countries (Clement, 2019). This means that 4.1 billion people have access to the largest information database. However, the use of the internet does not come without sacrifices. Globally, people are becoming more and more concerned with their online privacy and governments and web developers are finding it difficult to keep up with the ever changing environment of the internet and its complexity (Clement, 2019). The concerns about online privacy stem from the fear of being hacked, having one's identity stolen, fraud, malicious use of information etc. Data has become the new currency and it has become so valuable that organisations are building their business-models on the flow of data. Hence, the collection, storing and sharing of data has intensified as businesses have experienced the value that they can derive from these practices. With the increase in privacy concerns, a demand for more data protection has risen. Globally, legal action such as the 'US Privacy Act of 1974', 'The International Data Privacy Law' and EU's 'General Data Protection Regulation' (GDPR) has come into force to enforce the right to privacy. Moreover, several non-EU countries have adopted data privacy laws similar to the GDPR as a response to the growing issues of data misuse (Simmons, 2019).

1.1. Problem area

Over the past 25 years our lives have been increasingly digitised and technology has become an integral part of our everyday life. In the EU, legislation has been in place since the infancy years of the internet and in 1995 the Data Protection Directive set the first set of standards towards protecting personal data and the free movement of such data (EDPS, n.d.). In 2016, the EU passed the GDPR that replaced the 1995 Data Protection Directive. The GDPR regulation differentiates itself from the 1995 Data Protection Directive with an expansion of the definition of personal information so that online identifiable markers, location data, generic information, and clear privacy

notices are included (Virtual College, 2018). Additionally, the 1995 Data Protection Directive fined non-compliance with amounts up to one percent of the annual turnover, whereas the GDPR fines non-compliance with up to €20 million, or four percent of the annual turnover. These fines also entail that individuals can claim compensation of damages and the person responsible for data breaches can be sentenced to jail (Virtual College, 2018). By 25th of May 2018, the GDPR came in force and all EU member states had two years to comply and implement the regulation into national legislation. Any company that stores or processes personal information about an EU citizen within an EU member state must comply with the GDPR, also if they do not conduct businesses in the EU (Rossow, 2018). According to the GDPR, if data breaches occur the breach must be reported within 72 hours after the incident. The evaluation of how well the data team has handled the breach and how they have minimised any possible damages also impacts the size of the fine that will be given (Rossow, 2018).

As of 31 March 2020, 250 fines for non-compliance with the GDPR have amounted to a total of approximately €154,000,000 (Privacy Affairs, 2020). The largest fine was given to Google at an amount of €50,000,000, for not having a valid legal basis to process users' personal data for the purpose of ad personalisation (CNIL, 2019).
The increase in people's privacy concerns has surfaced to a large extend due to the aftermath of Donald Trump's 2016 presidential election campaign and the Cambridge Analytica scandal. Cambridge Analytica, a bureau that provides consumer research, targeted advertising and data related services to its clients. After Trump was elected as president of the USA, it was revealed that Cambridge Analytica since 2014 had obtained data on more than 50 million Facebook user through an application where people could log in with their Facebook account (Ingram, 2018). The application's purpose was for research, however its users' data was harvested, including data about their Facebook friends. Cambridge Analytica had obtained access to the harvested consumer data and used it for developing personalised marketing campaigns throughout the Trump election campaign. Cambridge Analytica CEO, Alexander Nix, claimed that the company could develop psychological profiles of consumers and voters, which would be much more persuasive and effective than any traditional advertising could (Ingram, 2018).

In late 2019, another incident of data privacy breaches occurred. This time as part of Brexit in Great Britain. AggregateIQ, a Canadian data firm, broke privacy laws in its work for the leading pro-Brexit group, as it had shared data collected by Vote Leave through Facebook, and without the users' knowledge, used the information they had disclosed to Facebook, for the purpose of creating Facebook advertisements aimed at potential voters (Reuters, 2019). AggregateIQ was later linked to Cambridge Analytica and once again Facebook came under pressure from the public (Reuters, 2018).

The aftermath of big scandals like Cambridge Analytica and AggregateIQ has made consumers more aware and interested in their online data privacy. The scope of the harm caused by a data breach arouses fear amongst consumers, as the consequences of such incidents are played out publicly. Consumers are scared of how a nation state actor can hold the intent to manipulate your decisions (Bowles, 2018) or how services can change for the individual on the basis of data generated through his or her online activity. Surveys show that consumers in the aftermath of data breaches scandals do not trust how tech giants like Facebook, Google, Apple, and Amazon manage their data (Tresorit, 2019). Data privacy specialists have for years advocated for more regulation on data privacy, as they understood early on, how much data is being generated on the consumer and how it is used without their knowledge, and they also forecasted how much damage this could bring along. The scandals of Cambridge Analytica and AggregateIQ have been ground breaking and have directed the consumers' attention towards how important and crucial it is for the consumer to understand, practise and protect their data privacy online.

1.2. Research question

The aim of this study is to investigate how consumers think of their own data privacy when they are using digital platforms. Privacy as a general term can be very subjective, hence we seek to determine how the broader majority defines data privacy and thus try to determine what they are doing to protect their data privacy. As studies throughout the years have determined, consumers' intentions to behave a certain way on digital platforms does not necessarily correlate to how they end up behaving. This

also goes for protecting their online data privacy. Consumers state that they wish to gain more control over their data and that they wish to stay private. However, statistics show that even after expressing this, their behaviour on digital platforms does not reflect that they are taking the measures to protect their data. The majority of consumers do not change their behaviour or alter it in alignment with their intention of staying somewhat private. We seek to investigate how the consumers' demand for strengthened data privacy correlates to their behaviour on digital platforms. The literature states that the divergence between the consumers' intention to protect their data more and what they actually do to protect it, is known as the privacy paradox. This study adopts the assumption that the privacy paradox exist. On these grounds, it will seek to determine what parameters affect the consumer to behave the way they do on digital platforms. Several schools of thoughts have tried to determined interferences with consumers' behaviour, therefore we will tests some of these parameters in the context of data privacy, as a means to possibly explain data protective behaviour in relation to the digital consumer anno 2020.

In the posterity of the GDPR and the EU Commission's increased focus on digitalisation, the research questions for this study is as follows:

How do EU citizens' demand for strengthened data privacy correlate to their behaviour in protecting their data on digital platforms?

To answer the research question we seek to uncover the concerns of the consumers when determining their data privacy on digital platforms. Second, we test what parameters influence the consumers protective behaviour, and analyse if other relevant parameters also affect this behaviour. This analysis will be followed by a discussion of the findings and of the changing landscape of digital platforms. Finally, we will provide our recommendations on what measures are needed for meeting the consumers demand for strengthened data privacy.

1.3. Delimitation

In the process of answering the research question for this thesis with the resources available, certain delimitations were made. Thus, this section will outline the scope of this thesis.

This thesis focuses on EU citizens privacy concerns and their behaviour on digital platforms, in order to uncover what causes the respondents to protect or not protect their data on digital platforms. As the GDPR applies to all EU citizens, this is also the reasoning behind delimiting our focus to respondents only from EU member states. Thus, the focus for this thesis is solely on the GDPR and no other EU law or national law concerning privacy.

As this thesis seeks to investigate how consumers' behaviour correlates to their beliefs and concerns for data privacy, it is necessary to establish that behaviour is delimited to the consumers' intended and self-perceived behaviour. Namely, we assume that the consumers' claimed behaviour corresponds to their actual behaviour on digital platforms. Thus, theories that explains the divergences in consumers intended behaviour and actual behaviour were included to provide a nuanced description of data privacy and consumer behaviour. By including this we are able to discuss the matter of consumer behaviour and challenge the belief that consumers can effectively utilise more control in practise. We thus base our study on the acceptance of the privacy paradox.

Moreover, the findings of this thesis are delimited to the conduct of an online self-completion survey based on theories on the privacy paradox and privacy in general, as well as semi-structured expert interviews and empirical data.

1.4. Project structure

The thesis will first introduce a background section of what has happened up until this study was conducted. As the GDPR has come into force, the last few years has changed the digital landscape for all EU member states. These changes will be outlined as a first.

Hereafter the theoretical chapter of relevant literature within the field of data privacy, consumer behaviour and digital platforms will be outlined. Specifically, the literature review will present and define the concept of privacy and the phenomenon of the

privacy paradox, while also shedding light on different angles to privacy. Lastly, the literature review will introduce the example of internet cookies as a data tracking tool and explain how consumer behaviour relates to different practises of cookie notice designs. From the theory presented the literature review will present hypotheses that are to be tested and determined in the analysis.

Thereafter, the methodological chapter will present and justify the thesis' research design, philosophy and approach. Moreover, a reflection of the quantitative and qualitative data collections, their interplay and the strengths of using these approaches will be elaborated. Lastly, the methodology will outline and discuss the reliability and validity of the methods, while also presenting the limitations of the study.

The analysis will present the findings from the qualitative data collection and set out to determine if the hypotheses can be confirmed or not. This chapter will on the basis of the qualitative data collection determine its respondents' privacy concerns and how they behave on digital platforms. In this chapter the findings are structured under three parameters - as presented in the literature review - which are trust, risk and convenience. Findings derived that cannot be placed under these, will be further investigated and elaborated. The analysis also presents a section of how a quantitative analysis of our data could supplement and support our findings.

The discussion will debate the concept of data privacy and what measures consumers can take to protect their data. Additionally, how the GDPR interferes with consumers and how the industry works under this regulation, will also be discussed. Based on the analysis and the discussion, a set of recommendations for policymakers will be provided with the purpose of optimising the GDPR and responding to consumers wish for more control.

Lastly the conclusion will sum up the thesis, conclude the main findings and finally answer the research question.

1.5. The data landscape

The increased focus on data privacy has brought with it significant changes to the landscape of digital platforms. The GDPR has become the reference point for all aspects of handling personal data thus serves as a big step towards increased protection of consumers' data privacy. However, there are some loopholes to be found

in the regulation and one goes for data transfer to third parties. In the GDPR, Art. 23 states that: "*the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union"* (GDPR, 2016, pp. 48). The idea with this was to ensure that EU-citizens would be protected no matter the nationality of the company from which they would purchase or be advertised to purchase from. However, there are possible scenarios of which EU-citizens data could fall outside the frames of GDPR and thus not be protected under this regulation. An example of this could be when a non-EU company provides a catalogue portal on its website, where consumers can browse products anonymously. Then, when they are ready to purchase, they can click on a product belonging to an independent third-party company, that has placed its product in this this catalogue, which will transfer the consumer to this company's website. If this company's website does not have any European languages or currencies conversions available, which in itself would appeal the consumer to purchase something, then this third party company can deny this data transfer as being connected to an offering. Moreover, the first company can deny having handled personal data from the consumer, as the consumer browsed anonymously and thus did not leave any data in the first place. Besides this, the company can deny having handled data related to offerings, as the consumer did not make the purchase through the product catalogue itself, because the purchase and data disclosure hereof was conducted on the third party's website (Magde, 2017). This example is a good illustration of why third parties have received public attention from both consumers and industries.

Browsing anonymously online like in the mentioned scenario has become possible for consumers with the incorporation of privacy enhancing technologies in internet browsers. In 2017, Apple introduced the ITP (Intelligent Tracking Protection) feature for the Safari browser, which prevents third-party cookies from tracking the consumers across different platforms (UrRahman, 2019). The ITP technology in the Safari

browser features three elements. First, when a consumer closes the browser, all tracking stops. Second, the provider of the browser is no longer allowed to target personalised ads towards individuals. Third, the advertisers have a restricted time period to measure the effects of their marketing through cookie tracking (Lundin & Jørgensen, 2020). Apple introduced in a later version of the Safari browser that first-party cookies are deleted after seven days (some first-party cookies only have a 24 hours deletion window) and blocks all third-party cookies by default (UrRahman, 2019). As a result, in 2019 Mozilla followed Apple's footstep and introduced their own privacy tool, the ETP (Enhanced Tracking Protection) for their Firefox browser, with the blocking of third-party tracking by default (UrRahman, 2019). For the consumer this means that they can stay more private across platforms and websites. However, for the marketeers and large organisations that build their business model on consumer data, these browser privacy measures have enormous impacts. As a result of the enhanced browser privacy features of the Safari and Firefox browser, around 20 percent of users that previously could be targeted through ads are now unreachable to advertisers. Google also states that publishers who bought ads on the Safari browser, their revenue has dropped with 50 percent since the launch of the ITP feature (Lundin & Jørgensen, 2020). Google's Chrome browser is not as restrictive as Safari and Firefox, however, privacy is a choice that the consumer has to make, therefore they offer a opt-in version of the ITP and ETP. On the Chrome browser, Google is only just starting to phase out third-party tracking and stated that by 2022 cookies are somewhat out phased. This means that in Google Chrome, cookies are still tracking the consumer after the browser is closed (Lundin & Jørgensen, 2020). Within the near future, cookies are forecasted to die on the Safari and Firefox browser, hence less data is to be extorted from consumers using these browsers.

Another area of data privacy that has received attention in the public debate, is related to location data. In December 2019, Apple launched the iOS 13 update where a new notification system was implemented. The notification could say: "*Facebook has used your location 107 times in the background over the past 3 days. Do you want to continue to allow background location use?*" (Haggin, 2019). Apple announced that the notifications are helping consumers to become more mindful of how many apps on their iPhones are tracking their everyday locations. The notification pops up periodically and so far millions of people have blocked apps ability to track their

locations when they are not using the app. As a result of the iOS 13 update, several organisations whose business model is built on accessing the user's location at all times have accused Apple of anti-competitive behaviour, as Apple's own built-in apps are not providing any notification. App developers argue that the new update may confuse the less technical users, who will assume that the app is not working properly and ultimately abandon and delete the app (Perez, 2019). Users can turn location tracking on indefinitely, however it is a multistep process that most will probably skip and the new update with still pop up sometime later on, providing the reminder that the app has used the location certain times within the last amount of days (Albergotti, 2019). Apple stated that they build hardware, software and apps to protect user privacy and not to know the consumers' location or the location of their device, hence they believe that the iOS 13 update is one step closer to empowering the consumer (Haggin, 2019).

While the use of tracking technology and location data from users constitute the business model for several known apps, such as the transportation app Uber and the dating app Happn (Uber.com, 2020; Happn.com, 2019), there are other ways to track users of smartphones and for other purposes. As the COVID-19 pandemic has spread to the entire globe affection over 200 countries in 2020, several companies have offered their help and taken part in the responsibility of the national governments' work to fight the virus (World Health Organization, 2020) One example is Apple and Google's new project for controlling outbreaks by automating contact tracing that would otherwise have been carried out by human interviewers. The way it works, is that Apple and Google will create a new feature in their iOS and Android systems, so that users can voluntarily download an app that will allow only recognised public health authorities to interfere with the system, also known as an API (Fung, 2020). Users that have been infected with COVID-19 can then type this data into the app, and other users with this app that have been in contact with this person will receive a notification. The tracking and the transfer of information runs through a Bluetooth connection. According to a Harvard University white paper "Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks" there are privacy risks connected to using the Bluetooth connection, as individuals can be linked to the owners of the accounts. The white paper proposes that the Bluetooth connection is supplemented with a feature that uses randomly generated codes in the form of soundbites that can

be picked up by other phones (Harvard University, 2020). While it is still too early to say whether the app will be adopted by the public, it raises an important question about the various usages of personal data and to what extent the consumer is willing to disclose certain types of data, be that browsing behaviour, location, health data or financial data.

Several theories state that trust is a parameter for disclosing personal information and increasing trust is also an aspect included in the GDPR. Art. 78 relates to encouraging the producers of products, applications and services that are based on the use of personal data, to consider the principles of data protection when designing these, in order for the controllers and processors to be able to abide by the rules on handling personal data (GDPR, 2016). Setting the stage for how products and services should be designed in the future creates ethical boundaries for developers which can help foster trust for all parties involved. From here, the Privacy by design concept has arisen in the public debate with the argument that it can serve as a competitive factor for companies that are able to brand their products, services as well as their company as taking their users' privacy seriously. One example of how Privacy by design concept has won foothold, is the Danish initiative on a labelling scheme for IT-security and responsible data use. The collaborators behind this initiative are the Confederation of Danish Industry, Danish Chamber of Commerce, SME Denmark, the Danish Business Authority and the Danish Consumer Council (Erhvervsministeriet, 2019). The label is to help consumers feel more safe when interacting with companies that brand themselves with this label, but it is also supposed to help companies that wish to take cybersecurity and data handling more seriously, but lack the tools to carry out their strategies for it. Thus, the label for IT-security and responsible data use is an example of how companies can grow and innovate without it being at the expense of the consumers' privacy. The idea of a labelling scheme has also entered into the discussions on AI technologies and their underlying algorithms, which constitutes the core foundation for new digital business models. In October 2019, The German Data Ethics Commission proposed a set of recommendations for rules on AI and algorithms. Here, they introduced the criticality pyramid, a model that assesses products and systems in regards to their algorithmic systems' ability to cause potential harm to its users, on a 5 level scale. 1 being "applications with zero or negligible potential" and 5 being "Applications with an untenable potential for harm". Based on this model, the

Data Ethics Commission proposes a mandatory labelling scheme for all applications on a least level 2 or upwards. Thus, the labelling scheme is an initiative that aims to guide companies in assessing their applications as well as guide legislators and society to appropriate regulatory instruments (Data Etische Kommissionen, 2019). On 19 February, the European Commission launched a white paper on AI along with its European Digital Strategy (European Commission, 2020). In this white paper, the Commission proposes a voluntary labelling for companies with no-high risk AI applications similar to the initiative of the German Data Ethics Commission. Thus, the debate on data privacy has entered several areas of digital technologies such as IoT, cybersecurity and AI, and moreover it has received attention on a European level. While the outcome of the Commission's new strategy is still unknown, it can be expected that it will bring changes to the ways the data industries operate today.

Thus, in the wave of new features in software, browser privacy, best practise initiatives, etc., the landscape for the consumer's privacy on digital platforms is changing and consumers are being reminded about their online activity and the data they generate. Overall, the concept of empowering the consumer as well as increasing their awareness about their data generation is impacting the industries a great deal. New lines are being drawn by policymakers in order to empower the consumer and their privacy and for data driven organizations, a rethinking of how to get a hold of consumer data in a transparent and consensual way is crucial.

2. Literature review

In 2015 the EU Commission conducted a survey regarding EU citizens data privacy concerns in the EU and the survey showed that more than 80 percent of the respondent felt that they only had partial or no control at all, over the information that they provide online (European Commission, 2015). On 25 May 2018, the GDPR presented by the EU Commission, came into force and contributed with an increased awareness amongst EU citizens regarding their data rights online. The goal of the GDPR is to give consumers more control over their data in order to protect their online privacy. In 2019, approximately one year after the implementation of the GDPR, 44

percent of EU citizens believed that the GDPR regulation protected their privacy rights more than prior to the GDPR (Deloitte, 2018). Consumers do care more about their privacy, also online. However, while consumers' awareness about their own privacy rights online is increasing, statistics shows that their behaviour does not follow suit in protecting these rights. In 2019, Cisco conducted a cybersecurity series, which revealed that only 32 percent of the respondents cared about their data privacy, were willing to act on it, and had already acted on protecting their privacy (Cisco, 2019). Somehow, consumers express a concern for their data privacy, however their behaviour does not follow suit.

To answer the research question the following section will present theories on data privacy, the privacy paradox and consumer behaviour on digital platforms. First, the mismatch between consumers attitudes and behaviour, namely the privacy paradox, will be presented, followed by a clarification of parameters that different schools of thought have stated causes the paradox to appear. Second, factors to consider in relation to privacy concerns are also elaborated, followed by a presentation of internet cookie tracking and privacy concerns consumers may have in relation to this.

2.1. The Privacy Paradox

The discrepancy between consumers' attitude and their actual behaviour regarding online privacy is known as the privacy paradox (Kokolakis, 2015). Several researchers have tried to explain the privacy paradox from different theoretical lenses such as social theory, behavioural economics and psychology. The phenomenon of the privacy paradox can be split into two parts when investigating the methodological approaches, namely surveys and experiments. The majority of existing research has investigated the phenomenon based upon surveys that aim to uncover the reasoning behind the perceived intention to disclose information. Experiments have been conducted to detect consumers' behaviour and the deviations from their intended behaviour. However, the experiments have received much criticism as they often cannot recreate a realistic context (Kokolakis, 2015). Hence, to investigate the phenomenon of the privacy paradox entails conducting both surveys and interviews to uncover consumers' intended behaviour to disclose their personal information, and experiments to uncover if they succeed in carrying out their intended behaviour.

2.1.1. Privacy

Privacy is often described as an individual's 'right to be let alone' (Wang, Lee & Wang, 1998). However, when the consumer conducts activities on a digital platform, privacy refers to personal information and invasion of privacy such as unauthorized collection of data, disclosure, or use of personal information as a direct result of electronic commerce transactions (Wang et al., 1998). Wang et al. (1998) divided personal information into two categories based on how they change over time: static private information and dynamic personal information. Static private information is referential information, historical financial information, health information, personal beliefs and personal documents (Wang et al., 1998). Dynamic personal information is information that changes significantly over time and that is collected over time and analysed for the purpose of composing a consumer profile (one's online activity history) (Wang et al., 1998). Dynamic personal information is known as the information that organisations deduce from your online behaviour and not what static information you type into e.g. required boxes when making a profile. When using digital platforms our behaviour generates massive amounts of data that organisations can use to digitally profile us as consumers. This information can explain when we are most likely to purchase certain products, what our preferences are and so on. Both static and dynamic personal information is crucial to include when investigating data privacy, as both categories of information qualify as personal identifiers that are specific to the individual's identity. Consumers value their privacy but do not take the right measures in order to actively protect it. There are a variety of explanations as to why this is. Consumers might not be aware of the many ways that they leave themselves vulnerable when using digital platforms, they might not know how to protect themselves, they might find it too overwhelming to establish and maintain privacy measures, or they might find it beneficial for them to trade their privacy for convenience, goods or personalised and better services (Coventry, Jeske, Blythe, Turland & Briggs, 2016). Consumers pay little attention to the data traces they leave online and most consumers know little about data collection and how it is used (Spiekermann, 2005). Hence, this could explain why the consumers do not protect themselves from cybersecurity and privacy risks. Given this, we predict that:

H_1: Consumers wish to gain more control over their data for the purpose of protecting their data privacy.

When talking about the privacy paradox, Holvast (1993) and Rosenberg (1992) distinguish between three modes of privacy: (a) territorial privacy which relates to the physical surroundings of a person, (b) privacy of a person, which relates to the protection against undue interference, and lastly (c) information privacy, which relates to people having the right to control how their personal data is gathered, stored, processed and deleted (Kokolakis, 2015; pp. 123). This research is interested in consumers' personal data relating to protection against undue interference and information privacy on digital platforms. As consumers have increasingly become more concerned with their data privacy online, surveys show that 60 percent of consumers are willing to share more of their personal data for the trade-off of receiving personalised benefits and discounts (Deloitte, 2018). Thus, consumers are not completely unwilling to share their data, however the data sharing process is dependent on an individual's evaluation of the trade-off that is being made.

Barry Brown (2001) was one of the first researchers to investigate the privacy paradox with his small research on consumers' behaviour when using the internet. Brown (2001) found that when consumers were asked about their beliefs regarding their online privacy, trust, risk and convenience played crucial roles. Several of the respondents from his research stated that they were hesitant about providing retailers with their private information on the internet, due to the possible risk of doing so, either as actual damage or perceived loss of privacy (Brown, 2001). The issue of trust was relevant as security online is extremely technical, and therefore the consumer had no chance in deciding whether or not the sites or the internet in general was secure enough for them. The knowledge and understanding of what the internet is and how consumers fit into it, is often intangible for the average consumer. "*A physical wallet is something which individuals known about and can control - a 'computer wallet' is something unknown, and not easily controlled*" (Brown, 2001, pp. 16). Brown (2001) discovered that despite hesitations, also with private financial information regarding the security of one's privacy online, the experiences and encouragement of relatives and friends were a strong enough factor for the consumer to experiment with the internet and thus they conducted a 'see what happens' attitude. The media affected

consumers' judgement, however, the opinions of relatives and friends and one's own experience weighted highest in the decision making process. This entailed, that if the consumer did not experience an immediate problem with their actions online, the risk they associated with online activity would decrease (Brown, 2001). However, convenience also dominated the consumers' decision of whether or not to use the internet. Brown (2001) described this as a privacy paradox, as the consumers seemed to be willing to use the internet and give up some of their privacy for a very little gain. Still to this day, consumers express their concerns about their online privacy, however, they are still willing to give up their personal information to online retailers, as long as they receive something in return (Kokolakis, 2015). The tendency to share one's personal information online is often directly linked with the cost savings of receiving discounts, loyalty carts and gifts offered by retailers.

2.1.2. Valuation of privacy

Carrascal, Riederer, Erramilli, Cherubini & Oliveira (2013) investigated how consumers value their personal identifiable information while browsing online. Their study showed that users tend to value their offline privacy higher, such as age, gender, address, economic status, higher than their online privacy. Consumers value their offline privacy at about €25, whereas their online privacy is valued at around €7. The difference was extraordinary, however they concluded that offline data often is more explicit and understandable for the consumer to grasp. Whereas, it is more difficult for the consumer to understand the implications of having their personal identifiable information tracked, mined, logged and used for digital profiling of themselves. Hence, Carrascal et al. (2013) found that consumers value their online privacy at the same price as a Big Mac when browsing online. They also found that there are different valuations when sharing data on different types of websites: consumers tend to value their privacy higher on online social networks and finance websites, compared to search databases or shopping (Carrascal et al, 2013). Previous studies have investigated the consumers' willingness to disclose their financial information and something could indicate that financial data and personal information is valued higher than other types of data (Phelps, Nowark & Farrell, 2000). On these grounds we predict that:

H_2: Consumers value their financial information higher than other types of data and hence would not like to share this, as it is perceived as private.

Carrascal et al. (2013) also found evidence that supports the idea that consumers are more willing to provide their personal information if a beneficial trade-off is being offered. Consumers have a tendency to trade their personal identifiable information for monetary rewards or improved services over increased 'free' services or targeted advertising (Carrascal et al, 2013).

Hence, it is proven that there exist a discrepancy in consumers' opinions and their actual behaviour. However, one explanation could be, as Carrascal et al. (2013) also found, that consumers have difficulties in understanding what data organisations are collecting on them online, the amounts of data that they collect, and how it is being used for targeting consumers with personalised marketing incentives. Consumers are simply not aware of the magnitude of how much data they generate or the scope of their data generation. The majority of consumers are most likely blinded by the benefits and value what these 'free' services provide them, thus explaining why they pay little attention to the subject.

2.1.3. The influence of trust and risks on privacy

From a behavioural economics approach, Acquisti (2004) found that consumers are not able to act as economically rational agents, when it comes to their personal privacy, which led him to his economic model. This model explains the inconsistencies between consumers attitude and their behaviour. From his research Acquisti (2004) found evidence of how the immediate gratification bias is causing the paradox. The immediate gratification bias explains that consumers have a tendency to value the present benefits higher than possible future risks (Kokolakis, 2015; pp.124). Acquisti (2004) came to the prediction that consumers might have a problem with self-control, as we tend to chase immediate gratification: "*... we tend to avoid and postpone undesirable activities even when this will imply more efforts tomorrow; and we tend to over-engage in pleasant activities even though this may cause suffering… in the future*" (Acquisti, 2004; pp. 25).

Hence, consumers value the personalised content, discount, offers, gifts etc. that they receive from retailers online, higher than protection against the perceived risk of losing

control over their personal data. Acquisti's (2004) economics of privacy revealed that consumers' decisions are not stable over time but reflect the economic and social costs and benefits of protecting privacy within a particular context (Coventry et al., 2016). The consumers' protection of their own privacy is thus determined in the context they dedicate to the trade-off. This leads us to the prediction that:

H_3: Consumers trust digital platforms, because they do not experience consequences of sharing their data.

Acquisti (2004) concluded that the privacy paradox cannot be resolved by increasing awareness or educating consumers about their rights or the precautions of using the internet, as the consumer cannot be trusted to make rational decisions when it comes to their own personal privacy online. Often some consumers come to the realisation that protecting themselves from privacy intrusion is unavoidable, leading to decreased willingness of adopting strict privacy protection measures to their everyday lives (Acquisti, 2004). To overcome the paradox Acquisti (2004) suggested that a mixture of technology that is designed with privacy enhancing tools, consumer awareness, and regulatory policies, as these could possibly increase privacy-related welfare. Acquisti's suggestions are translated into what we today know as Privacy by Design. Privacy by Design aims to ensure that the incorporation and implementation of the basic privacy protection principles and privacy enhancing tools are present from the very early stage of making a product (Datatilsynet, n.d.).

In 2007, Norberg, Horne and Horne conducted an extensive research which investigated the privacy paradox with the focus of the relationship between what consumers intend to disclose in regards to personal information and their actual disclosing behaviour. Norberg et al.'s (2007) research, on the contrary to previous studies that mainly focused on willingness to provide information, focused on the degree to which intentions followed actual behaviour in terms of privacy. Their conceptual model of the privacy paradox stipulates that behavioural intentions to disclose are solely linked to the risk of doing so, and that the actual disclosing behaviour is directly linked to trust. This means that when asked about ones intention to disclose, the related risks have significant influence on the response, whereas when asked to disclose in a given situation the actual disclosing behaviour is influenced by the trust relationship between the parties (Norberg et al., 2007). This mean that Norberg et al. (2007) claimed that risk influences the intentions to disclose, but it is not

as strong of a influencer to be carried out into an actual disclosing behaviour. However, it is only trust that directly influences the actual disclosing behaviour.

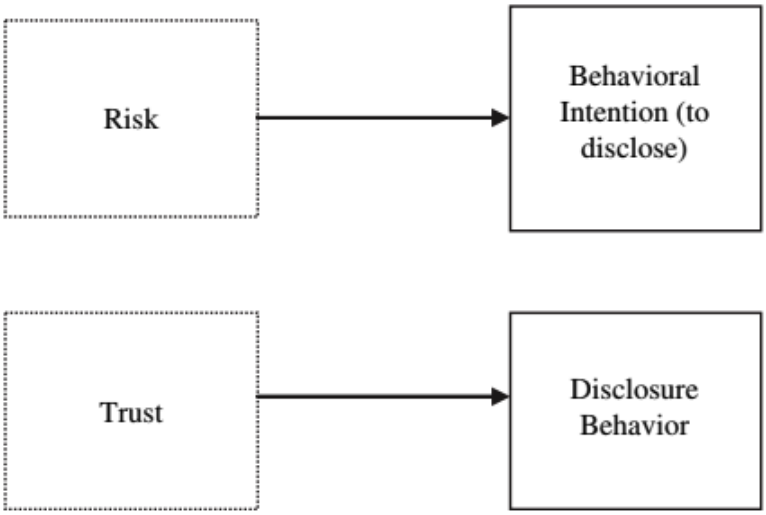


Figure 1. Norberg et al. (2007), pp. 105

Norberg et al. (2007) came to confirm the existence of the privacy paradox and concluded that consumers tend to disclose substantially more personal information than they previously stated that they intended to. They also identified a varying level of disclosure in relation to the information categories: personal identifiers, financial, preferences, demographics, etc. (Norberg et al., 2007). Consumers tend to be more sensitive about disclosing their medical, financial and family information, relative to their product or brand consumption or their media usage behaviour (Norberg et al., 2007). The consumers disclose in relation to the given context of whom they disclose to and what type of information they are asked to disclose. Thus, they stipulates that behavioural intention is not an accurate indicator of people's actual behaviour. Norberg et al. (2007) pointed towards consumer educational incentives in order to align the privacy paradox implications of intentions deviating from behaviour, as they supported the belief that explicit planning influences the relationship between intentions and disclosure.

2.1.4. Intention-behaviour gap

From the phycological school, the privacy paradox relates to what Sniehotta, Scholz & Schwarzer (2004) describes as the intention-behaviour gap. Sniehotta et al. (2004)

investigated the underlying psychological processes that leads intention to action. Intentions are explicit decisions that concentrate the consumer's motivation towards a goal in terms of direction and intensity (Sniehotta et al., 2004). The gap occurs when the consumer intends to act but somehow fails to realise these intentions. Action planning, self-efficacy and action control are some of the most dominant influencers if a consumer is to act in accordance to his or hers intentions (Sniehotta et al., 2004).
To bridge the intention-behaviour gap, the process is divided into two parts: the motivational phase and the volitional phase. In the motivational phase the consumer develops the intention to change, on the basis of self-beliefs, risk perceptions, outcome expectancies and perceived self-efficacy. In the volitional phase the intended behaviour must be planned, initiated and maintained, while relapses also must be to managed. Sniehotta et al. (2004) do not believe that risk awareness is a strong predictor of behaviour. However, outcome expectancies play a crucial role for the consumer to outweigh the possible positive and negative outcomes. If positive perceived outcomes outweigh the negative ones, the chances of developing a strong intention to change behaviour increases (Sniehotta et al., 2004). Additionally, the perceived self-efficacy: one's own belief in that one has the capabilities to accomplish a certain task with one's own actions and resources is crucial to develop a strong intention to change the behaviour. When the consumer has developed the intention, he or she moves from the motivational phase into the volitional phase. In the volitional phase, self-regulatory efforts are crucial and must be practised until the new behaviour becomes habitual (Sniehotta et al., 2004). Planning is how the consumer develops a mental representation of a suitable future situation, and it is a crucial tool for implementing intentions. This is also referred to as action control. Self-monitoring, awareness of standards and efforts are important actions in the course of self-regulation and action control (Sniehotta et al., 2004).

Ölander and Thøgersen (1995) claimed that the intention-behaviour gap were determined by three determinants: motivation, ability and opportunity (the MOA model).

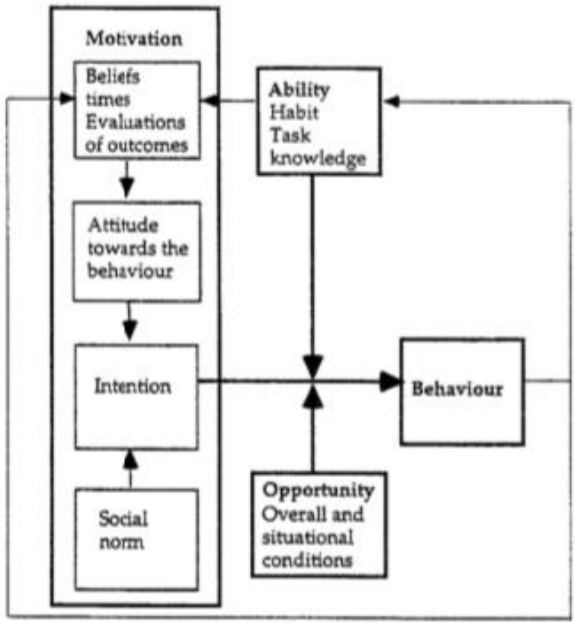


Figure 2, Ölander & Thøgersen (1995), pp. 361

The first determinant, motivation captures that the consumer takes on an action towards a the targeted object (Ölander and Thøgersen, 1995). The consumer's intention to engage in a behaviour transforms motivational factors, such as attitudes and social norms, into a behavioural disposition. The second determinant, ability, implies that the consumer carries out his or her behaviour disposition. Motivation as a determinant, entails that the consumer is capable of acquiring the ability it takes to perform the intended behaviour. The concept of ability is operationalised with two factors: habits and task knowledge. The consumer learns routines and habits that makes it possible to perform a task almost automatically while needing a minimum of conscious attention (Ölander and Thøgersen, 1995). This entails that the failure of carrying out the intended behaviour often is a direct consequence of old habits. Ölander and Thøgersen (1995) suggested that insufficient information, lack of understanding the message, or forgetting important information, may lead to the failure of reaching their goal. The third determinant, opportunity, is a precondition for performance of a given new behaviour. The fewer delays, diversions and obstacles that come between the intention and the actual performance of a specific act, the better facilitated the conditions are for the intended behaviour to be performed (Ölander and Thøgersen, 1995). For the consumer to close the gap between their intentions and their lack of behaviour, the consumer must foster a strong motivation,

have the ability and see the opportunity to change his or hers old behaviour for the sake of performing the intended and new behaviour.

2.2. Degree of sensibility in disclosure of information

When investigating the privacy paradox, it is important also to recognise that personal information comes in several shapes and that the consumer attributes different valuations to these (Kokolakis, 2015). Most researchers have investigated the privacy paradox based on different types of information, however, one must acknowledge that information about location, health, age, weight, personal preferences and browsing history are valued differently from consumer to consumer. Kokolakis (2015) suggests that it is not appropriate to investigate the basis of the paradox based on different types of personal information, as the levels of sensibility varies. Mothersbaugh, Foxx II, Beatty and Wang (2012) challenged the existence of the privacy paradox, as they examined the sensitivity of information in the context of privacy. Sensitivity of information is the potential loss associated with the disclosure of information, where losses can be physiological (loss of self-concept due to embarrassment), physical (loss of health or life), or it can be material (loss of financials or assets) (Mothersbaugh et al., 2012). They claimed that the discrepancy between consumers' intended disclosure of information and their actual disclosure is directly linked to the belief that sensitive information is perceived as riskier and more uncomfortable to reveal. Thus, they claim that risk plays an important role in whether or not an individual discloses information or not. Hence, people do not disclose as they intend to, based upon how sensible they believe that the information is to them individually. Mothersbaugh et al. (2012) supported Norberg et al. (2007) in the claim that trust is more influential to the actual disclosure than the perceived levels of risk are. For the industry to match the consumers' intention with their behaviour, the consumers should; have greater control and customisations over the information they are giving up, experience higher levels of trust in organisations, and adapt information request to the situation (Mothersbaugh et al., 2012). Some researchers also stipulate that organisations with strong reputation and high levels of consumers trusting the brand find it easier to make consumers disclose more sensitive information about themselves (Mothersbaugh et al., 2012). Thus, these organisation hold an advantage in collecting user data.

2.3. Threats related to disclosure of information

Not only does the level of sensitivity of information disclosure affect whether or not consumers are willing to disclose what they intend to. Consumers experience different types of privacy concerns such as social threats (harassment, bullying or stalking), organizational threats (marketing or secondary use of data by the data collector or a third party), and improper access by an employer or the public (Kokolakis, 2015). A study on online social networks, revealed that organisational threats negatively influence the amount of information that consumers disclose, due to the fear that their data will be collected, stored and processed. Hence, organizational threats result in consumers disclosing less information, whereas social threats have no significant impact on the amount of information that consumers disclose (Krasnova, Günther, Spiekermann & Koroleva, 2009). Krasnova et al. (2009) came to find that consumers tend to disclose less personal information about themselves if they fear having their data tracked, logged or processed by an organisation and a third party on a platform. However, if consumers fear social threats on a platform, the amount of information they disclose is not decreasing, as experienced with organisational threats. Consumers rely heavily on privacy settings, restricting access from unwanted audiences, and the usage of nicknames instead of full names (Krasnova et al., 2009). The study concluded that consumers selectively engage in privacy conscious self-communication based upon what type of concern they connect to the disclosure. Krasnova et al. (2009) suggest that fair information practises, increased privacy settings controlled by the consumer, transparency, enhanced access control and education of the consumers in how to best protect and control their identity and context, is crucial to overcome privacy concerns.

2.4. Internet cookies versus privacy

The consumers' discrepancy in how they intend to protect their privacy and how they actually behave, makes it possible for organisations to design 'nudges' with the intent to affect the consumers' privacy behaviour (Coventry et al., 2016). Design nudging is often seen when organisations track consumers' behaviour on their digital platforms

with e.g. the use of cookies. When seeking to nudge the consumer in the form of cookie notices, the idea is to present options that nudges the consumers towards a certain behaviour. Studies have found that nudges that use a social norm references have a strong influence on consumers as they mimic the behaviour of a group, and thus appeal to the individual's social need for group affiliation and social conformity (Coventry et al., 2016).

Before investigating consumer behaviour in relation to cookie notices, it is essential to define what a cookie is. "*A cookie is a small piece of data sent from a website, which is then stored on a user's browser and transmitted back to the website every time the user browses a site. Cookies are promoted as being necessary to enhance the user's experience by aiding navigation, identifying preferences, allowing personalization, targeted advertising and remembering login credentials*" (Coventry et al., 2016, pp. 3). For businesses, cookies are their main source to track their website traffic, clicks, adjust its offering for returning customers and to advertise more strategically (Bornschein, Schmidt & Maier, 2020). Tracking consumers' behaviour on digital platforms with cookies raises privacy and security issues, as they can log usernames, passwords, credit card details, addresses and other personal identifiable information, while also tracking consumers' behaviour across websites in order to profile the consumer. However, as a cookie is tracking consumers behaviour online, consumers also see a convenience in receiving personalised content and auto filled boxes that saves them time.

Studies have shown that convenience plays a crucial role for the consumer when they use online platforms. Organisations that operate online have placed emphasis on offering consumers convenient shopping, which takes form in terms of speed enhancement on websites, ease of reaching the retailer, identifying, selecting and obtaining products, and making easy transactions (Jiang, Yang & Jun, 2013). When investigating the aspect of convenience in consumers' behaviour on digital platforms, researchers identify two key elements of convenience: time and effort (Jiang et al., 2013). Time saving is linked to the consumers reaction when being forced to wait, whereas effort saving is linked to the minimisation of cognitive, physical and emotional activities that consumers experience when purchasing goods and services online (Jiang et al, 2013). Convenience is influenced of the non-monetary costs of time and

effort, meaning that the consumer value the saving of time and effort the highest when they purchase online.

2.4.1 Studies on cookies

Besides the convenience in allowing cookies to track one's behaviour and thus trading privacy and data for personalised and convenient surfing online, studies have revealed that consumers habituate to the cookie notification over time and ultimately do not pay enough attention to them (Coventry et al., 2016). The cookie notification banner interrupts the consumer in achieving their primary goal, which can create security vulnerabilities where they accept all cookies and end up giving up more privacy than they originally wish to. If returning to the convenience that consumers are seeking when they browse online, the aspect of a cookie notice being displayed on their screen, could be a possible explanation to why consumers have started to ignore them, as they simply interrupt the consumer in his or her actions. Additionally, a cookie notice that forces the consumer to on the spot make the decision whether or not to accept or decline cookies that track their behaviour, is inconvenient. Hence, the consumer clicks any button to make it disappear so that they can continue with their primary purpose. Several studies have been conducted, not only on cookie notices but also on consent dialogs in general. It is a known fact that consumers do not bother to read notices and do not care about warnings. Possible explanations are that the consumers lacks choices, knowledge or habituation (Böhme & Köpsell, 2010). For years, interface designers have studied and trained consumers to clicking through dialogues for the purpose of redeeming their primary purpose of using the website. Consumers often take a dual path in their decision making process: either they make systematic decisions where they take all information into account, or they resort to heuristics as a convenient shortcut (Böhme & Köpsell, 2010). In some instances studies have also found that the use of a default button also affects the consumer by 'guiding' them in their behaviour (Böhme & Köpsell, 2010). This is also a known nudging design of the cookie notice. As a result, consumers view the default button in dialogue boxes as a recommendation, when or if in doubt. The above mentioned theories findings on dialogue boxes leads us to predict that:

H_4: Due to inconvenience, consumers tend to allow privacy pop-ups in order to access the content they are seeking without calculating the privacy risks before clicking.

Based upon studies like the above mentioned, the EU introduced the GDPR regulation in 2018 to empower the consumer and gain back control over their own data. The GDPR regulation forces organisations that operate in the EU, to disclose their information privacy practises by displaying a cookie notice to all visitors on their digital platform (Bornschein et al, 2020). The cookie notice must be a visible notice, it must disclose how the website will use the obtained private information, and the consumer must be given the choice of refusing the collection of data (Bornschein et al, 2020). As the GDPR regulation only regulates the overall principles, the EU member states are allowed to variance the cookie notice design to some degree. This means that websites vary the visibility and content of their cookie notice. Some websites has implemented small bars hidden in the edges of the screen, whereas others has implemented a fly-in overlay window, in which an action to allow or not must be made in order to proceed on to the website. Additionally, the content also varies, as some websites only inform the consumer about the usage of cookies (the cookie notice design), whereas other websites allow for the consumer to define what cookies they will allow, also known as the cookie choice (Bornschein et al., 2020).

Bornschein et al. (2020) conducted a study where they investigated the effect of the different combinations of the cookie notice design and the cookie choice, and how this affected the consumer's risk and power perceptions. From their pre-study they found that 36 percent of the investigated websites do not feature a cookie notice, even though they make use of cookies. From the vast majority of the websites that did provide the cookie notice, they found that they use a cookie notice with no choice, so that the consumer only could confirm and not decline the tracking of their behaviour. Simultaneously, these websites also make use of low visibility of their cookie notice design (Bornschein et al., 2020). This indicates that organisations have not shifted the power to the consumer but that they simply stay ‘within the lines’ of the GDPR. Overall, Bornschein et al. (2020) found that when the consumers are notified with visible cookie notices and when they are offered a choice, their perceived power increases, whereas solely providing a notice increases the consumers risk perception. Therefore, they concluded that notifying the consumer about data collection is insufficient and that the GDPR has not led to a higher degree of consumer power.

Other researchers have investigated if personality trait affect whether the consumer accepts or declines a cookies. Coventry et al. (2016) found that social norms have a high effect on the consumer when they are met by a cookie notice. This means that the phrasing in a cookie notice plays a crucial role too (Böhme & Köpsell, 2010), as if it is stated that most people like you did 'this' or a default button is visible, then the majority of consumer will mimic this behaviour. Additionally, they also found that personality traits like impulsivity and risk-taking affects the decision making process when they have to decide whether or not to allow cookies.

Overall, it is crucial to overcome any possible habituation that the consumer might hold, in order to make sure that they pay attention and understand why they need to decide on cookies on given websites. Egelman, Cranor and Hond (2008) made a study on phishing warnings and they found that warnings or pop ups must interrupt the primary task, provide clear choices, fail safely (one must read all before it is possible to close the window), and prevent habituation (meaning that design must be different). Minor changes must be done regularly with the design of the cookie notice in order for the consumer not to be habituated when they see them. By altering the design, the consumers are more likely to read and make a reasoned decision on whether or not they should accept certain types of cookies.

This type of decision making when designing cookie notices and the general presentation features when making a digital platform, is known as opt-in and opt-out marketing. Opt-in marketing refers to organisations explicitly asking for permission to e.g. collect the consumers data and give the consumer a choice over what cookies they allow when they enter the website (Kumar, Zhang & Luo, 2014). Any time after opt-in, the consumer can opt-out again. Opt-out marketing refers to organisations e.g. not providing a notice about their use of cookies but tracking them without permission from the consumer, but with the possibility to decline all cookies (Kumar et al., 2014). The opt-out marketing method is not reminding the consumer what their rights are and the consumer must actively reach out to the organisation in order to opt-out. The two approaches are heavily discussed in the debate about consumer privacy. The Direct Marketing Association recommends that the opt-out method is the best approach, however other researchers claim that the opt-in method where the consumer is

empowered and has more control is more effective, both for the industry and the consumers (Milne & Rohm, 2000).

Bornschein et al. (2020) forecasted that if consumers decide not to allow cookies tracking their behaviour on digital platforms, the whole system of online consumer acquisition will be challenged, as this makes it impossible for organisations to track where their website traffic is originating from. Data driven businesses that build their business model upon consumer data is challenged on its existence. Additionally, the system of 'free' services that some digital platforms offer and that the consumer does not pay for, at least with money, will also be challenged. To run a 'free' service in the shape of a digital platform is expensive and currently consumers are paying with their data which helps organisations optimise, personalise and expose consumers to convenient browsing, shopping and services. As the GDPR allows for less visible cookie notices, this could possibly explain why the majority of websites do not take more severe actions in empowering the consumer. A future without cookies where consumers are leaving browsers - for the sake of other more private browsers - or declining cookies, will entail that organisations in no way, shape or form can track their website traffic. Content based business - like online newspapers - will also be endangered, as advertising will be blocked across digital platforms, resulting in these businesses losing their main stream of revenue (Bornschein et al, 2020). The environment of increased consumer awareness and the realm of GDPR, the future for these businesses are challenged and for survival they must begin to either comply with the demand of the consumer or rethink its whole business model, if they seek to survive.

3. Methodology

As consumers throughout the years have expressed their concerns with their online privacy, this study aims to explain why consumers behave the way they do on digital platforms and how this correlates to their wish for more privacy on digital platforms. In this chapter the methodological choices will be justified and explained. First, the research design of both the quantitative and qualitative data collections will be

explained, followed by a clarification of the study's philosophy of science and the research approach used to answer the research question. Lastly, we will discuss the reliability and validity of our research and present the limitations of this study.

3.1. Research design

3.1.1. Quantitative data: consumer survey

The primary data for this study was collected from a publicly shared consumer survey. This approach was chosen as we became aware of a lack of research agreement between the theories of privacy paradox, which all stated very different reasons for under which consumers do or do not protect their data privacy as they claim they do. To uncover which reasons were the most evident, we decided that it would be of relevance to conduct our research based on answers from consumers instead of relying only on empirical data. The survey consists of a range of questions that aim to determine consumer privacy concerns and their claimed behaviour on digital platforms. Thus, the mode of generalisation for this survey is statistical generalisation, as this research aims to estimate the likelihood that the trends observed in the survey will hold for the larger group i.e. the population of EU citizens (De Vaus 2002).

3.1.1.1. Construction of the survey

The survey consist of two elements. The first part has its focus on the respondents self-reported behaviour on digital platforms for the purpose of uncovering how they interfere with these and how much, as well as which data, the respondents intentionally share when they use digital platforms. The second part, will consist of causal questions asking why they behave the way they do. The questions put forward thus seek to uncover the intentions of protecting one's personal data and what parameters are dominating when doing so. The parameters of which we seek to measure the impact are as determined in the literature review divided into trust, risk and convenience. The survey consists of 17 questions (see Appendix 1) of which nine questions provided answer options in the form of statements, namely the matrix structure. As we sought to investigate consumers' attitude on data privacy, the questions we asked were defined as attitudinal question (Kristensen & Hussain, 2016).

Here, the 5 point Likert scale format was used to measure the extent of agreement of each statement with:

- Strongly disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

We do acknowledge the fact that our choice survey structure presents a challenge for us as researchers. This is due to the complexity of using the matrix combined with a Likert scale, compared to only using only Likert scale questions. This can also have affected the respondents ability to complete the survey.

When constructing surveys, it is important that the question content fits the purpose of uncovering the issues of interest. There are five distinct types of question content: attitudes, attributes, behaviour, believes, and knowledge (De Vaus, 2002). In this study, we were interested in uncovering what privacy concerns consumers identified with digital platforms and for what reasons they were willing to give up some their privacy. Thus, we were mainly interested in asking questions with content relating to people's behaviour on digital platforms, but also in their beliefs about and attitudes towards privacy, as well as their knowledge about e.g. cookies and privacy enhancement technologies, as these may impact the consumers' behaviour. A behaviour content question was stated as follows: "I allow all cookies", which related to sharing ones data through cookie tracking on internet browsers. A question relating to belief content was: "I believe that I can control my data by restricting cookies" and was asked to establish what people think is true rather than on the accuracy of their beliefs. An attitude content question was stated as: "I believe that digital platforms are currently doing enough when it comes to protecting my privacy" and was asked to establish what consumers think is desirable when it comes to privacy on digital platforms. A knowledge content question was states as: "I do not know what cookies does". The survey also contained a few attribute content questions, also known as demographics, about age, gender and educational level, which were used in the introduction of the survey for the purpose of collecting characteristics on the

respondents to crosscheck if these represented the larger scale of all EU citizens and as control variables for our quantitative analysis later on.

Overall, the matrix questions consisted of statements that were closed-ended, as this enables us to statistically analyse the data afterwards (Kristensen & Hussain, 2016). Additionally, the survey also introduced two why-questions as we wanted the consumers to explain in their own words, why they are concerned with sharing certain types of data, and why (if they claimed so) they would not like to share their data. These elaborating questions were asked to investigate if additional reasonings, other than those that the literature review presented, might have interfered with the privacy paradox. By asking these elaborating questions, we have heightened the valence of the study, as no elaborations deviated from our matric statements (Saunders, Lewis & Thornhill, 2007).

Besides the nine matrix Likert scale questions and the two free text elaborating question, the final six questions consisted of multiple choice formats. The three demographic questions were choices between multiple nominal categories, whereas the two final were choices of multiple attitude statements (De Vaus, 2020).

Moreover, to ensure that the questions we sought to ask the respondents did not come off as inconsistent in terms of subject (Kristensen & Hussain, 2016), we collected the questions under five overall themes: ‘Demographics’, ‘Digital platforms’, ‘Terms, conditions and cookies’, ‘Your data on digital platforms’, and ‘Your personal protection online’. Additionally, we included an introduction letter for the respondents to read when they first opened the survey. This was done to increase the motivation for the respondents to answer the survey and to provide the respondents with the sense that their contribution was influential for the survey to become a success (Kristensen & Hussain, 2016).

3.1.1.2. Survey sampling

As this study seeks to investigate EU citizens privacy concerns and their behaviour on digital platform, this study sought to represent the larger population of the EU member states. Hence we sought to conduct a probability sampling (De Vaus, 2002). The sampling size of the survey was 202 with a stratified random (Bryman & Bell, 2011) selection of participants. 202 participants opened and started the survey, however only 126 of these answered all questions, which gave us a total response rate of 62.4

percent. The participants were in the age group under 21 to 60+, male and female with nationalities from any EU member state.

However, the survey was shared with a link on various digital platforms with different target groups to obtain responses from a broader range of users. The survey was shared on Facebook to reach a broad target across nationalities, age groups and educational backgrounds, and on LinkedIn, which particularly targets people with academic backgrounds. The survey was also shared on University sites at Copenhagen Business School, as well as Maastricht University. To target other segments rather than the segments of younger university students, the survey was shared at our respective workplaces and at our families workplaces, to ensure that people from a broader range of age groups with different educational backgrounds answered the survey. To ensure a representable sampling as much as possible, we tried to encourage voluntary participation by stating that participants taking their time to answer this would be of much appreciation, however it was voluntary (De Vaus, 2002). Additionally, it was also stated that their participation would be completely anonymous.

However in terms of sampling representability, as the survey was shared on platforms that we ourselves make use of, hence the respondents will to some extent represent our own demographics, our sampling has become a non-probability convenience sampling (Bryman & Bell, 2011). Hence, this study cannot state anything about the broader class of the EU population, however it can suggest something about a group of EU citizens matching our respondents demographics. This entails that the generalisation based on representation of the broader EU population has decreased as a consequence hereof, however not on the aforementioned group of this study (Saunders et al., 2007). Moreover, as the survey was shared on global networks, we were unable to control for non-EU citizens' participation. Further elaboration of the sampling representability of the broader class of EU population can be found under 'Descriptive' in the analysis.

3.1.1.3. Data analysis

3.1.1.3.1. Qualtrics

The primary data collection consisted of a survey in the customer experience software Qualtrics. To properly analyse the survey data, we first made use to filtering of answers in Qualtrics. While 202 individuals had opened and begun answering the survey, only 126 of these were able to complete it. Thus, to ensure that that our data was not flawed by this, we removed all the answered from respondents that did not complete the entire survey. Additionally, the data was also analysed for suspicious answering patterns, such as if someone repeatedly answered in one end of the Likert scale or continuously answered 'neither agree nor disagree'. None of these behaviours were detected, hence filtering against this was not necessary.

As part of the survey flow in Qualtrics, we enabled the function 'force response' on all of questions, to ensure that the results would not be subject to missing or incomplete data. As we made use of the 5-point Likert scale with a forced choice format we sought to encourage the respondents to provide an actual response and determine their stance on the given matter before proceeding (Wivagg, 2008). As we are aware of data privacy being a complex and intangible topic for the majority of the population, we sought that those respondents that either had 'no opinion', were 'not sure' or did not know about the question they were given, have probably answered 'neither agree nor disagree'. However, a possible explanation to why 76 respondents did not complete the survey, could be that they did not feel that the 'neither agree nor disagree', which is a neutral answer on Likert scale, truly reflected their opinion (Wivagg, 2008). The issue with this method is that it may force the respondents to express views that they do not really hold (Bryman & Bell, 2011). "*Some respondents really may not know how they feel about an issue or may not know the information requested, and forcing a response would result in the collection of erroneous data*" (Wivagg, 2008; pp. 290). Ultimately, the choice of force response could have caused 76 respondents to terminate their participation. By forcing the respondents to make a choice and expressing their opinion, we tried to eliminate the respondents from taking the 'easy way out', as consumers laziness refrains them from making an effort in evaluating their own behaviour on digital platforms (Bryman & Bell, 2011). Thus, we do not believe that using forced choices has affected the data quality.

Additionally, the Qualtrics survey software also offered visualization tools of the data collection, which allowed us to visualise our response rates with tables. All tables used for the analysis chapter were retrieved from the visualization tools in Qualtrics, with the percentages and not the counts as measures. The data and visualisation tools from Qualtrics enabled us in conducting a qualitative analysis of the survey data.

3.1.1.3.2. Stata

In addition to using quantitative data as input for our survey, we investigated the possibility of conducting a quantitative analysis of our hypotheses, to support the findings of our qualitative analysis. Here we made use of the statistical programme Stata. It must be stressed however that this quantitative analysis was not incorporated in our initial research design, which resulted in the variables of our hypotheses being by no means optimal for such an analysis. This is also why it was not possible to test all four hypotheses in a quantitative analysis. However, we chose to quantify our hypotheses for the purpose of demonstrating the process and how it could be used as a supplement to our findings from the qualitative analysis. In order to carry out linear regressions of our hypotheses, we identified the dependent and independent variables of each hypothesis. Not all four hypotheses were included in the linear regression models, as it was not possible to identify survey questions that directly supported the independent variables of private H_2. However, for H_1, H_3 and H_4 finding variables for linear regressions was possible to some extent.

The process of deriving the linear regression can be exemplified with H_1. The dependent variable in H_1 was identified as “protection of data” and the independent variable as “wish for control”. To identify the dependent and independent variables the questions relating to these were identified. The questions of the survey followed the 5-point Likert scale, which means that they contained five values: ‘strongly disagree’, ‘disagree’, ‘neither agree nor disagree’, ‘agree’ and ‘strongly agree’. While these values are treated as ordinal values from 1-5, with 1 being ‘strongly disagree’ and 5 being ‘strongly agree’, they are not suitable for a linear regression as they are not continuous variables. Hence, we sought to aggregate our data into clusters and from the means of the these, obtain continuous variables that could be included in linear regression models. The means of each cluster serve as the dependent and independent variables in our hypotheses. Our first attempt in Stata included gathering

all ordinal values, meaning all the questions from our survey that could be treated as variables in a linear regression, and aggregating these. We sought to use as much of our data as possible, however some questions were excluded. The only questions we excluded from our correlation tests were the demographics; age, education and gender that serves as control variables, and elaborative questions in which respondents were asked to explain their opinion on the given topic. However, as the clusters did not correspond to what we sought our variables to represent and as the questions in the clusters did not correspond to the independent and dependent variables identified, we made a second attempt.

In the second attempt, we chose to aggregate only certain questions separately. These questions reflected our dependent and independent variables for each hypothesis. Six separate correlation tests were conducted for each variable of the three hypotheses, namely H_1, H_3 and H_4. Thereby, we were able to control that these clusters were now meaningful in terms of the questions they contained, while still using the factor analysis to ensure that our clusters were statistically reliable. The first correlation test was done on the dependent variable of H_1, namely the wish protection of data. This correlation test consisted of the five chosen questions: “I want to keep certain types of data about myself private”, “I regularly set, check or change my privacy settings”, “I make use of privacy protection tools and apps”, “I try to educate myself and I investigate how I can control the data that I generate”, and “I do not believe that protecting my data myself has any effect on my data privacy”. To ensure sampling adequacy of our chosen questions and to identify how suited our data was for a factor analysis, the Kaiser-Meyer-Olkin Measure (KMO) was conducted (S., 2016). The KMO score for this correlation was 0.687, which is below the generally accepted value of 0.8 to 1. Hence, this introduces a limitation to the reliability of this correlation, which must be accounted for when analysing the outcomes of the test. Hereafter, we conducted a factor analysis based on this correlation for the purpose of validating the combination of the selected questions (Stata.com, n.d.). The factor analysis resulted in one factor that the questions gathered around. When checking the factor, all values above 0.40 were accepted as valid, which produced one factor that gathered the questions: “I try to educate myself and I investigate how I can control the data that I generate” and “I make use of privacy protection tools and apps”, thus eliminating three of the questions from the gathering in the correlation. To test how closely related the three questions that the factor analysis validated, the Cronbach’s alpha test was

applied (UCLA, n.d.). Generally, alpha values above 0.5 are accepted. The reliability coefficient of the alpha test was 0.76. Subsequently, we aggregated these two questions by taking the mean of these and produced a new continuous variable that could represent protection of data. The same procedure was carried out across all independent and dependent variables of the hypotheses 1, 3 and 4 (Appendix 2).
It is crucial to acknowledge that when conducting the above mentioned tests we generally accepted lower adequacy scores across the KMO and reliability scores of alpha. Both for the KMO and the alpha tests, we generally accepted score levels of 0.5 and above, however for some variables we accepted lower variables for the sake of demonstrating how a linear regression could be made of the hypothesis. This was the case for the variables of control and trust, as both scored lower than 0.5 in the KMO and the alpha test respectively. Moreover, the factor produced with questions representing the variable trust, were below the value of 4.0.
When conducting the linear regressions, we used stepwise regression. This entails adding variables step by step, and checking all candidate variables to test whether their significance changes when adding the variables on to the model. We added our control variables in the following order: age, educational level, gender. Both age and education may be a determining factor for the general awareness about data privacy, so we were interested in identifying whether these control variables themselves were significant.

3.1.2. Qualitative data

3.1.2.1. Empirical data

This study also used secondary data consisting of empirical data in the form of expert interviews, journals, reports, articles and a podcast. These were all important contributors in shaping and validating this study. While the expert interviews have been given a designated section which will be further elaborated, the remaining empirical data sources in the form of the statics and public opinion polls that have been introduced earlier in this report, will be elaborated in the following section.

The European Commission's Eurobarometer on Data Protection looks into people's awareness on data protection as well as their attitudes towards disclosing personal

information online and their perceived control over their data. Since 1973, the Eurobarometer has provided EU member states with surveys on various topics on behalf of the European Commission. The Data Protection survey was conducted a year prior to the GDPR enforcement and designed to support the data protection reform. Thus, the report served as an important insight into the scope of data protection as a topic on the EU agenda and helped set the frame for our study. The most important findings from this report were related to the respondents' opinions on control and disclosure of personal data as well as privacy policies and settings. A majority of 31 percent of the respondents did not feel that they have control over their personal data at all, and 71 percent answered that there is no alternative other than to provide their personal information in order to get access to products and services. Moreover, only 18 percent of the respondents read the entire privacy terms. Over half of the people using social networks have tried to change their privacy settings and the ones that have not done so did not find it necessary or did not know how to do it (European Commission, 2015).

In 2019, Cisco published the report "Consumer Privacy Survey – The growing imperative of getting data privacy right". This survey examined the consumers' experiences and opinions about data privacy, and one of the main findings of this survey was that people do care about data privacy and that many take actions to protect their privacy. This was one of the surveys that inspired this study, as it provided evidence for the fact that data privacy concerns and awareness actually exists among EU-citizens. Another important finding from the survey that paved the way for our study, was that an increasing amount of consumers find it difficult to protect their data and have a hard time figuring out what businesses are using their data for (Cisco 2019). This finding provided grounds for investigating what role controllability plays in protecting ones data privacy on digital platforms. Moreover, the survey found that a majority of 45 percent believed that national governments were primarily responsible for protecting data privacy. This paved the way for our desire to include Danish Data Protection Agency as part of our expert interviews.

In 2018, Deloitte launched the report, "A new era for privacy – GDPR six months" which investigated the effect of GDPR and whether or not the regulation had obtained the desired results for organisations and consumers. The report included a survey on consumers from both EU and non-EU countries and their opinion about GDPR, which was of particular interest to our study. The main finding in the survey was that (19

percent) respondents from EU member states were more sceptical about organisations' intentions when handling their data compared to respondents from non-EU countries (7 percent). However, 44 percent of the respondents felt that organisations cared more about their customers' privacy now that GDPR is in force (Deloitte, 2018). The survey also found that despite the greater transparency that GDPR brings with it, consumers are not necessarily spending more time and dedicating more attention to reading the privacy terms of organisations. 32 percent of the respondents still do not read the privacy terms, with a higher rate from respondents from EU member states compared to those from non-EU countries. This raises an important question of whether being protected by regulation like the GDPR provides a higher sense of trust for the respondents from EU member states, resulting them to avoid reading the privacy terms. This was an interesting insight and thus also inspired our study to further investigate this parameter under which consumers protect their data, through the testing of our hypotheses.

Besides the mentioned reports, we also included articles from among others The Wall Street Journal, Forbes, Tech Crunch, The Washington Post and Wccftech, which all provided insights into the public discussion regarding digital platforms. In addition to these articles, GroupM's podcast, "GroupM Talks", provided valuable insights into the technical aspects of how digital platforms operate and how they collect and process consumer data as part of their business model. We found it important to supply the reports, which mostly represent the consumer opinions, with data from the perspective of the industry of digital platforms. Moreover, the articles and the podcast helped set the direction for our study, as it enabled us in shaping the survey questions in a current and relevant manner.

3.1.2.2. Source criticism

Due to the nature of data privacy being an area that has been discussed vigorously in public debates and thereby also is topic that is subject to politicization, we found it inevitable to devote a separate section that takes a critical look into our data sources.

The European Commission's executive role of proposing new legislation with adoption from the Council and the Parliament is a valid indicator of how the Commission represents the interest of EU-citizens. The Eurobarometer conducted for the Commission is carried out by an independent team of experts, with which it can be

argued that this source is trustworthy in terms of its know-how and that it represents both the industry and consumers. However, while the EU Parliament and the Council play indispensable roles in the EU Commission's work to propose new legislation, the EU Commission as a source can be criticised for not representing the consumers interests isolated, as it inevitably takes a plus sum approach to solving Pan-European issues that also includes the interests of industries as the main economic drivers.

Cisco is a software company that develops, manufactures and sells networking hardware and software as well as other technological products and services, and the company specialises in technical markets, such as IoT and domain security. Therefore, it can be argued that Cisco serves as a trustworthy source in the discussion of data privacy, as it represents extensive know-how on both organisations' and consumers' interaction with organisations through technology. However, the B2B model of Cisco also implies that it represents the organisations to a higher extend than the consumer, as it customers are mainly businesses and not the end-consumer. This may mean that Cisco's interests lies more with the digital platform than with the users of digital platforms, the consumers, and thus make their approach to the survey biased towards the industry (Cisco 2020).

Deloitte is a consultancy which implies that its work is directed towards guiding and advising its clients which represent the industry (Deloitte 2020). However, many of Deloitte's clients are within the government and public service sector, which could also imply that Deloitte indirectly works in favour of the consumers and thus represent their wishes. Thereby, we argue that Deloitte is a trustworthy source for this study.

TechCrunch and Wccftech are both online publishers that specialise in the tech industry and provide news within the sector as well as analyses on emerging technological trends (TechCrunch 2020; Wccftech 2020). While this could imply that these sources represent the tech industry, including digital platforms, and thus rise questions as to its bias towards the industry, TechCrunch as well as Wccftech's articles have proven to be quite objective in their approach of providing analyses from the perspectives of consumers, developers and tech companies alike. For this reason, we argue that both publishers can be considered trustworthy sources.

Many of the same indications are applicable for GroupM's podcast "Digital Beyond Cookies", which analyses the trends within digital marketing and how digital platforms have adapted their business models to the GDPR. The critical analyses and objective

insights raise the trustworthiness of a source that would otherwise imply representation of the digital platform industry.

As far as Washington Post, Forbes and The Wall Street Journal, these are globally acknowledged publishers and provide news and analyses on broader topics such as the general public debates. For this reason they have served as useful and trustworthy sources in the general enlightenment on digital platforms and data privacy.

While we have critically evaluate our sources against their bias either towards the industry or the consumers, it would have been desirable to incorporate reports from consumer organisations. However, for this study we did not find any reports of relevance from consumer organisations.

3.1.2.3. Expert interviews

Prior to construction the survey, we sought to clarify the insight from the theory with current trends anno 2020 regarding data privacy. To do so, we reached out to experts within the field of data privacy and security and digital platforms, that we recon could shed light on how the landscape for how consumer data privacy has evolved since the theoretical literature was published and in the posterity of the GDPR. The expert interviews involved both academic and professional experts from the aforementioned fields. Moreover, we were interested in the opinions and experiences of experts from the digital platform industry, academia and authorities in order to gain more nuanced insights on data privacy and its stakeholders.

3.1.2.3.1. The experts

We conducted an interview with Anette Høyrup who is a Senior Legal Adviser at the Danish Consumer Council. The Danish Consumer Council is *"...an independent consumer organisation that works to promote sustainable and socially responsible consumption and well-functioning markets with the purpose of ensuring consumer rights and making consumers a power factor in the market..."* (Forbrugerrådet Tænk, 2020). Anette was able to provide a point of view from the consumer organisations which lobby to the policymakers on what legal actions should shape the framework for industries when it comes to data privacy. Annette's insights into the role of ownership and responsibility between the consumer and businesses

brought up questions to whether or not consumers should be equipped to and are capable of managing their own data.

The second expert interview which also represented the consumers from an academic point of view, was with Jan Michael Bauer, who is an Associate Professor at Copenhagen Business School, Department of Management, Society and Communication. Jan has been involved with several studies on how the consumer can be tricked into accepting cookie banners by designing them in a certain way. His insights were useful, as he shed light on how the industries operate with the purpose of triggering certain cognitive elements in the consumers to make them act in a certain manner, all while staying within the legal framework. His insights inspired us to incorporate questions regarding terms and conditions and cookie notices, as consumers meet these on an almost daily basis when browsing the internet.

The third and last expert interview we were able to conduct was with Dorte Lundin, Programmatic Lead at GroupM Denmark. GroupM is the biggest digital media agency group in Denmark, which gathers the agencies m/SIX, MediaCom, Mindshare, and Wavemaker. As GroupM has many clients which are digital platforms, such as Ekstrabladet, a Danish news Media, this interview enabled us to represent the challenges that the digital platforms are currently facing. Dorte shed light on how the digital landscape is changing, what challenges the business models at the moment, and how data driven businesses are forced to seek new ways of operating.

3.1.2.3.2. Semi-structured interviews

The expert interviews were all semi-structured interviews that allowed for open answers from the experts, but still maintained the direction for the interview under the main topic which is consumer behaviour on digital platforms (Kvale, 2007). Due to COVID-19 we were only able to conduct three interviews with experts, two of which were over the phone. To ensure that the experts could speak as freely as possible and without feeling restricted, we choose to conduct the interviews with Annette and Dorte in Danish, as this is their mother tongue, and one interview with Jan in English as it was his preference. Prior to conducting the interviews, we had decided that one of us would take the lead and act as the interviewer and the other would take notes and contribute if questions occurred to her.

For each of the interviews we presented ourselves to the experts, the theme of our thesis and why we have chosen them for the interview (Kvale, 2007). Hereafter, we asked for the experts to introduce the specifics of their job position and how they are working with their respective fields of data privacy and digital platforms. We choose the format for semi-structured interviews as this would enable us to ask elaborating questions throughout the interview situation (Kristensen & Hussain, 2016). We developed an interview guide (see Appendix 3) consisting of nine questions relating to the experts opinions and experiences within their fields relating to data privacy and digital platforms. The purpose of these questions were to provide a mini tour of somewhat detailed explanations to our questions (Kristensen & Hussain, 2016). We saw no need for having a grand-tour explanation from the experts, as the purpose of the interviews merely was to uncover trends and possible gaps between what the theoretical literature stipulates and what their reality anno 2020 looks like.

The expert interviews were transcribed after completion, as the analysis of a written text often eases the process of deriving value from the interview instead of working with an audio file (Kristensen & Hussain, 2016). As our study does not seek to investigate any linguistic elements, we chose to transcribe the interview into written language where grammatical errors were corrected. From the transcriptions the reader will find that we have used [...] which means that a word has been inserted (Kristensen & Hussain, 2016), e.g. "*… Good luck with your [thesis]*". In Appendix 4,5 and 6 all three transcribed expert interviews are available. Hereafter the interviews were coded, by both of us, to identify relevant themes and concepts that would be of relevance to cover in the literature review and incorporate into the survey. Concepts uncovered were cookie tracking and consumer conceptualisation on this matter, ITP and ETP in relation to internet browsers, Privacy by design, and consumers valuation of their data privacy.

This study takes an inductive approach to the expert interviews with questions that are aimed at collecting objective data from the experts' experiences and knowledge on the topic. The aim of the expert interview were therefore that the observations made in these interviews would set the basis for the consumer survey questions. By including the insights that the three experts introduced into the survey, we believe that we have provided a more well-rounded survey. Thus, the survey includes a wider range of elements in determining what factors affect consumers' behaviour relating to data privacy on digital platforms. Moreover, by taking an inductive approach to the

expert interviews any personal bias, that we might otherwise have constructed in the survey questions, were minimised (Kvale, 2007).

3.2. Research philosophy

Determining the research philosophy for our study is crucial, as this relates to the development of knowledge and the nature of that knowledge (Saunders et al., 2007). The research philosophy that one adopts contains crucial assumptions about how one view the world, and hence defining the epistemology and ontology is important to ensure that researchers' views and assumptions are aligned (Saunders et al., 2007). Epistemology concerns what constitutes as acceptable knowledge in a field of study (Saunders et al., 2007). The epistemology for this study is positivism, as we seek to test hypotheses in order to explain laws to be assessed (Saunders et al., 2007), which in this study are the reasons for why consumers give up different parts of their data privacy. As we collected our data in the form of a online self-completion survey, we claim to extensively have removed our own feelings and values which is in accordance to the positivist standpoint of data collection, namely being objective (Bryman & Bell, 2011). The positivist paradigm allows us to derive hypotheses from existing theory, tests these and thus conclude how different parameters affect consumers' data privacy concern and whether or not these change the consumers' behaviour on digital platforms.

The ontology of our study is objectivism, which implies that the social phenomenon of data privacy is influenced by external factors such as the GDPR, making it a tangible object that can be measured (Bryman and Bell, 2011). As data privacy is a social phenomenon which is ascribed different values based upon subjective valuation, the GDPR sets what data privacy consists of and hence what we must adhere to in order to secure privacy of data. However, we also acknowledge that total objectivity is not possible to accomplish for this study, as the concept of data privacy described in the GDPR, is grounded on the subjective meaning that consumers derive from it. Hence, as we are interested is investigating what parameters affect consumers' behaviour and as data privacy does not have one explicit definition, total objectivity is not possible. By deriving hypotheses from acknowledged theory and by measuring valid parameters, we believe to have further decreased the level of subjectivity in our

research. Additionally, we also acknowledge and argue that data privacy can be characterised as a latent phenomenon, thus making it difficult to measure entirely objectively. In regards to this argument, we made careful considerations to the design of our research in order to ensure validity in our measurement. This process will be further elaborated in the section 'Validity'.

3.2. Research approach

For this study the use of both qualitative and quantitative data in order to understand our research problem results in the use of Mix Methods (Kristensen & Hussain, 2016). The purpose of using Mix Methods is to create new knowledge that can contribute to creating an understanding of a given problem (Kristensen & Hussain, 2016). We first conducted the qualitative method of semi-structured expert interviews for the purpose of uncovering whether existing theory covers all plausible parameters that influence behaviour, and secondly we conducted the quantitative method of consumer surveys, this study takes on a sequential exploratory research approach (Kristensen & Hussain, 2016). The exploration of this study is evident as there exists a lack of consent between researchers as to what causes the privacy paradox. Additionally, the use of expert interviews to uncover possible undiscovered trends within the field of data privacy supports that this is an exploratory study (Saunders et al., 2007). The Mix Method also enabled us to triangulate our methods of qualitative and quantitative data. By triangulating the semi-structured expert interviews with the quantitative survey data, we were able to nuance our knowledge towards how data privacy on digital performs is perceived by multiple stakeholders and thus enabled us to make a more well-rounded analysis and discuss the parameters that may affect privacy concerns and the privacy paradox. This uncovers how consumers are claiming that they behave on digital platform.

Our research approach for this study, with the survey as our primary data, is a combination of deductive and inductive, as we are testing whether existing theories on the privacy paradox can be validated or not. We did this by constructing a survey in which the questions were based on testing the hypotheses that were presented in the literature review, namely:

H_1: Consumers wish to gain more control over their data for the purpose of protecting their data privacy;
H_2: Consumers value their financial information higher than other types of data and hence would not like to share this, as it is perceived as private;
H_3: Consumers trust digital platforms, because they do not experience consequences of sharing their data;
H_4: Due to inconvenience, consumers tend to allow privacy pop-ups in order to access the content they are seeking without calculating the privacy risks before clicking.

These hypotheses are deducted from the theories presented in the literature review and are formulated to test the potential relationship between consumers' behaviour on digital platforms and their data privacy concerns. The deductive approach is also relatively more used in positivism, which correlates to our research philosophy (Saunders et al., 2007). Robson (2002) presents five stage in which a deductive research will progress (Saunders et al., 2007):

1. Deducing a hypothesis, that tests a causal relationship between two or more variables or concepts, from theory;
2. Expressing how the variables or concepts of the hypothesis relates to each other;
3. Testing the hypothesis;
4. Examining the outcome, as to confirm or deny the hypothesis;
5. If necessary, propose modifications of current theory in the light of the findings.

As the hypotheses were tested against the data collected from consumers' online self-completion survey responses, meaning that we as researchers were not physically present during the observations, we believe to have pursued the principle of scientific rigour (Saunders et al., 2007). However, as we are the ones forming the survey questions and thus providing predetermined statements to determine consumer behaviour and privacy concerns in relation to the Likert scale, we still claim to have obtained scientific rigour, as the statements were deduced from existing theory and the expert interviews.

As, the expert interviews were used to set out the frame of understanding privacy concerns and challenges on digital platforms, we argue to have undertaken an

inductive research for the sake of challenging the current theory. From the expert interviews it was uncovered that consumer knowledge or awareness should be considered as it might affect the privacy paradox. Thus theory should follow data (Saunders et al., 2007). Additionally, the findings from the survey confirmed this, thus presenting itself as an inductive source of data used to answer potential gaps or missing elements in the current research of privacy and consumer behaviour.

3.3. Reliability

The reliability of a study is concerned with whether the results of a study are repeatable, meaning that the study can be reproduced at a later point in time and produce the same results. In practice, this means that the measures in this study, namely consumers' data privacy concerns and their behaviour on digital platforms, should be consistent in order to be reliable (Bryman and Bell, 2011). This was considered when constructing the survey. In our survey, we actively avoided ambiguous or vague question wording due to the fact that the questions may be read differently on different occasions as a result hereof (De Vaus, 2002). Doing so could lead to responses that are unreliable.

To avoid discrimination in the sample, it is important that there is variety in the key variables. Therefore, we asked the respondents about their age, gender and educational level in order to check that the sample was representative to the population. We claim that the survey is representative in terms of gender ratio for the population of the EU, as the majority of the respondents were female (Eurostat, 2020). However, it is important to mention that not all demographics directly represent the overall EU citizens (see 'Descriptive' in the analysis chapter). This study is however still representative of the opinions uncovered for the given survey sample, which represents a group of the overall EU citizen population.

By conducting a consumer survey the level of generalisation is higher than if it only contained qualitative data in form of the expert interviews. Additionally, by sharing the survey across international social networking platforms and different networking groups, we believe that the answers represent a larger sampling size of digital platform users thus enabling an increase in the level of generalisation.

As both of us have engaged in analysing the survey data and in the coding of the expert interviews, we claim that this has further strengthen the reliability of the this

study, as we both have interpreted the empirical data. Thus, possible biases have been minimised through the evaluation of each other's interpretations and resulting in an aligned coding and understanding of the data.

3.4. Validity

The validity of a study is concerned with the integrity of the conclusions generated from a research. The main types of validity that can be distinguished are measurement validity, internal validity, external validity and ecological validity (Bryman and Bell, 2011). Measurement validity is about ensuring that the measures used in a study actually reflect the given concept. This study's approach to address measurement validity was to make sure that the latent concept of data privacy was measurable. First, previous studies on data privacy have shown that data privacy can mean different things to people, both in terms of controllability, valuation and context (Acquisti, 2004; Carrascal et al., 2013; Krasnova et al., 2009). Second, people handle their own data privacy differently. Some people take preventive measures thus being more proactive in protecting their data privacy, i.e. by constraining the amount of data they generate or share when they use digital platforms, or by choosing enhanced privacy technologies, such as internet browsers with intelligent tracking prevention or enhanced tracking prevention over other internet browsers that do not provide these technologies. Other consumers take more reactive measures to protecting their data privacy, by configuration the privacy settings on their IoT devices or mobile phones. These findings support the fact that data privacy can be characterized as a latent concept, which indicates that it is difficult to measure if not entirely unmeasurable. In order to ensure measurement validity of this latent concept, our approach was to measure the latent concept by implying a certain understanding of data privacy. This was done by making a predetermined definition which the respondents' answers were measured against. The predetermined definition was embedded in the construction of questions with answer options, allowing the respondents the opportunity to express their opinion openly but still within the direction of the predetermined definition.

The internal validity is related to the causal relationship between to variables and whether it can be validated that, if x causes y, then x is also responsible for variations

in y. In this study, we addressed the internal validity in connection to the causal relationship between respondents' data privacy concerns and their intended behaviour on digital platforms, which was tested against the parameters of convenience, trust and risk. Another internal factor that was not included was the respondents' intended behaviour versus their actual behaviour on digital platforms, i.e. his or her behaviour being in exact accordance to what he or she responded in the survey. Due to the design of our study, which does not include an experimental part, we were unable to test the causality between our respondents' intended behaviour versus their actual behaviour. Thus, the internal validity of our survey has a deficiency in terms of relying solely on the variable of intended behaviour. This limitation will be further elaborated in the section 'Limitations'. The focus of our study is therefore to uncover the causality between the underlying parameters of the respondents' behaviour on digital platforms and to their demand for strengthened data privacy. This was done by asking questions relating to their behaviour in order to test the hypotheses against the parameters that influence their data protection behaviour. These behavioural questions were then followed by questions as to why the respondents behave the way they do on digital platforms. These questions of why were either guided by answer options or elaboration fields where the respondents could write their own answers. Thus, we were able to test if e.g. trust or lack thereof was a dominant influencer for data privacy protecting behaviour.

The external validity of our findings face challenges due to the fact that our limited resources inhibited us from obtaining the desired generalisability of our sampling. This will also be elaborated in the section "Limitations". The unnaturalness of having to answer a survey can imply limited ecological validity (Bryman and Bell, 2011). Our approach to this challenge was to introduce our survey with a few words on topic and duration of the survey and mention that answers are anonymised. Moreover, we timed our survey to be launched at a time when most people were home in connection with lock-down in several countries due to COVID-19, and potentially resulted in more invested responses.

3.5. Limitations

While the research of this study has been carefully designed to provide the most reliable results, limitations are present. First, the time frame of this study did not allow for the desired extensive research on data privacy. The most optimal research design would be to also conduct an experimental design, in which participants first respond to the survey of this study for the sake of uncovering what they say about their behaviour on digital platforms (their intended behaviour), e.g. whether or not they read through the terms and conditions. The second step would then be to conduct an experiment on the respondents and investigate how they actually behave on digital platforms. Monitoring the respondents online browsing behaviour over a longer period of time would have provided us with enough data to control if the behaviour that the respondents claimed to perform corresponds to their actual behaviour. Simultaneously with the observations, it would have been interesting to test the respondents' perceived knowledge about data privacy versus their actual knowledge. As we cannot guarantee that the respondents actually know what they claim to know, semi-structured interviews with the respondents could have revealed their true level of knowledge. If we were to ask them about their knowledge, we could not guarantee the objectiveness of their answer and thus it would not be valid to rely on these answers solely. Therefore the most optimal process would be to conduct additional semi-structured interviews with the survey respondents, and hereafter monitor their online browsing behaviour, as this would allow us to test their actual knowledge about data privacy and examine the causality between knowledge and behaviour. This experimental design would allow us to be able to identify the variables of intended versus actual behaviour, as well as perceived versus actual knowledge. Due to limited resources and time, we were unable to take on an experiment of this size, but refer to this option, should this study be replicated at any point.

Second, we acknowledge the limitations related to the results from our survey. In order to ensure a higher response rate, we refrained from asking the respondents about their nationality as another demographic question, as the amount of questions and the matrix Likert-scale question already were extensive and as we saw no need to single out any EU member state for the analysis. However, due to this choice and due to the fact that we posted the survey on international networking platforms, we are unable to

fully guarantee that all of our respondents are EU-citizens. We sought to accommodate this challenge by emphasising in the survey title, introduction and attached post on the platform that the survey was aimed at EU-citizens only.

Additionally, in the context of the results of the survey are limitations related to culture. According to Edward T. Hall's theory on cultural contexts, the communication in low context cultures is more direct whereas the communication in high context cultures is more indirect. This may have affected the level of disclosure in the respondents' answers in terms of e.g. honesty about behaviour on digital platforms or knowledge about data privacy. Moreover, institutional frameworks such as national data regulation can also affect people's trust and awareness about data privacy in digital platforms, and thus cause variety in the respondents' answers. This variety may have affected the reliability of the findings, as these would potentially not be representative for all EU-citizens equally but differ from country to country (Patil, Lu, Saunders, Potoglou & Robinson, 2016). However, as we seek to uncover what parameters determined when and what data consumers are willing share, we do not believe that incorporating national or cultural dimensions was of relevance.

Fourth, another limitation is related to the research design can be found in the measurability of the overall topic and concept of data privacy. It can be argued that data privacy is a latent concept which does not correspond to an objectivist ontology. However, although we argue that the concept can be measured with offset in a predetermined definition of data privacy, we acknowledge that data privacy could also be examined from the ontological position of constructionism. We believe this would be an option for further qualitative research, as data privacy may be a social phenomenon which can be shaped by public debate in different cultural and social settings. Here it must also be recognised, that since we test the correlation between consumers behaviour and privacy concerns, in form of a survey, we must regard the responses as true and equal to their actual behaviour. However, when asked about one's knowledge to a complex and difficult theme as data privacy, we cannot know for sure that when the consumer claim that they know what a cookie is, that they fully know how a cookie works, and what the difference is of certain types of cookies. If this were to be determined, there would be a need for asking the respondents elaborating

questions to test if they really know what they claim. This was not possible due to limited resources and time.

Fifth, for the expert interviews we were not able to conduct an interview with the Danish Data Protection Agency due to COVID-19 and their own limited time for thesis interviews. Thus, it was not possible for us to include expert knowledge from the authorities' view and fulfil a fully representation of consumers, the industry and the authorities.

Lastly, as mentioned under 'Reliability', the survey does not show strong direct resemblance of the broader class of the EU age ratio nor the educational level obtained, because the majority of our survey respondents are 21-30 years old (Eurostat, 2018) and the majority of the respondents hold a university degree (European Commission, n.d.). These findings present a limitation in terms of the direct representability of our survey in comparison to the divisions between EU citizen. It would have been preferred to obtain a larger sampling of respondents in the older age ranges and with a lower educational level than university degree, as this would have entails a generalisability to the broader class of EU citizens.

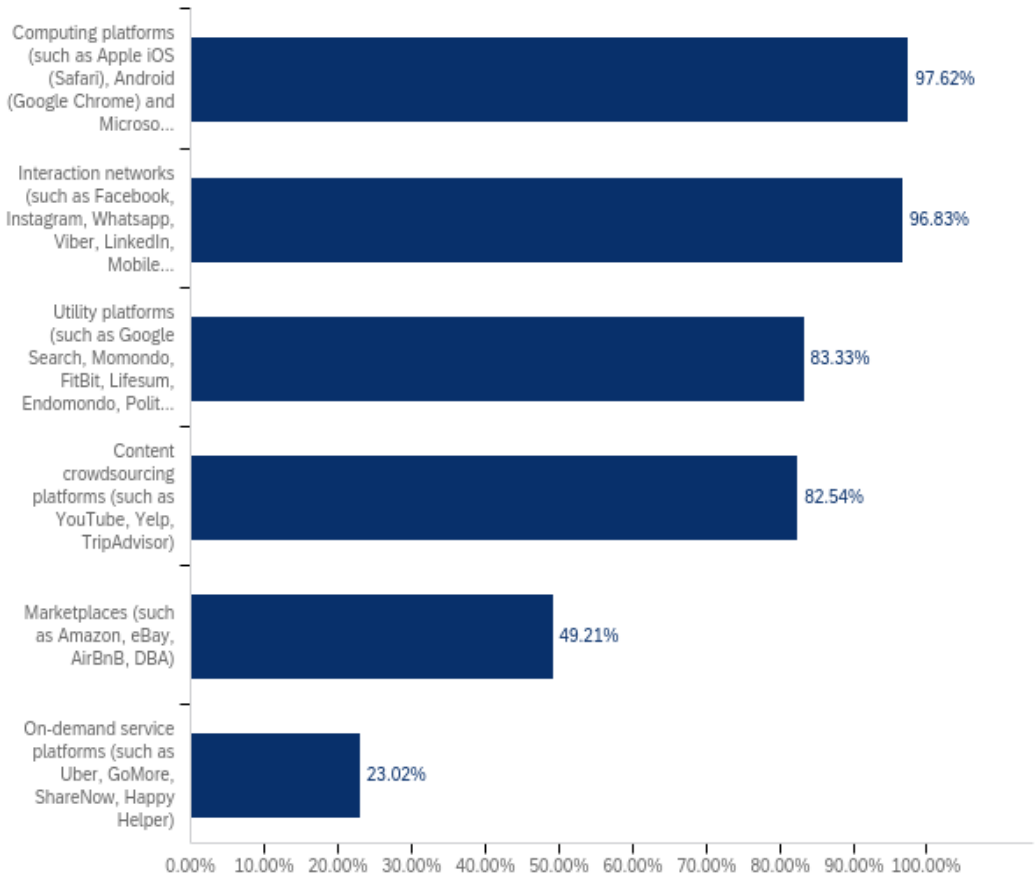
4. Analysis

Previous studies have pointed towards different reasons, as to why a privacy paradox emerges when people advocate for strengthened data privacy protection. Based on the theories presented in the literature review, we have set out four hypotheses for data privacy concerns, which were tested in the survey. The hypotheses can be broadly linked to three parameters that the literature review presented as interfering with the privacy paradox, namely trust, convenience and risk (Brown, 2001). Before we dive into the testing of hypotheses, each parameter is worth introducing as well as how each differs from the others. While convenience is more obviously separable from the remaining two parameters, risk and trust have proven to be more intertwined. Theories point towards the fact that consumers' privacy concerns derive from a lack of trust in the security measures on digital platforms, as it is a highly technical and complex matter to comprehend. Consumers thus associate increased risks when they,

in some instances, feel forced to give up some of their personal information for the sake of continuing to a site or making a transaction. The fears related to these risks could be the loss of once privacy or damage either social or physically. Lastly, convenience is essentially the reason for why the internet was invented. We save time, efforts, money etc. by conducting our shopping online, by applying for jobs online, or by obtaining knowledge online. The literature stipulates that these three parameters directly affect consumers' privacy concerns.

4.1. The consumers' most used digital platforms

On the basis of the survey we can establish that our respondents are largely present on a variety digital platforms, varying from computing platforms to interaction networks and marketplaces. On a monthly basis, the respondents of the survey used all the types of digital platforms that were presented to them (Hunt, 2016). Computing platforms, interaction networks, utility platforms and content crowdsourcing platforms are the four platform types that more than 80 percent of the respondents use monthly.



Appendix 7, question 4 – "Of the following digital platforms, please indicate the platforms you use on a monthly basis: (you can choose more than one)"

Computing platforms are understood as platforms that allow for interaction between the platform users and third-party developers such as Apple's iOS, Google's Android systems and Microsoft's Windows (Hunt, 2016). The interaction between the platform's users and its developers appears through app stores or marketplaces where recommendations, feedback and monetisation of apps take place. 97.62 percent of the respondents stated that they make use of computing platforms on a monthly basis. This could be explained as most consumers own a smartphone or a computer which are most likely products of Apple (the iPhone or Mac), an Android phone or computers that run on Microsoft's software. Computing platforms are embedded in most consumers' digital equipment, hence the majority of our respondents answered that they use this type of platform.

Second and with almost as many percentage, are interaction networks with 96.83 percent of the response rate. Interaction networks are platforms that facilitate interaction between consumers and businesses and can take shape of a message, voice call, image or money transfer (Hunt, 2016). These platforms, such as Facebook, Instagram, WhatsApp, MobilePay and Slack, the respondents stated to use heavily on a monthly basis. Something could indicate that the majority of consumers use this types of digital platform for the purpose of establishing a solid channel of interaction with their family, friends, colleagues and acquaintances.

As both utility platforms and content crowdsourcing platforms amounted to almost the same percentage, these also stood out as they also succeed 80 percent in response rate. Utility platforms are often identified as 'free' service where the platform users attracts businesses and not the other way around (Hunt, 2016). Examples of utility platforms are Google Search, Momondo, Fitbit and Ekstrabladet, as these attract users with their offering of 'free' services, such as Google search, who then attracts businesses that display ads when the consumer searches for content on Google search. The distinction here is that users go to Google search to search for content (it is the primary goal), not to see ads. 83.33 percent of the respondents stated that they use utility platforms on a monthly basis, which could indicate that consumers might be favouring the 'free' services that digital platforms can offer, which are perceived as free as there is no involvement of money. Carrascal et al. (2013) stipulated that consumers find it difficult to understand the extents to which data driven businesses collect the users data when they make use of their platform, as a payment instead of

money. Perhaps consumers might not be aware of the extends to which their data is collected as payment in the trade of a ‘free’ service. However, it is also important to acknowledge that consumers could be well aware of the extents of data collecting and might approve of this. The factors of awareness and personal limits are crucial if approval of data sharing explains why a vast majority of consumers make use of ‘free’ services.

Additionally, 82.54 percent of the respondents stated that they use content crowdsourcing platforms on a monthly basis. This type of platform collects large sets of content from a group of users and share this with a wider base of the platforms users (Hunt, 2016). YouTube, Yelp and TripAdvisor are all content crowdsourcing platforms. Content crowdsourcing platforms differ from interaction networks, as the platform users interact with the platform and the interaction is anchored in the content and not in specific accounts as on interaction networks (Hunt, 2016).

The vast majority of responses in the four above mentioned platforms, could suggest that the consumers’ primary goal of their digital platform usage is to nurture their relations with other people and to obtain content relevant to them. The division between the responses given in Appendix 7, question 4 did not come as a surprise, as they reflect very well why consumers engage in online activities (European Commission b, 2019).

On the other hand, it was quite interesting that marketplace and on-demand service platforms, were the platforms that the respondents stated that they make the least use of on a monthly basis. Marketplace and on-demand service platforms are often linked to the trade of services for money, as the offerings on these often entail a purchase. This finding is interesting as the majority of the respondents make use of digital platforms (computing platforms, interaction networks, utility platforms and content crowdsourcing platforms) where the service most often entail a trade-off between a ‘free’ service for data and not money. This could indicate, based on the respondents’ behaviour, that they value their money higher or see a higher risk associated with conducting payment activities online, compared to using a ‘free’ service in exchange for data. Thus, consumers might prefer free services over payment services. A possible explanation could be found in the fact that data as an intangible asset is harder for the consumer to grasp, thus making it difficult to rationally valuate one’s data and therefore the consumers might adopt a ‘see what happens’ attitude when

they trade with their data (Brown, 2001). If this is the case, consumers might be subject to the immediate gratification bias (Acquisti, 2004), as no immediate consequences are experienced and only benefits are received from the platforms.

4.2. Parameters

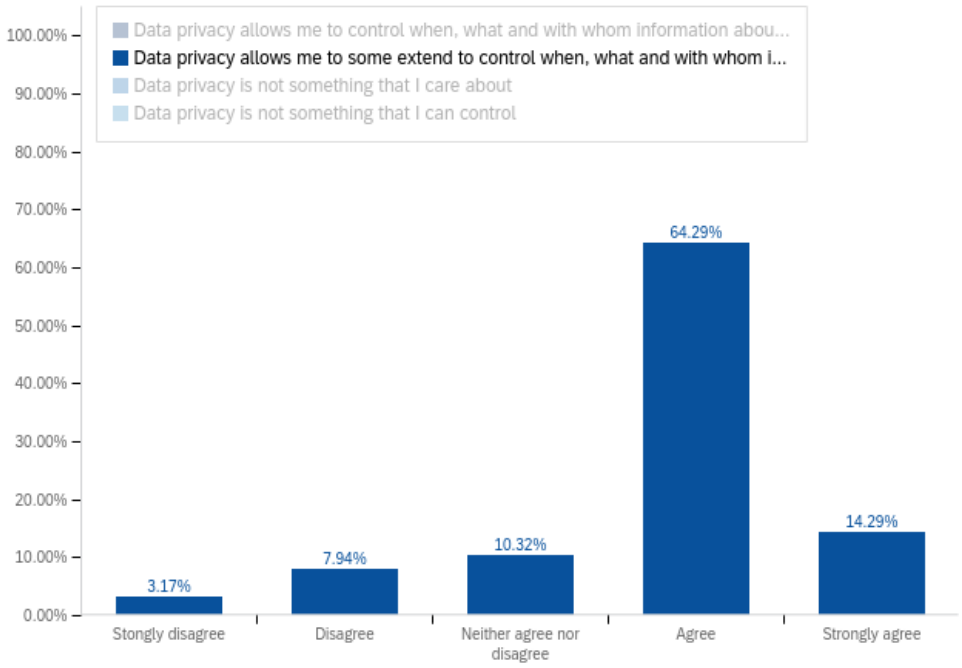
From our survey, we found that our respondents data privacy concerns is influenced by all three parameters of trust, risk and convenience. However, we also came to discover that consumers' level of awareness is yet another and crucial parameter that calls for elaboration. Theories do mention awareness as a factor of influence when it comes to people's privacy concerns, however no theory has solely investigated this parameter in relation to the privacy paradox, and even though researchers have introduced awareness as a possible solution to the privacy paradox, many of them stipulate that more research on this parameter is needed. The findings from our survey thus entail that awareness as a fourth parameter would be of relevance to include in this study. On these grounds the following sections will present this study's findings on how people's data privacy concerns are influenced under the four parameters of trust, convenience, risk and awareness.

4.2.1. Trust

To determine whether or not trust plays a role in how people behave on digital platforms, we asked the respondents several questions related to trust.

In question 6, we found that 34.13 agreed and 25.40 strongly agreed with the statement: "I do not trust how my data is currently being handled". Clearly, more than half of this respondents group do not trust the current data collection, sharing, storing and processing. To determine whether the lack of trust is linked directly to the digital platforms, we asked them in questions 10, whether or not they trust digital platform with their data. Here, we found that a majority of 41.33 percent of the respondents agreed with the statement. Thus, it can be derived that this respondents group does not trust digital platforms with their data.

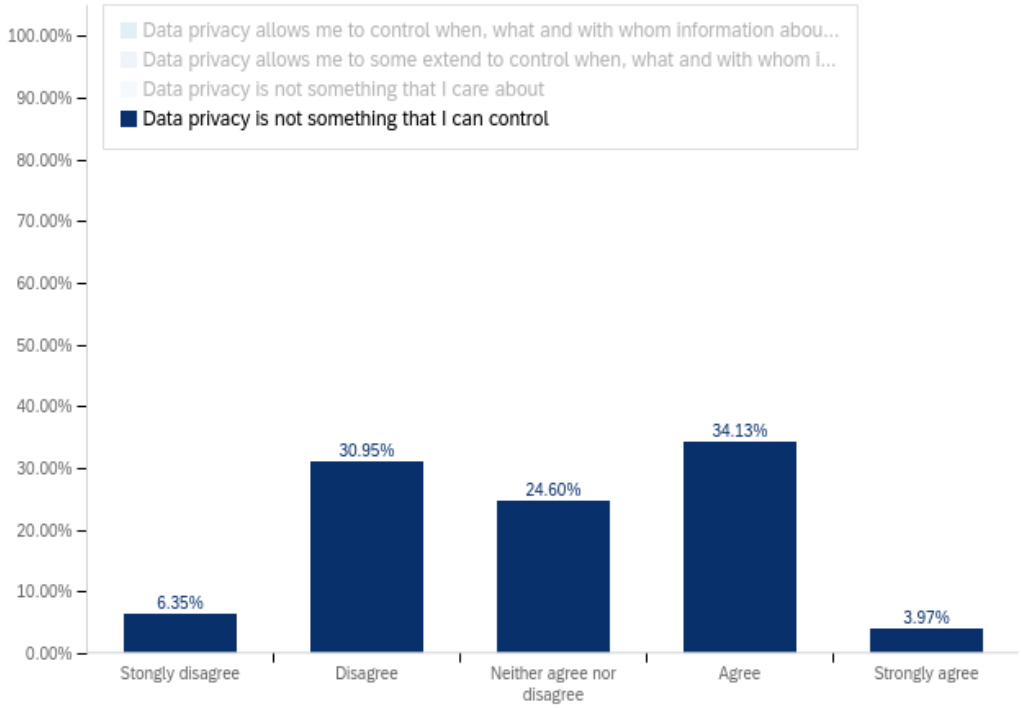
Some of the survey questions were also linked to having control over data, as it can be argued that a wish for more control over one's personal data indicates some degree of mistrust from the consumers. If there exists no mistrust, it can be argued that it is not as relevant to demand more control over one's personal data, and the desire for more control might not be as evident as expressed by consumers. When asked in question 5, how the respondents understand the concept of data privacy, a majority of 64.29 percent answered that data privacy allows them to some extent to control when, what and with whom information about them is being shared.



Appendix 7, question 5 – "How do you understand the concept of data privacy?"

This could suggest that the respondents do not feel that data privacy equals complete control over personal data. This discovery is quite interesting as it could suggest that consumers have adopted the premise of using digital platforms, i.e. you are not in full control of your data. This premise corresponds the aforementioned statistics stating that more than 80 percent of EU citizens feel that they only have partial or no control over their data privacy (European Commission, 2015). By being in full control, we differentiate between providing data that you are fully aware that you are providing (static information) versus the data you generate, that is used for profiling your online behaviour and your preferences, which you might not be aware of (dynamic information) (Wang et al. 1998). Businesses often analyse your data for the purpose of profiling you and your whereabouts and this is what we identify as the data that the consumer is not fully aware of is being generated.

From question 5, it was additionally uncovered that there are almost as many respondents that believe that they cannot control their data privacy, namely 34.13 percent, compared to 30.95 percent respondents that believe they can.



Appendix 7, question 5 – "How do you understand the concept of data privacy?"

These response rates could indicate that the respondents have adopted the mentioned premise because they for unknown reasons find it acceptable. The 34.13 of the respondents that believe they cannot control their data privacy, might be completely fine with not having full control over their data. However, linked to consumers' increasing wish to gain more control, this wish could entail just having more control than they currently possess. The majority of the respondents are buying the premise of not being in full control. Linking this to the trading of data for 'free' services, consumers might accept the premise, while also being subject to the immediate gratification bias (Acquisti, 2004), as mentioned earlier.

Based on the above mentioned arguments, we can thus only partially confirm our hypothesis: *H3: Consumers trust digital platforms, because they do not experience consequences of sharing their data*. Our respondent group clearly state that they do not trust how their data is being handled and that they do not trust the digital platforms with their data. Consumers might experience a lack of current control over their data privacy, however as they experience more benefits than consequences, possibly due

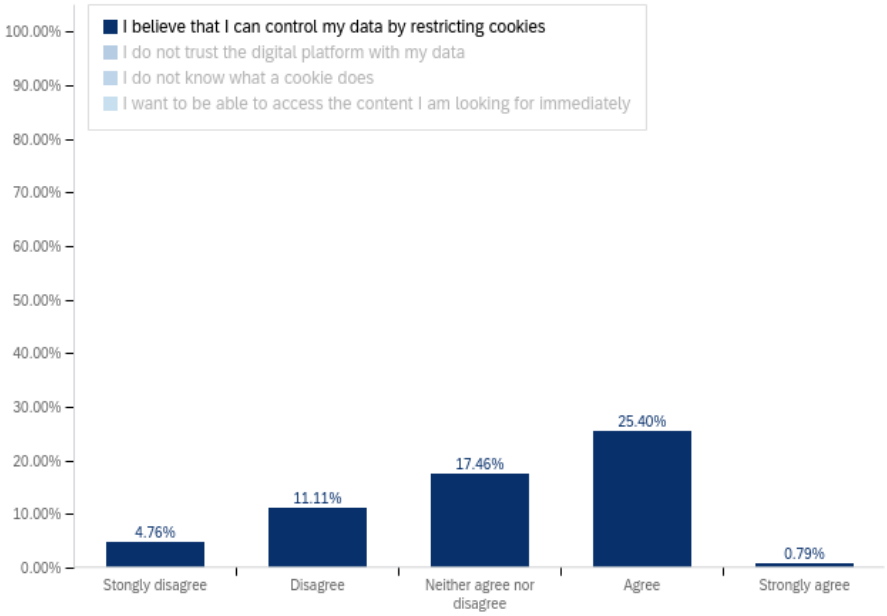
to the immediate gratification bias, they are still sharing their data with digital platforms. We can therefore not conclude that the lack of experiencing consequences increases the level of trust that consumers place in digital platforms. Our findings indicate that trust does not increase if consumers do not experience consequences of sharing their data. Hence, we must assume that trust increases on the basis of other factors.
One could argue that not much has changed the consumers' opinion on their data privacy since the launch of the GDPR, as 80 percent of EU citizens stated back in 2015 that they only felt like they had partial or no control over their online data (European Commission, 2015). Has the GDPR truly given consumers more rights or does the lack of change indicate that consumers have become more informed of data technologies and practices in general, hence making them continuously feel only partially in control of their online data?

Moreover, elaborating further on question 5 we also found that 45.24 percent of the respondents disagreed with the statement that they do not care about their data privacy. Hence, data privacy is something that the consumer might not need to have full control over, however it is a topic on which they seek to continuously care about. As Appendix 7, question 5 visualises, there is only a small majority that believes that they cannot control their data privacy (34.13 percent) compared to those that believe they can (30.95 percent). The small difference between 'agree' and 'disagree' makes us question if consumers believe in their own ability to control their data (Ölander and Thøgersen, 1995)? One could derive from the small majority, that either these respondents do not believe that it is truly possible to have control over their data, either due to hostility from the industries and lack of regulation, or because they simply do not know how to act in order to gain more control over such an intangible asset as data. Of the minor group of 30.95 that stated that they believe that they can control their data privacy, we cannot conclude if these have bought the premise of not being in full control. However, it can be argued that they believe that they can do something, just not to which degree or what such measures consist of.

When the respondents were asked in question 10 why they restrict cookies, a majority of 42.67 percent answered that they believe they can control their data by doing so. The second highest amount of respondents, namely 41.33 percent, answered that they do not trust the digital platforms with their data. These findings could indicate that

consumers take active measures towards protecting their privacy by restricting their cookies one way or the other, as a means of gaining control over their data because they do not place trust in digital platforms. This is supported by the results from question 17 in which respondents are asked if they believe digital platforms are doing enough to protect their data privacy. Here, 57.18 percent answered that digital platforms could do more to protect the consumer's data privacy and 23.02 percent answered that they do not do enough to protect the consumers. Hence we can determine that consumers do not place trust in digital platforms regarding sharing their data with these.

Another interesting finding was that even though the majority of the respondents stated that they believe that by restricting the use of cookies they can control their data, an almost as large amount of respondents stated that they 'neither agree nor disagree' with restricting cookies as a way of controlling their data.

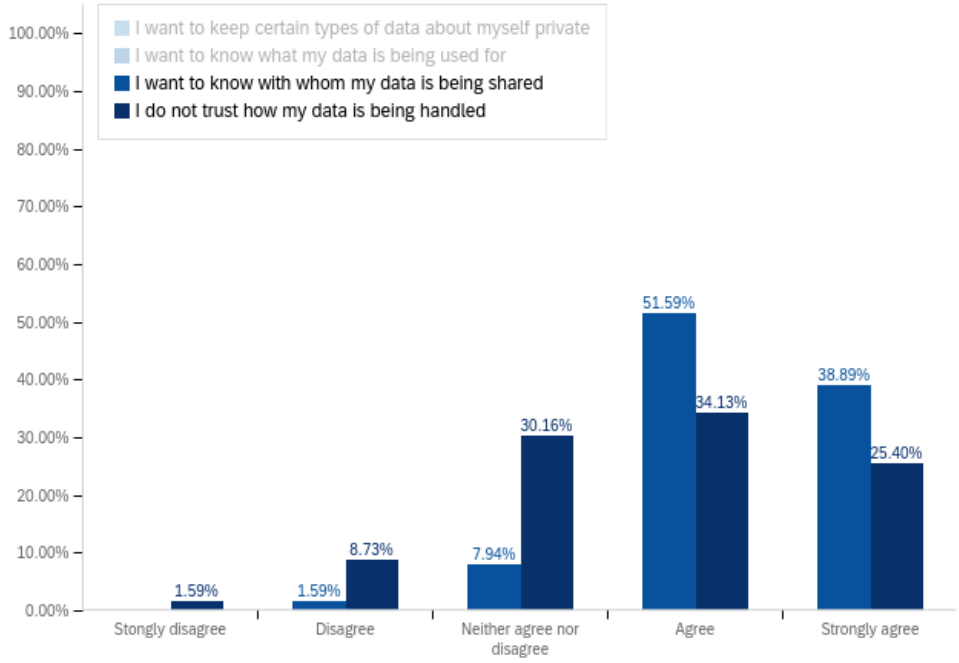


Appendix 7, question 10 – "If you restrict the use of cookies, please indicate why"

A plausible explanation to why we received such a large group of 'neither agree nor disagree', could be due to consumers not believing that restricting the use of cookies will make much of a difference in the overall picture of gaining control over their data. The consumers' mistrust to businesses and digital platforms could be linked to them having the idea that even though they restrict the use of cookies, businesses will find a way around this issue and find new ways of harvesting their data. Perhaps

consumers' mistrust organisations to such a degree that even if the businesses obtained their data illegally, the consumer would not know how to hold the businesses responsible. It can be argued that because the respondents do not find that digital platforms are doing enough to protect their data privacy, people place less trust in them and thus they desire more control over their own data. On these grounds, we can confirm the existence of the hypothesis: *H_1: Consumers wish to gain more control over their data for the purpose of protecting their data privacy*. As presented, several of our questions conclude that our respondents wish for more control in terms of; knowing what data they are sharing, whom they are sharing the data with, for what purpose their data are being used, and that measures they are taking in their online activity such as restricting cookies, are for the purpose of protecting their data privacy.

Additionally, our findings also revealed that the willingness to share personal data is connected to the relationship between the receiver of their data and the consumer (Norberg et al. 2007), and the purpose of data usage. In question 6, we asked our respondents why data privacy is important to them.

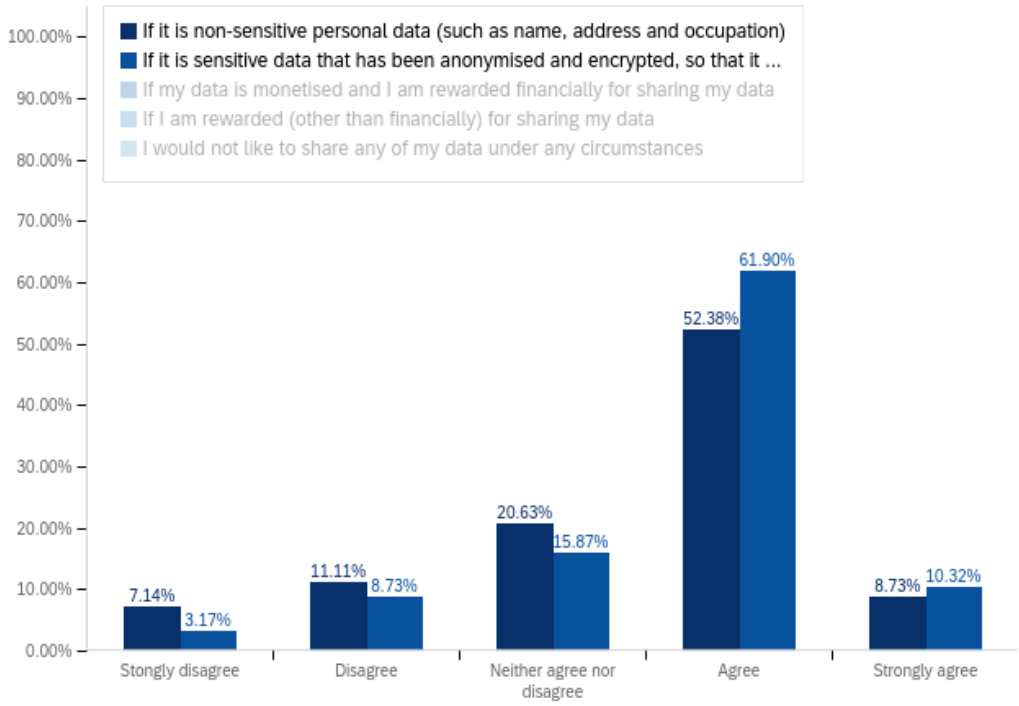


Appendix 7, question 6 – "Data privacy on digital platforms is important to me because:"

51.59 percent answered that they want to know with whom their data is being shared. This could suggest that people do not trust their data with parties of whom they have no knowledge about or prior experience with. As presented in the literature review,

research has stipulated that trust in relationships is a direct influencer of whether one is willing to disclose information or not (Norberg et al., 2007). Our finding support this claim, as 34.13 percent of the respondents stated that they do not trust how their data is currently being handled. Trust is simply not present for half of the survey respondents, which could indicate a unwillingness to provide data. It is relevant to question whether the current privacy measures condoned by the industry is enough for the consumer? Is there a need for e.g. specifying who the third party is, when the consumer is to decide whether or not he or she should allow cookies? Would the consumer find it easier to determine if one should allow or deny cookies, if all the companies that make up third-parties are listed? Some cookie notices do list who their third-parties are, however it requires that the consumer navigates through a difficult path of buttons to access this list, however not all companies provide this though. Additionally, we could ask ourselves whether the consumer would give up more data if the purpose of use were to be elaborated? Research has proven that lack of sufficient information can keep us in habituation, thus making it more difficult for the consumer to continuously re-evaluate the trust relationship between themselves and the digital platforms (Ölander and Thøgersen, 1995). These questions are relevant to ask in order to understand why consumers seek the answers of to whom and why they should share their data. As a majority of the respondents do not trust how their data is being handled, another large part of 30.16 percent stated that they neither agree nor disagree. This could suggest that the respondents have not yet determined on what basis trust to the digital platforms is built or given any thoughts about whether they should be concerned or not. A possible explanation could be found in the lack of knowledge about the topic, as presented earlier from Böhme & Köpsell (2010). Due to lack of understanding and interest in one's data privacy or because of habituation of their online behaviour, the respondents simply have not given this much thought. Habituation (Böhme & Köpsell, 2010) is something that individuals rarely are aware of and identifying the impact of habituation in a situation regarding one's data privacy might be even harder to alter.

When the respondents were asked in question 14 under which circumstances they would be willing to share their data, 61.90 percent answered that they would share sensitive data that has been anonymised and encrypted, so that it cannot be linked to their identity.



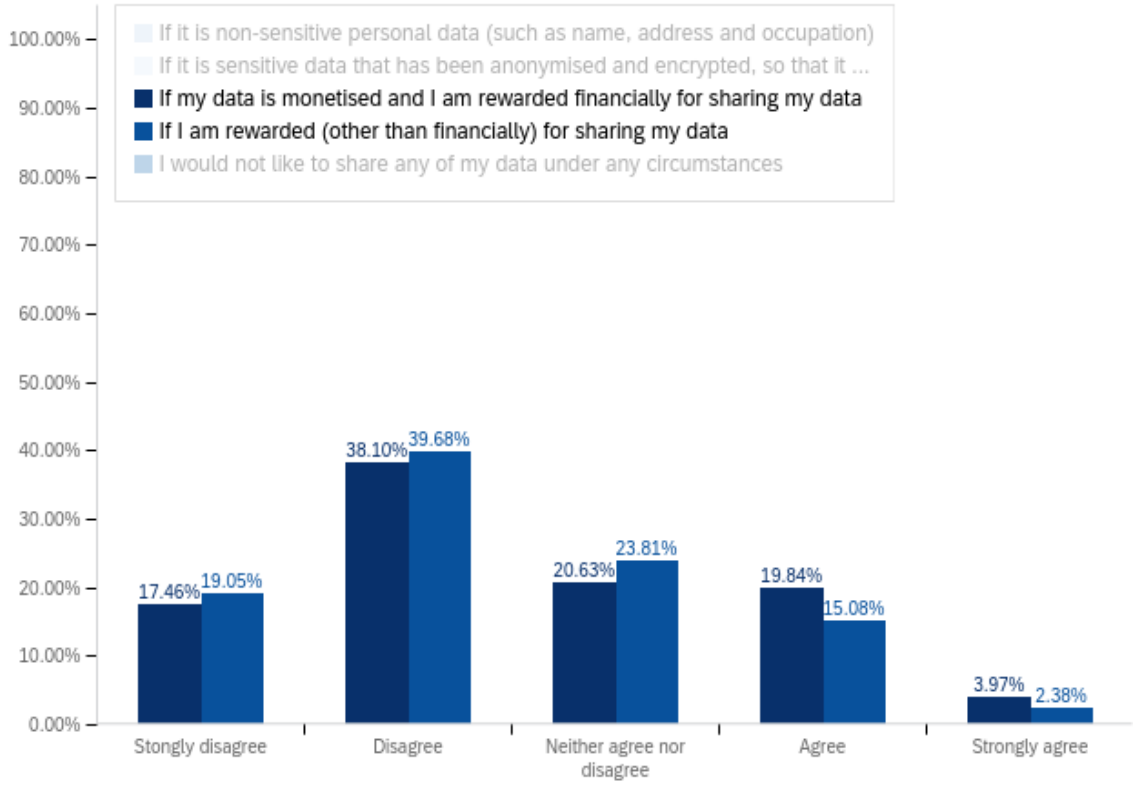
Appendix 7, question 14 – "Please indicate under which circumstances, you would be willing to share your data"

This finding poses an important question for interpretation. How come the majority of consumers seem to be ready to go beyond sharing basic non-sensitive personal data and instead prefer sharing sensitive personal data that has been anonymised and encrypted? It could be argued that consumers' desire for more protection of their data privacy makes them want to be completely anonymous and thus obtain the highest imaginable degree of privacy, i.e. not being an identifiable individual. However, from this question it is crucial to distinguish that there exists a difference between anonymised and encrypted data, and that we gathered two quite different data protection methods under the same statement in question 14.

Anonymised data excludes personal identifiers such as your name, age, zip code, birthday etc. However, the data in the form of the content you produce is still accessible and readable to everyone. The produced content such as a message thread from a platform is still readable, however no one knows who the owners of the conversation are. Encryption on the other hand is a form of hidden language that requires a key to decode in order for it to be readable. This entails that all personal identifiers and the content produced is hidden for the reader unless one has the encryption key to decode the encrypted content. All letters might be replaced by symbols or numbers, thus making it impossible to understand or derive meaning from

it. When introducing anonymization and encryption it is crucial to include that these methods can also be implemented to different degrees. You can remove all personal identifiers or just a few, or encrypt to a certain extend. These distinctions may or may not have been obvious to the respondents when they answered neither agree nor disagree. However, as over 60 percent of respondents answered that they see anonymization and encryption as the best possible way to protect one's data - from the choices given to them - we cannot identify if the respondents see both methods a equally protective or if one is preferred more over the other. Either way, consumers prefer these measures over other measures.

As the literature stipulates that consumers tend to be more willing to share their data for the trade-off of money or non-financial rewards (Carrascal et al, 2013) we wished to investigate if this is also true. However, we have come to find that this does not correlate to what our survey revealed. The majority of our respondents stated in question 14, that even if their data is monetised and they are either financially and non-financially rewarded, this will not convince them to share their data.



Appendix 7, question 14 – "Please indicate under which circumstances, you would be willing to share your data"

Furthermore, a large group also stated that they 'neither agree nor disagree' with the two statements. Hence, we could interpret that wanting to monetise their data could be determined by evaluating the type of data and the platform. However, it is also important to recognise that the intention-behaviour gap (Sniehotta et al., 2005) might play a role here as well. Perhaps, to the 'neither agree nor disagree' respondents the cost and benefits of protecting their privacy differs depending on the context (Acquisti, 2004). One respondent clearly stated in question 15: "*I will only share my data if the trade-off is relevant to me*" (Appendix 7, question 15). The context of the trading between data for 'free' service is hence of importance. Another explanation can be found in the amount of value that the digital platforms provide to the consumers. The trade of data for that specific 'free' service might be beneficial enough in itself. Not only do the respondents hesitate to share their data for any monetisation rewards, they also want to know the purpose. When asked in question 15 to elaborate why they are not willing to share their personal data, some of the most repeated words were "purpose" and "reason" (Appendix 7, question 15). If people do not know for what purpose their data is being used, they tend to be less willing to share it. If consumers are not provided with sufficient information of the reasons for obtaining their data, they will not break out of their current habituation of data sharing and suddenly begin a new behaviour of sharing more than they are currently doing (Ölander and Thøgersen, 1995). Thus the previous finding of consumers not trusting digital platforms stands, however certain individual evaluations of the context and possible gain can affect consumer to share their data.

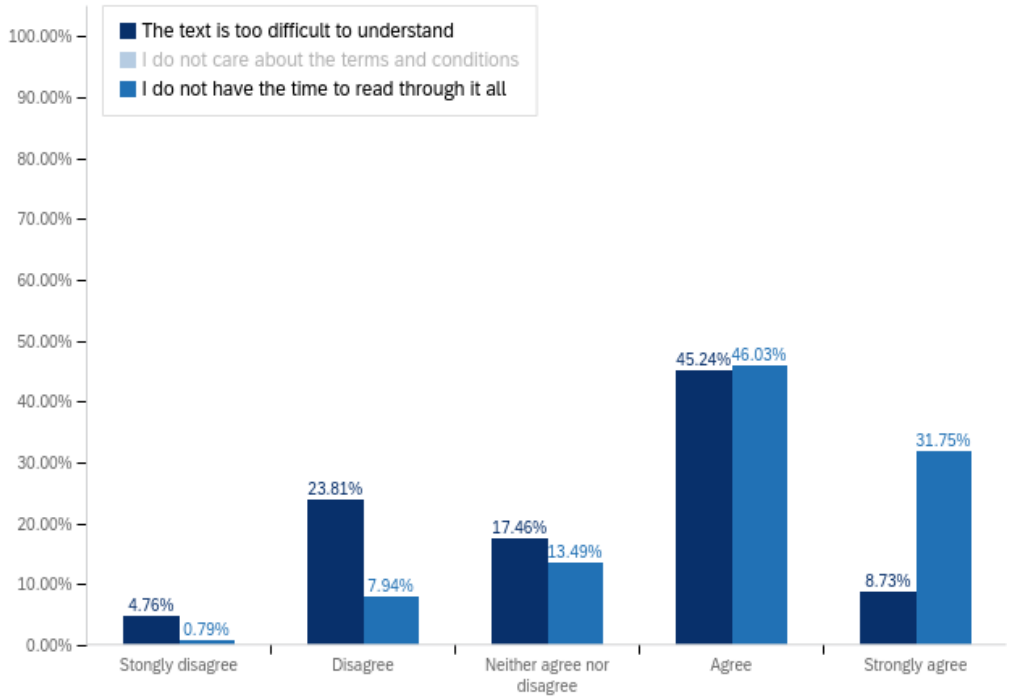
4.2.1.1. Subconclusion

When analysing how trust as a parameter influences consumers' behaviour on digital platforms, we can conclude that our respondents link trust to the degree of control over their data. We found that consumers link the restriction of cookies and protective measures to control, which suggests that there is a need for control. Therefore, we were able to confirm *H_1: Consumers wish to gain more control over their data for the purpose of protecting their data privacy*. The majority of our respondents feels that they only have somewhat control over their data privacy. However, our findings suggest that consumers have bought the premise for using digital platforms, i.e. one is not in full control over their data. Moreover, we were able to only partially confirm

H_3: Consumers trust digital platforms, because they do not experience consequences of sharing their data. Our respondents stated that they do not trust digital platforms, however they do still share their data. Additionally, we found that low levels of trust is related to unfamiliar relationships, which could explain why respondents prefer to have their data anonymised or encrypted before sharing it. Additionally, the respondents also stated that no rewards, neither financial or non-financial, will make them share their data, only a valid purpose will.

4.2.2. Convenience

While data protection can be implemented in various ways, these all have one thing in common: they are time consuming for the consumer to conduct. Our findings strongly suggest that consumers refrain from devoting their full attention to the content of terms and conditions. This was reflected in question 7, where the respondents were asked whether they read the terms and conditions if it pops up when using a digital platform. The highest response rates were seen in the statement: “I always read through the whole thing”, where 66.67 percent ‘strongly disagreed’. This finding is remarkable in itself, as the use of extremes such as ‘strongly disagree’ and ‘strongly agree’ are generally rarely used by respondents in Likert scales (Albaum & Murphy, 1988). Hence, we must interpret this as a strong indicator that consumers consequently do not read through the full content of terms and conditions. In the following question 8, the respondents were asked to indicate why they do not read terms and conditions.

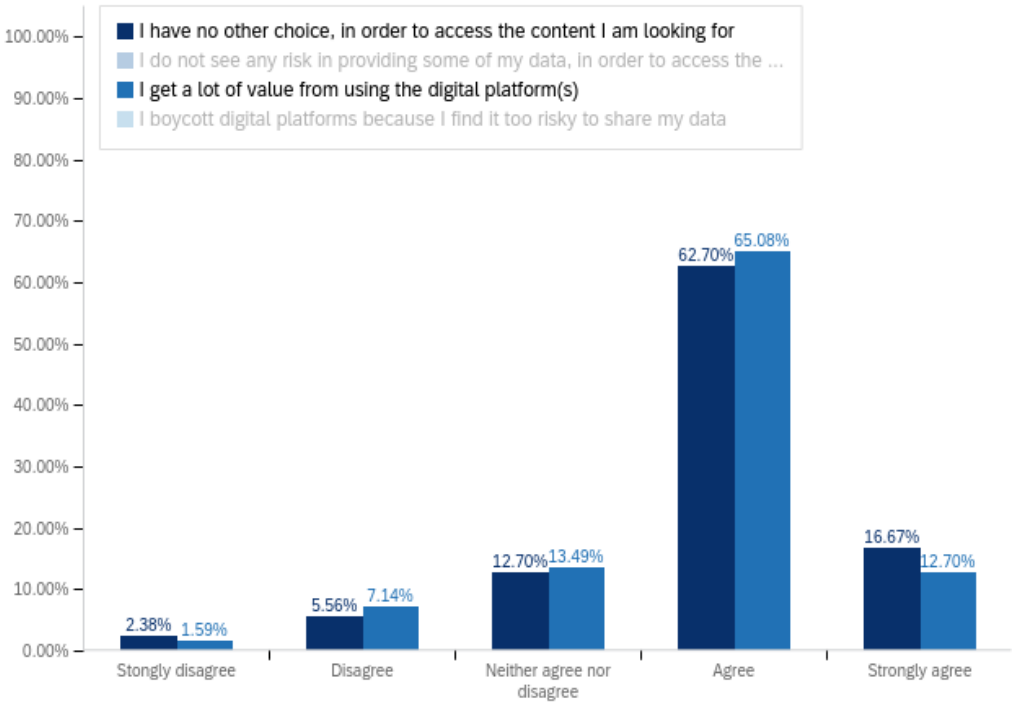


Appendix 7, question 8 – "If you do not read the entire terms and conditions, please indicate why:"

46.03 percent answered that they do not have the time to read through it all and 45.24 percent stated that the text is too difficult to understand. This supports the literatures stipulation about the two key elements of convenience: namely time and effort (Jiang et al., 2013). The respondents do not seek to place the requested amount of time it takes to read terms and conditions texts, nor place the efforts it takes in trying to comprehend what the text states. Our respondents group thus correlate with the literature's stipulation: consumers value the saving of time and effort the highest when they are online (Jiang et al., 2013).

However, a majority of 50.79 percent disagreed with the statement "I do not care about the terms and conditions", which could indicate that people's lack of attention towards the digital platform's privacy terms is not a result of being careless, but merely because the text is either too difficult to understand or too time consuming to read. Either way poses as inconveniences to people. It could be argued that even though terms and conditions is a legal text that stipulates the rights of the different parties involved, it is problematic that only a limited group of people is able to read and fully comprehend its meaning. This constitutes a barrier that should be addressed, as the legal term is directed towards a target group that is too narrow, namely juridical individuals and not the actual target group.

Convenience also interferes when people disclose their personal information. When the respondents were asked in question 11, if they provided any of their data on digital platforms and why, a majority of 65.08 percent answered that they do so, because they receive a lot of value from using the digital platforms. However, 62.70 percent felt that they had no other choice in order to access the content they are looking for.



Appendix 7, question 11 – "Do you provide any of your data online on digital platforms? Please indicate why:"

This could suggests that the primary reason for disclosing one's personal information might be voluntary, as doing so brings an extensive amount of value to the respondents. However, even though it might be voluntary, consumers still feel that they do not have any other choice, but have the consumers tried not to e.g. allow cookies and then see if they could access the content? A small experiment like this might be inconvenient or too time consuming for the consumer to even try out for themselves. In some instances, the choice of 'do not allow cookies' in a cookie notice blocks the access to the platform, however on some platforms they do not. However, on the basis of the response rate we can argue that inconvenience in testing different methods for gaining more control, might play a dominant role in consumers online behaviour. On these grounds, we can confirm the hypothesis *H4: Due to*

inconvenience, consumers tend to allow privacy pop-ups in order to access the content they are seeking without calculating the privacy risks before clicking.

For the purpose of simplification and recognition we introduced the concept of terms and conditions pop-up windows and cookie notifications to the respondents, as both are common concepts that meet the consumers when they make use of digital platforms. Especially, cookie notifications are useful in this study as they also make up a part of the GDPR, hence digital platforms are by law expected to notify the user of how they collect data. However, the mentioning of cookies in GDPR is referred to as a grey zone.

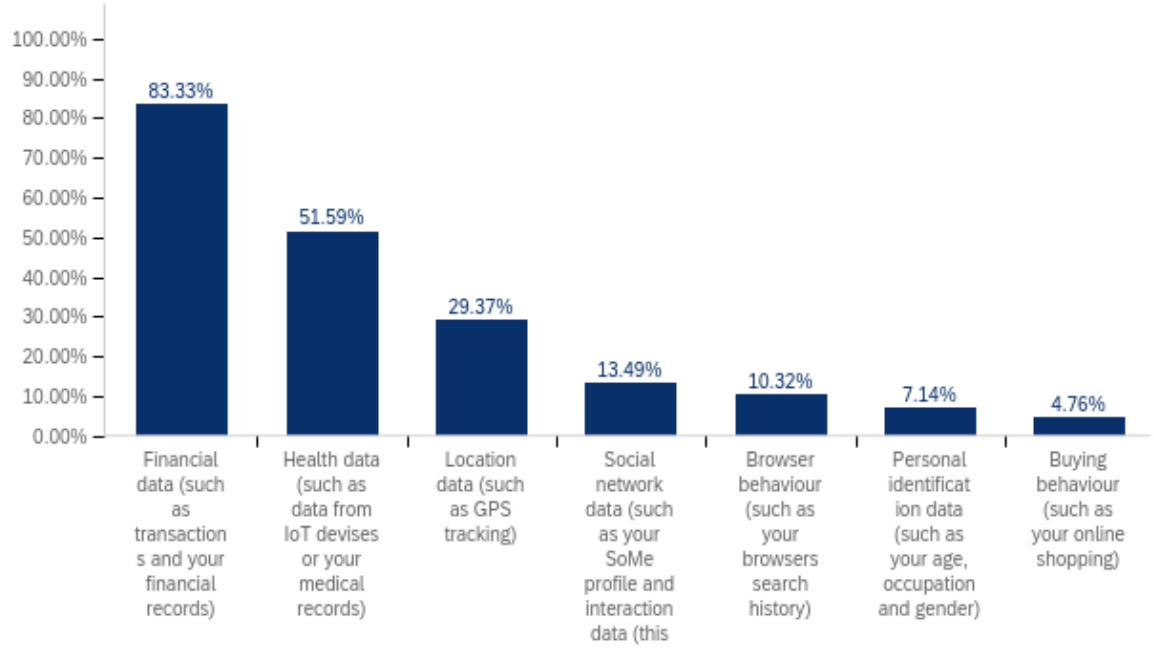
4.2.2.1. Subconclusion

When considering convenience as a parameter for consumers' behaviour on digital platforms, we found that respondents clearly stated that they find it too time consuming and difficult to read and understand the entire terms and conditions. This correlates to what theory states, namely that saving time and effort is valued the highest when consumers are online. On these grounds we were able to confirm *H_4: Due to inconvenience, consumers tend to allow privacy pop-ups in order to access the content they are seeking without calculating the privacy risks before clicking*.

4.2.3. Risk

Despite the indications that the parameter of risk is closely connected to the two other parameters of trust and convenience, we found it appropriate to devote a separate section that elaborates how risk itself influences consumer behaviour on digital platforms. Our survey revealed that people attribute different levels of risk to different types of personal data, which can indicate that certain types of data are valued higher than others (Kokolakis, 2015; Carrascal et al., 2013; Phelps et al., 2000; Norberg et al., 2007). When asked in question 12 which types of data they would least like to share online, a majority of 41.67 percent responded their financial data. Thus our findings support, as the literature also stipulates, that financial track records and money transactions are data types that consumers value the highest in terms of keeping these private from others. Second and third most valued types of data that

the consumers would least like to share, are respectively their health data (51.59 percent) and then their location data (29.37 percent).



Appendix 7, question 12 – "Please indicate what types of data listed below, you would least like to share online"

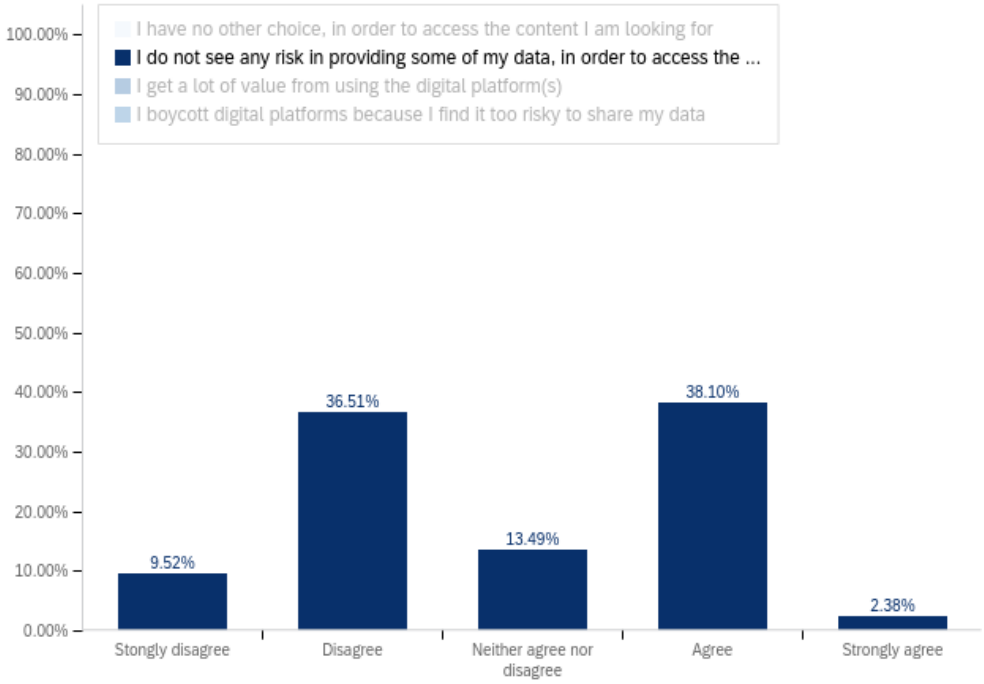
Besides financial data as the primary data type, our findings further correlate with what the literature stipulates i.e. that health data is also being valued high (Kokolakis, 2015; Mothersbaugh et al., 2012). Mothersbaugh et al. (2012) concluded from their study that health data is highly valued to the consumer due to the degree of sensitivity and risks associated to disclosing it to others. A possible explanation to why the respondents value their health data to such a high extent could be found in the sensibility of this type of information, or as it has come forward recently in the media, an individual's health data can be exploited by his or her employer or by the insurance company. Instances has surfaced were insurance companies offer insurances based upon people's health data and alter their life insurances based upon life expectancy, and not on overall metrics (Chen, 2018). In question 13, some of the respondents stated their concerns about sharing health data: *"... health data I am afraid will be used to deny me access to certain services ...*", "*I heard about a woman who couldn't get a loan in her bank because they had obtained her health data which stated that she once had a depression ...*" and a third: "*I fear that sharing health data could have a strong impact on my life, e.g. affect insurance coverage*" (Appendix 7, question 13).

Consumers thus associate risks with disclosing sensitive information about themselves as this can result in losses of material kind (Mothersbaugh et al., 2012).
However, location data with its almost 30 percent response rate, was a surprising finding. Despite the increase in IoT devices, which are known for their extensive location tracking mechanisms (O´Dea, 2020), location data is the third least type of data that the respondents wish to share. A possible explanation can be found in an increased awareness on the consumer side, as a direct response to Apple's iOS 13 software update, which introduced regular pop-up windows on devices stating how regularly an app has tracked one's location within a given period of time. Hence, consumers are currently becoming increasingly aware of how their IoT devices and mobile phone apps can track their whereabouts. Additionally, linking this finding to the previous mentioned incentive of knowing what the purpose of sharing ones data is, it appears to be difficult to justify the need for location data if the service that the digital platform provides is not built around location identification, as in the case of platforms like Uber, Happn or Google Maps.
The respondents' browser behaviour, personal identification data and buying behaviour were the data types that they are the least concerned with sharing. Norberg et al.'s (2007) findings which show that consumers are more willing to disclose their media usage and product consumption, may provide a possible explanation to our findings. Consumers may not be as concerned with sharing data from their browser and buying behaviour, perhaps because they have experienced benefits related to sharing these, such as personalized targeting or offers.

In the following question 13, the respondents were asked to elaborate why they would be concerned with sharing the types of data that they would least like to share. Here, some of the repeated words were "personal", "sensitive" and "private", where several respondents expressed that these data types were not something they wanted to be public to other people. A general comment is that the respondents fear that their data can be exploited or get in the wrong hands and be used against them. Something could suggest that the respondents' concerns with sharing personal data is linked to the threats these face if disclosed (Kokolakis, 2015). Moreover, the word "misuse" was mentioned in connection to financial data being misused for fraudulent purposes. Our finding thus show that our respondents are more concerned with their territorial, personal and informational privacy (Holvast, 1993, Rosenberg, 1992), as location,

financial and health data received the three highest response rates. Consumers hence associate risks to sharing their data, as they fear misuse of their most personal and sensitive data. On these grounds, we can confirm the hypothesis *H_2: Consumers value their financial information higher than other types of data and hence would not like to share this, as it is perceived as private*.

Furthermore, as the graph of question 11 indicates, the respondents are divided in terms of how much risk they attribute to digital platforms.

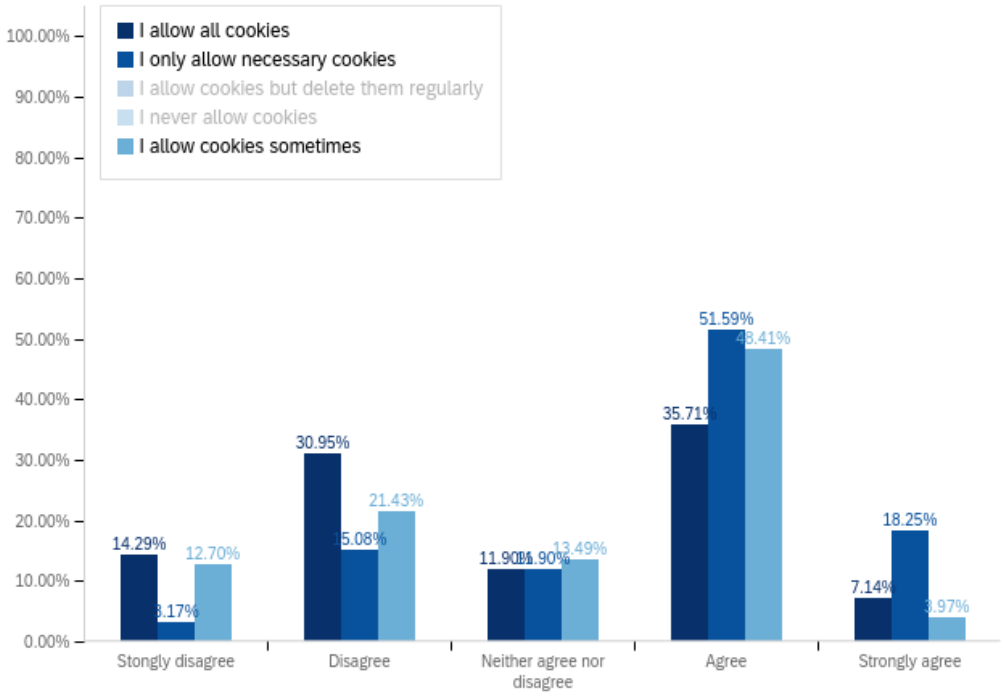


Appendix 7, question 11 – "Do you provide any of your data online on digital platforms? Please indicate why:"

The amount of respondents who see no risks in providing some of their data on digital platforms (38.19 percent) is only slightly larger than the group who identify risks (36.51 percent). Due to lack of time and resources it was not possible for us to uncover what these risks consists of, or if the respondents see risks differing from platform to platform. This would be of interest to determine, should risk as a parameter be further investigated. However, we can concluded that half of our respondents may have accepted the premise of trading their data for a digital platform service, whereas the other half is sceptical and might not approve this trade-off. Either because the trade-offs are not clear to them or because the risks associated with trading are not high enough for them to boycott the platform completely. Here it is important to keep in mind that the group that associates risk might not have boycotted the platform,

however we cannot exclude that they have not taken any other measures to minimize their data generation on these platforms. The question also offered the option of answering “I boycott digital platforms because I find it too risky to share my data” in order to identify how big a role risk plays in the decision to provide personal data. This answer had the third highest overall response rate of 46.03 percent strongly disagreeing, which indicates that while there seems to be more or less voluntary reasons for providing personal data on digital platforms, an active decision of boycotting the platforms for the sake of privacy is not one of them. This observation is quite interesting as it could indicate that the value consumers receive from the digital platforms exceeds the perceived risk of using them, thus resulting in consumers not boycotting the platform entirely. However, there is also a distinction to be made here, namely to reduce or to boycott. These are two very different measures for protecting ones data privacy and our formulation of the question: “I boycott digital platforms because I find it too risky to share my data” can be said to present an extreme measure, which not many people are willing to take. Thus, as mentioned earlier, it could have been interesting to investigate to what extent consumers reduce their use of a platform if they see risks associated with using them.

Additionally, we also found that when asked in question 9 whether our respondents allow cookies when browsing on the internet in general, they were divided in terms of whether or not they allow all cookies, where of 35.71 percent leaned towards agreeing with this statement. Moreover, a majority of 51.59 percent agreed to only allowing necessary cookies and 48.41 percent agreed to allowing cookies sometimes.

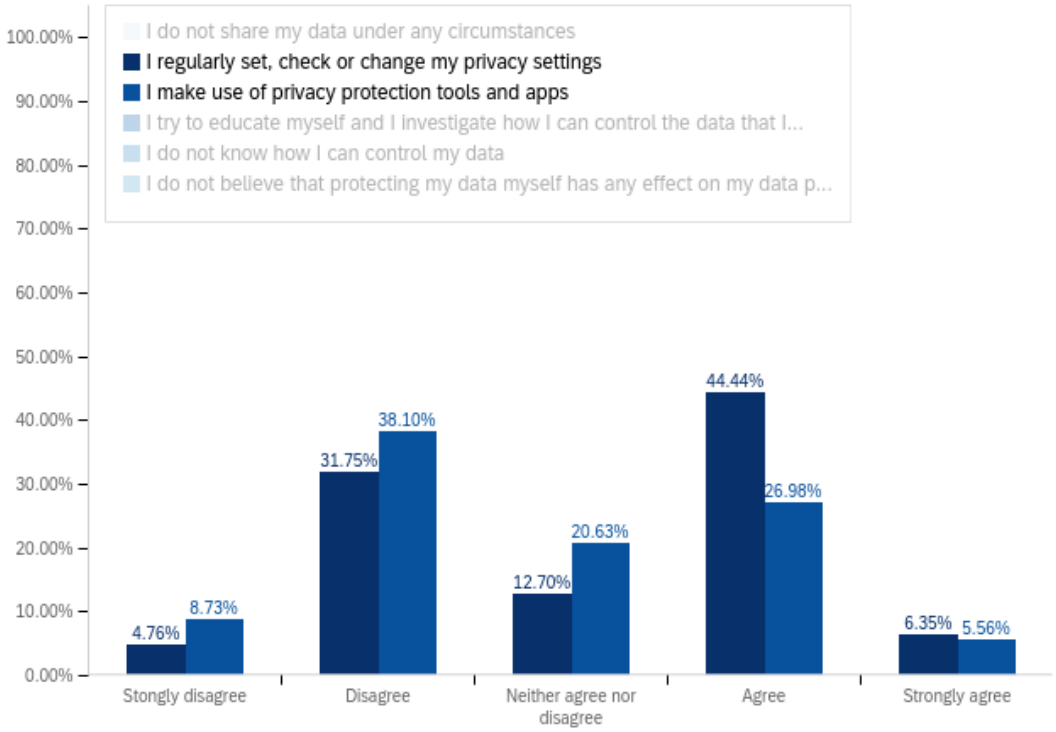


Appendix 7, question 9 – "Do you allow cookies when you browse on the internet in general?"

However, it is important to remember that the option of choices in the cookie notice design is not always displayed, as mentioned in the literature review. Hence, we also asked the respondents if they allow cookies but regularly delete them again. Hereby, the majority of the respondents either 'disagreed' or 'strongly disagreed' with this method. From the question: "I allow cookies sometimes", a vast majority stated that they sometimes do allow cookies. There can be more explanations as to why this is. One possible explanation could be that the consumer is aware of what kind of cookies they will allow or on what digital platforms they are willing to share their data, hence their cookie preferences differ from platform to platform based on reasonable considerations. Another explanation might be that consumers' choices to deny or allow cookies are somewhat random and depended on the context the individual finds itself in, e.g. being in a hurry, being attentive etc. A third possible explanation could be that the consumers' habituations are determined by the design of the cookie notice. Egelman et al.'s (2008) study on habituation could explain why the consumers could be habituated by the cookie notice design.

These findings may indicate that people do attribute some risk to allowing cookies and therefore take active measures to protecting their privacy by restricting cookies. This can also explain why a relatively smaller amount of 35.71 percent allow all cookies.

In question 16, 44.44 percent of the respondents answered that they regularly set, check or change their privacy settings, while only 26.98 percent agreed to making use of privacy protection tools and apps.



Appendix 7, question 16 – "How do you protect your data?"

33.33 percent answered that they try to educate themselves and investigate how they can control the data they generate. These findings could indicate that people do take active measures in trying to protect their data privacy either proactively or actively, which correlates to what the literature stipulates (Krasnova et al., 2009), as it may minimise the perceived risks. However, what is left unanswered is why people choose certain methods of data protection over others, and whether this is related to risk or convenience. It can be argued that changing privacy settings (Krasnova et al., 2009) is a more convenient method than using privacy protection apps and tools, as the latter would require the active behaviour of downloading the app, which demands time and effort. Privacy settings on a given digital platform are somewhat more at hand and available for the user, while simultaneously offering the ability to use the platform. The answer may lie in another underlying and not as evident parameter of the consumer's awareness about what is actually the safest method in the given situation.

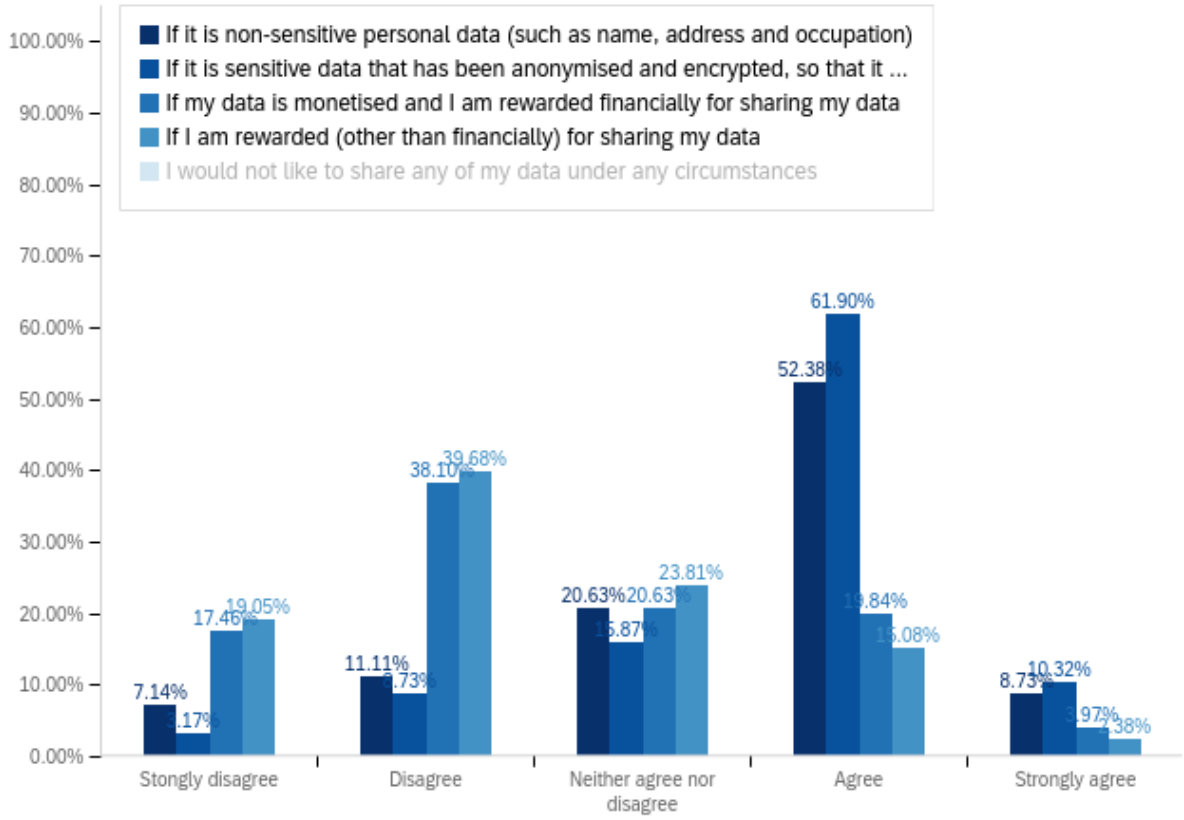
4.2.3.1. Subconclusion

To sum up, our findings showed that the parameter of risk has a direct impact on consumers unwillingness to share their financial data. We were also able to confirm *H_2: Consumers value their financial information higher than other types of data and hence would not like to share this, as it is perceived as private*. The main reason for this is the sensibility of disclosing this type of information and its associated risks. The risks relate to fear of misuse and exploitation, e.g. in cases of fraudulence. Overall, the risks that consumers associated with using digital platforms do not seem to exceed the value they receive. We are able to conclude this as no respondents were willing to go as far as to boycotting a digital platform.

4.2.4. Awareness

From our survey, we were able to establish that people are generally aware of how using digital platforms may compromise their privacy. When asked in question 9 whether or not they allow cookies when browsing online, a majority of 51.59 percent answered that they only allow necessary cookies, which could indicate that they are aware of how doing so, to some extent, can protect their privacy. However, in question 16 when asked how they protect their privacy, 30.16 percent agreed that they do not know how they can control their data, compared to 28.57 percent who disagreed with this statement. This might indicate that while people are aware of how they can protect their privacy by restricting their use of cookies, another large group of respondents are still not entirely sure about how they can control their data, as this would otherwise have resulted in a higher disagreement rate. We were not able to determine if this was linked to a lack of belief in cookie restrictions as a privacy measure. Nevertheless, we cannot deny that there is a need for consumers to be educated about the different measures they can take in order to protect their privacy online.

Moreover, question 14 investigated under which circumstances consumers would be willing to share their data. Our findings showed a higher response rates of ‘neither agree or disagree’ for all five statements we presented, compared to the remaining survey questions.

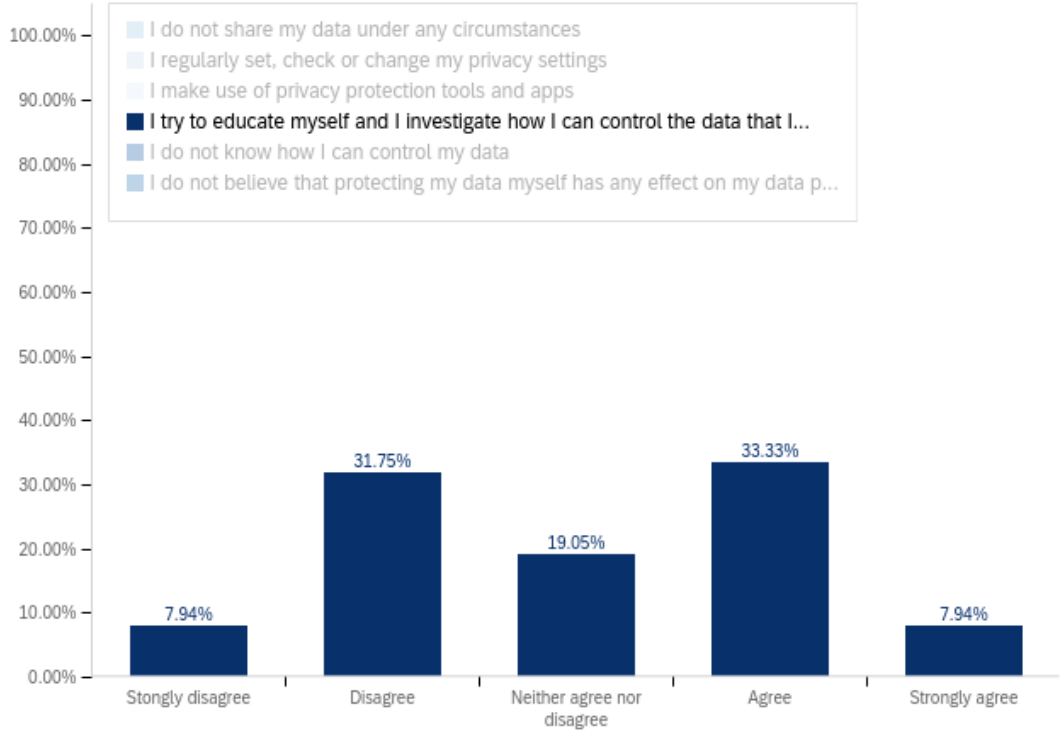


Appendix 7, question 14 – "Please indicate under which circumstances ´, you would be willing to share your data"

These results might suggest that the respondents have not decided under which circumstances they are willing to share their data and with whom, which could be connected to the possible explanation that people are not entirely sure how exactly to protect their data privacy. These findings also suggest that the respondents have adopted a 'see what happens' attitude (Brown, 2001), as questioned earlier. As privacy is a subjective and individually interpreted concept, while also being extremely complicated to navigate through in a digital age, consumers might operate with an individual evaluation of each privacy matter they are faced with, instead of adopting general guidelines to what they will agree to or not. Have consumers even made up their minds about what privacy means to them and how or even to what extents they should protect it?

Besides the frequency of allowing cookies we also asked for what reasons the respondents would restrict the use of cookies, in order to determine how important they view the cookie notice in protecting their data privacy. 32 percent of the respondents stated that they know what a cookie does, hence claiming that they also

know how it can protect their data. This response rate is not that high compared to the fact that cookie notices are something that the consumers meet on a daily or weekly basis, when using digital platforms. This percentage could indicate that consumers do not really comprehend how easily they can begin to protect their data, with an understanding of the use of cookies. 21.33 percent of the respondents clearly admitted that they do not know what a cookies does, which further supports this argument. If the consumers' perceived self-efficiency, namely their belief in their own capabilities to protect their own data privacy, is not present, they will never begin to investigate how to take active measures (Sniehotta et al., 2004). Hence, as consumers find data protection complex and intangible, while not having experienced any invasion of privacy yet, status quo of not fully understanding privacy protection tools could remain.

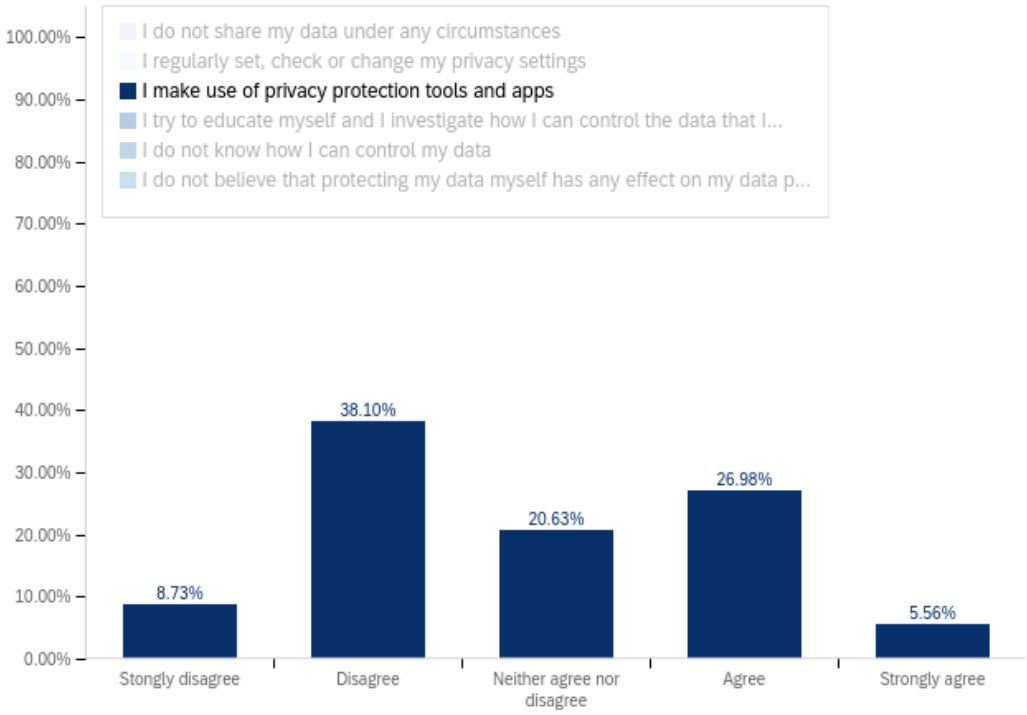


Appendix 7, question 16 – "How do you protect your data?"

From question 16, only a small majority of the respondents stated that they seek to educate themselves about how to better protect their privacy. As mentioned earlier, data privacy can be a subjective concept and it can be difficult to comprehend in depth how technologies affect data privacy, as technology is evolving fast. Why the respondents are so divided in terms of educating oneself could suggests that consumers wish to keep up with the technological trends and seek to be informed. It

could be argued that consumers try to engage in action control (Sniehotta et al., 2004) however somewhere between self-monitoring, awareness of standards, and the efforts demanded, they are lost and they do not succeed in implementing their intentions of taking new measures to protecting their data privacy (Norberg et al., 2007). Perhaps, some consumers might also have come to the realisation that protecting themselves from intrusion of their privacy is unavoidable and therefore they do not adopt a strict privacy protection measure (Acquisti, 2004).

Another finding from question 16, showed that a majority of 38.10 percent disagreed with using privacy protection tools and apps to protect their privacy.



Appendix 7, question 16 – "How do you protect your data?"

This finding suggests that applications such as using certain browsers, downloading extensions (such as the add blocker for the Chrome browser) and apps, is something that the consumers do not necessarily place much trust or benefit in. This belief could possibly be due to the fact that many of the privacy protection tools do not necessarily decrease the amount of data that is provided or generated. Take for example the adblocker from the Chrome browser, it only blocks the adds that are visible, however they are still there if the ad block is turned off. This entails that the data is shared and analysed and on these grounds the user receives personalised ads, but the user has merely chosen not to have these ads displayed or aired on his or her browser. This is

often how privacy protection tools work. Some privacy protection tools minimise or simply do not track or log any behaviour on the platforms. However, most commonly the user is either reminded about the data that he or she is sharing or is able to block the marketing incentives forwarded. This finding suggests that the respondents might be aware of this and understand that privacy protection tools do not necessarily result in one becoming more private.

Additionally it was found in question 11, that 62.70 percent agreed that they share their data because they believe they have no other choice if they wish to access the content they are looking for. This observation is quite interesting, as the GDPR is put into force for the purpose of making sure that the consumers have a choice and that they have the possibility to practice the right to privacy, also online. These responses could suggest that consumers are not familiar with how the GDPR translates into their daily life and what tools they can use to become more private. Moreover, these findings could indicate a possible lack of faith in the GDPR, regardless of whether the consumers understand the GDPR or not, as the consumer feels subject to condone with how the organisations are playing the game and do not know how to enforce GDPR themselves.

4.2.4.1. Subconclusion

When investigating how awareness as a parameter affects consumers' behaviour on digital platforms, we found that consumers have not made up their minds as to under which circumstances they wish to share their data. Moreover, we found that a larger percentage than expected does not know what a cookie does. As consumers face cookies daily and interact with these, their lack of knowledge supports the need for better public awareness on data protection. Our findings also showed that the lack of consumer awareness around the complexity of data protection, results in consumers not protecting their data in accordance to their wish for more control over their data.

4.3. Data management with Qualtrics and Stata

4.3.1. Descriptive

As mentioned previously, then the data collection survey programme Qualtrics was used, where a total of 202 people participated. However, only 126 of these were valid for the use of analysis, as Qualtrics coding system also include those participants that open and starts the survey but for unidentified reasons do not carry through with it. As the Qualtrics coding system also notified us during our construction of Likert scale and matrix questions, this combination may result in some participants not carrying through with the survey, which could explain this defection.

Out of the 126 responses, 70.63 percent (89 people) of these were females, 28.57 percent (36 people) were male, and only 0.79 percent (1 person) preferred not to say. The age division between the respondents showed a majority of 80.95 percent (102 people) were in the 21-30 age group, 7.94 percent (10 people) were in the 31-40 age group, 4.76 percent (6 people) were in the 51-60 age group, both the age groups under 21 and above 60 years old received a 2.38 percent (3 people) each, and lastly only 1.59 percent (2 people) were in the 41-50 age group.
Out of the 126 responses, the majority of 89.68 percent (113 people) stated that they have obtained a university degree, 7.94 percent (10 people) hold a degree from secondary school, 1.59 percent (2 people) hold a degree from primary school and 0.76 percent (1 person) preferred not to say.

The mentioned demographic variables are shown in respondents, percentages and the EU ideal percentage. The ideal percentage is based on the division of the presented variables at EU level, to investigate how our data collection corresponds to the demographics of the EU population. Our data shows that there is a slight overrepresentation of females for the gender ratio (Eurostat a, 2020), however this corresponds to the EU distribution. On the other hand, the younger age groups and the high educational level is largely overrepresented in this study compared to the EU population. Thus, we can only generalise our findings based on the our sample of EU citizens, as it does not directly resemblance the broader EU population.

Control variable	Survey respondents	Survey percentage	EU percentage
Age			[1]
< 21 years	3	2.38 %	20.7 %
21 – 30 years	102	80.95 %	11.8 %
31 – 40 years	10	7.94 %	13.2 %
41 – 50 years	2	1.59 %	14.2 %
51 – 60 years	6	4.76 %	14.1 %
> 60 years	3	2.38 %	26.0 %
I prefer not to say	-	-	-
Gender			[2]
Male	36	28.57 %	49.0 %
Female	89	70.63 %	51 .0%
Other	-	-	-
I prefer not to say	1	0.79 %	-
Educational level			[3]
Primary school	2	1.59 %	23.1 %
Secondary school	10	7.94 %	46.2 %
University degree	113	89.68 %	30.7 %
I prefer not to say	1	0.79 %	-

Table 1: Representation of age, gender, and educational level compared to EU level

4.3.2. Linear regressions

In addition to the qualitative analysis of our findings of correlations between consumers' behaviour on digital platforms and their privacy concerns, we sought to conduct a quantitative analysis to investigate if quantifying our qualitative data would uncover additional aspects of our identified qualitative correlations. However, it is important to note that quantifying our data is merely an addition to our qualitative

[1] Age ratio retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Ageing_Europe_-_statistics_on_population_developments#Older_people_.E2.80.94_population_overview
[2] Gender ratio retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php/Gender_statistics
[3] Educational level ratio retrieved from https://ec.europa.eu/eurostat/cache/infographs/womenmen_2017/dk_dk/bloc-2a.html

analysis, which we claim is more suitable and weighs higher in terms of its reliability. The reasoning behind this is that the survey sets out questions that are related to one another in a way that includes interpretations and assumptions. These are notoriously more difficult to rationalise through quantification as oppose to qualification. Thus, quantifying our data implies a compromise between, on one side being able to analyse the effect of different variables in the regressions of our hypotheses, and on the other hand fulfilling the requirements of statistical reliability of variables. While we were able to control what questions from the survey were included in the each correlation test of factor variables for our regressions, we were not able to control which clusters represented the highest reliability scores. Therefore, we were also unable to control what variables were best suited, quantitatively speaking, to be included in each regression.

We were unable to make a linear regression for H_2, as our survey did not provide us with any findings that were valid enough to represent our independent variable "perception of private". The reason for this is that the only findings related to the perception of financial data as being private, derive from a elaborative question in our survey, in which our respondents were asked to explain their opinion. In our assessment of possible ways of to how convert this categorical data into an ordinal value, thus allowing for quantification, we did not find any suitable matches and therefore chose not to make a linear regression on this hypothesis.
Moreover, the linear regression for H_3 has a low degree of validity as the variable used to represent the dependent variable of 'trust' has a low reliability score. However, we chose to make the regression for this hypothesis in order to display what the process would look like.

4.3.2.1. Test of hypothesis 1

H_1: Consumers wish to gain more control over their data for the purpose of protecting their data privacy.

In order to identify if there is a relationship between the wish for control and protection of data privacy the first step was to conduct a scatter plot (see Figure 3). The scatter plot shows the coordinates for each case in the data sets, and has a linear fit in order

to more easily evaluate the relationship. From Figure 3 the relationship between the consumers' wish for control and their data protection appears to follow a negative linear trend. The scatter plot merely shows if there is a relationship between the variables and not whether one variable causes the other. Having established that there is a relationship between our variables, we can carry on with a further examination with a linear regression.

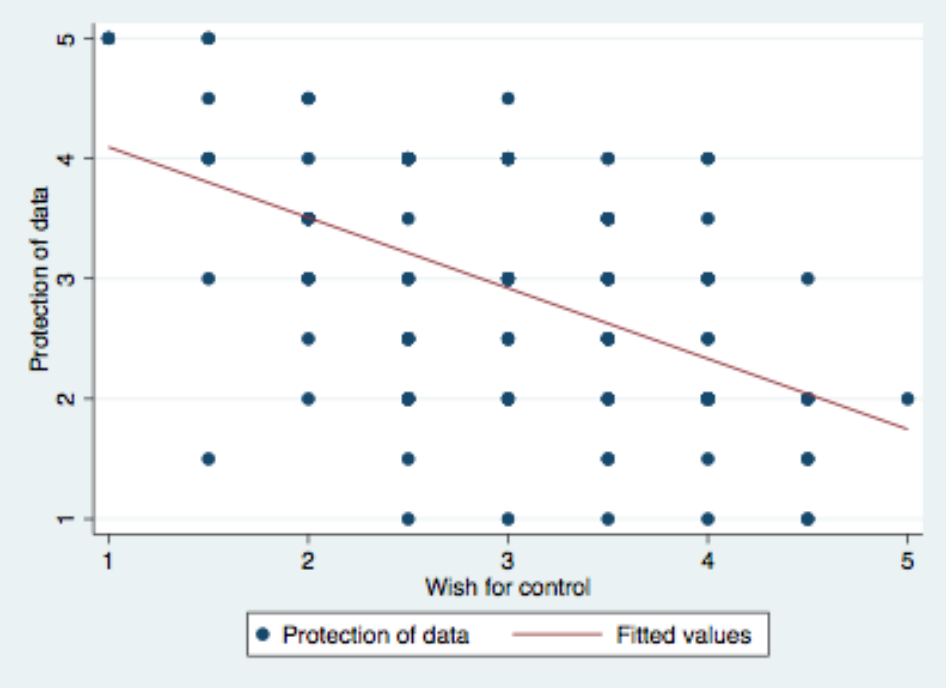


Figure 3: Scatter plot of the relationship between wish for control and protection of data

The following regression models are estimated with Ordinary Least Squares (OLS) in order to control for other factors that may impact consumers' level of protection.

Table 2 shows the estimate of different models and their effect on consumers' protection of data. Before commenting on the table, it is important to elaborate what the variables reflect, as these consist of the mean value of various other variables. Therefore, it is important to underline the meaning of these questions in order to describe what the variables actually represent. The dependent variable is "protection of data" and consists of the questions: "I try to educate myself and I investigate how I can control the data that I generate" and "I make use of privacy protection tools and apps". Educating oneself on privacy protection and making use of protection tools

reflect actions towards protecting one's data, and hence these questions represent the dependent variable "protection of data". The independent variable is "wish for control" and consists of the means from the question statements: "Data privacy is not something that I can control" and "I do not know how I can control my data". Not knowing how to protect one's data can be argued to be an underlying reason for wishing for more control, and therefore we argue that these questions can be used to represent the independent variable "wish for control".

In column (1), (2) and (3) the dependent variable "protection of data" is tested in three models against the independent variable "wish for control" and our basic demographics which function as control variables, namely age, education and gender. Thus, in column (1) we see the variables "wish for control" and age, and their effect on consumers' level of data protection. Column (2) shows a model in which the educational levels effect on data protection is included and column (3) includes gender in the model and estimates its effect on protection of data. The first model shows that the estimate of wish for control is very significant and negative, which indicates that consumers' wish for control has a strong negative effect on their level of data protection. This suggests that the more control consumers wish for, or as explained previously, the less control people feel that they have over protecting their data, the less they protect their data by taking active measures towards protecting it. Moreover, column (1) shows that the effect of age on protection of data is negative itself but that the estimate is not significant. In column (2) we included the control variable education, in which we see that the wish for control slightly increases but remains still significant. In column (3), we control for gender and here we find that wish for control increases while remaining significant.

Protection of data	(1)	(2)	(3)
Wish for control	-0.587***	-0.584***	-0.570***
	(0.0879)	(0.0880)	(0.0885)
Age	-0.00978	-0.0271	-0.0403
	(0.0829)	(0.0851)	(0.0855)
Education		-0.194	-0.197
		(0.212)	(0.212)
Gender			-0.200
			(0.158)
Constant	4.704***	5.296***	5.640***
	(0.333)	(0.728)	(0.776)
Observations	126	126	126
R-squared	0.266	0.271	0.281

Standard errors in parentheses: *** p<0.01, ** p<0.05, * p<0.1

Table 2: Protection of data with three different models

On the basis of these significant results we are able to conclude that consumers' wish for control has a strong effect on their level of data of protection, which suggests that the more control consumers wish for, or as explained previously, the less control people feel that they have over protecting their data, the less they protect their data by taking active measures towards protecting it.

4.3.2.2. Test of hypothesis 3

H_3: Consumers trust digital platforms, because they do not experience consequences of sharing their data.

As with the previous hypothesis, we start by determining whether or not the relationship between trust and consequences of sharing data exists by conducting a scatterplot as seen in Figure 3. The figure shows that there is a relationship between trust in digital platforms and the experienced consequences of sharing data and that

it follows a positive linear trend. On these grounds, we can carry on with our linear regression of hypothesis 3.

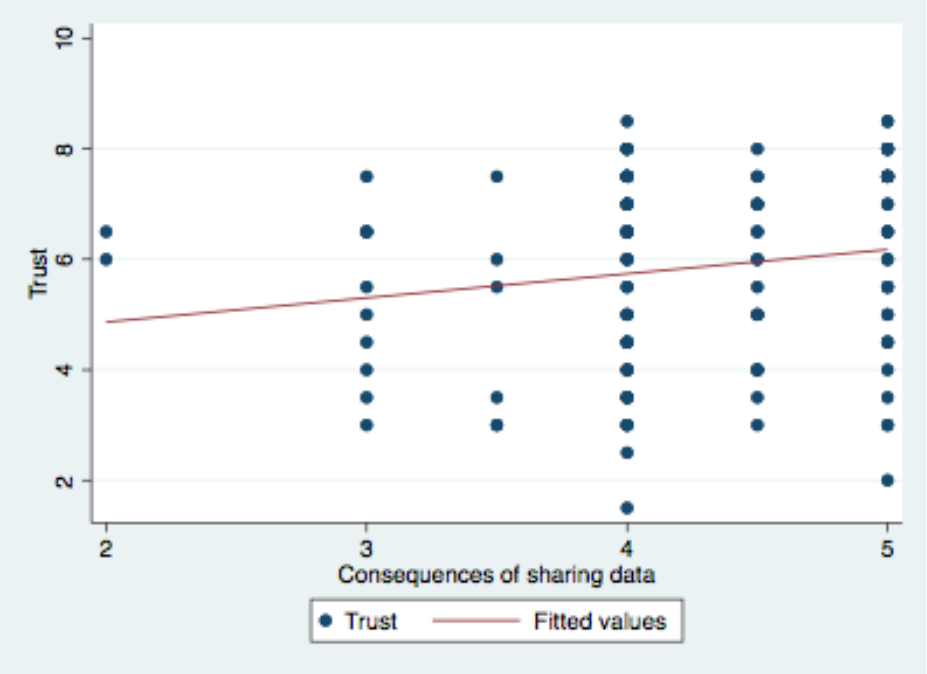


Figure 4: Scatter plot of the relationship between trust in digital platforms and the experienced consequences of sharing data

Table 3 shows the trust in digital platforms with three different regression models that it estimates our independent variable and the control variables' effect on consumers trust in digital platforms.

As with the previous H_1, the following Table 3 calls for some elaboration on the variables. The dependent variable is "trust" and consists of the question statements: "I do not trust how my data is being handled" and "I do not trust the digital platform with my data". These questions relate to consumers' level of trust, however as the questions imply a mistrust for digital platforms, these questions reflect a lack of trust as oppose to an actual trust in digital platforms. Thus, the dependent variable "trust in digital platforms" actually reflects mistrust. While we do acknowledge that this combination of questions as a reflection of our dependent variable of trust in our H_3 may seem somewhat far-fetched and difficult to comprehend, we chose to include the regression models in order to display what it would look like. The independent variable in Table 3 "consequences of sharing data" consists of the questions: "I want to know with whom my data is being shared" and "I want to know what my data is being used

for". Wanting to know with whom one's data is being shared and for what purpose, can arguable be a precondition for the consequences one experiences when sharing data. Thus, the independent variable "consequences of sharing data" reflects consumers' wish to know the data sharing purpose and its receiver.

Column (1) shows that the "consequences for sharing data" has a positive and strong effect on consumers' "trust in digital platforms", and that the estimate is significant. With reference to the aforementioned elaboration on the independent and dependent variables' actual reflection, this could indicate that the more consumers wish to know the purpose of their data sharing and its receiver, the higher their mistrust in digital platforms become. Moreover, age has a negative effect on consumers' trust in digital platforms, but the estimate is nevertheless significant. This could suggest that the older the consumer is the less he or she (mis)trusts digital platforms. In column (2) we include the control variable "education" into the model and find the effect of "consequences of sharing data" on "trust in digital platforms" has increased slightly, however the estimate is still as significant as in model (1). Furthermore, we see that while the negative effect of "age" has increased when including the control variable "education", the estimate of age is still significant. In column (3), we include the control variable gender into the model. Here, we see that the estimate of "consequences of sharing" data's effect on trust in digital platforms decreases again and becomes less significant. Moreover, the effect of age decreases slightly, however the estimate remains significant.

Trust in digital platforms	(1)	(2)	(3)
Consequences of sharing data	0.448**	0.453**	0.447*
	(0.225)	(0.227)	(0.229)
Age	-0.297*	-0.306*	-0.311*
	(0.159)	(0.164)	(0.166)
Education		-0.0962	-0.0959
		(0.410)	(0.412)
Gender			-0.0872
			(0.306)
Constant	4.635***	4.913***	5.100***
	(1.026)	(1.570)	(1.707)
Observations	126	126	126
R-squared	0.056	0.056	0.057

Standard errors in parentheses: *** p<0.01, ** p<0.05, * p<0.1

Table 3: Trust in digital platforms with three different models

Based on these significant results we can conclude that the experienced consequences of sharing data, stemming from the wish to know the purpose of data sharing and its receiver of it, has a positive effect on consumers' (mis)trust in digital platforms. This suggests that the more consumers wish to know the purpose of their data sharing and its receiver, the higher their mistrust in digital platforms become. Moreover, the significance of the estimate of age suggests that the older the consumer is the less he or she mistrusts digital platforms.

4.3.2.3. Test of hypothesis 4

H_4: Due to inconvenience, consumers tend to allow privacy pop-ups in order to access the content they are seeking without calculating the privacy risks before clicking.

As with the remaining hypotheses, we will start with creating a scatter plot in order to establish the existence of a relationship between inconvenience and risk. From Figure

5, it can be deduced that the relationship follows a positive linear trend. This justifies further examination with a linear regression.

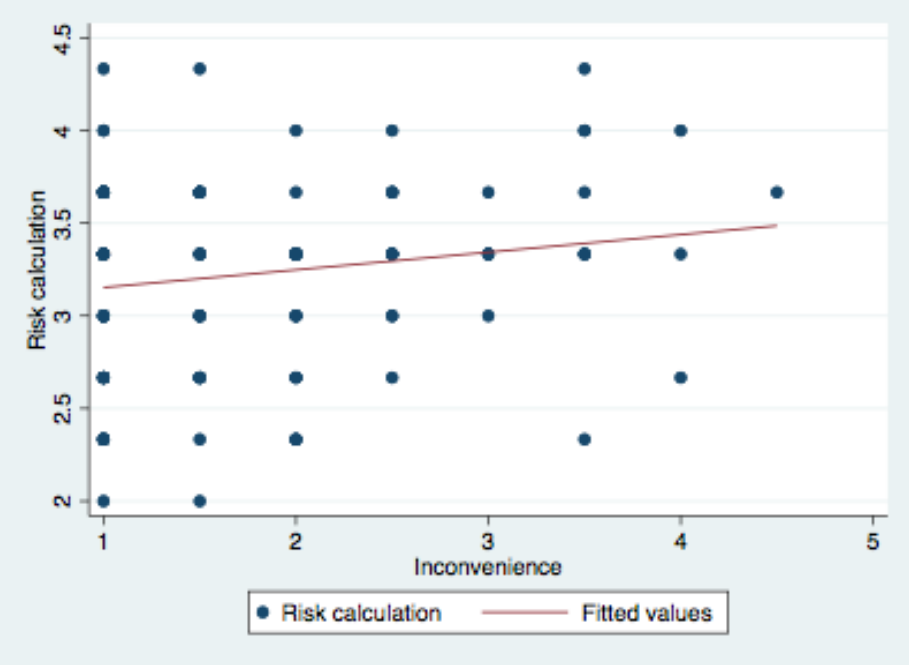


Figure 5: The relationship between lack of risk calculation and inconvenience

Table 4 estimates the effect of our independent variable inconvenience on risk calculation, as well as the effect of our control variables age, education and gender. The dependent variable is “inconvenience” and this variable consists of the two questions: “I read through most of it” and “I always read through the whole thing”. These questions can be said to imply an inconvenience, as reading through terms and conditions, either most of it or the whole thing, can be regarded as somewhat time consuming and effortful, thus serving as an inconvenience. The “risk” variable presents the lack of risk calculation and consists of questions related to allowing cookies, namely “I allow all cookies”, “I only allow necessary cookies” “I allow cookies sometimes”. Of the questions related to allowing cookies, these three can be argued to be connected to risk calculation, as they represent measures towards decreasing risks. Thereby, these questions suggest some degree of lack of risk calculation, as they all imply some degree of allowing as oppose to restricting cookies which purpose is to minimise risk. A lack of risk calculation is thus defined as allowing rather than restricting cookies.

Column (1) shows the first model in which the effect of inconvenience and age on consumers' risk calculation on digital platforms is estimated. In column (2), the control variable education is included in the model, and in column (3) the control variable gender is included. In the first model, we see that inconvenience has a low but positive effect on the risk calculation, but that the estimate is not significant. Moreover, we see that age also has a low but positive effect on risk calculation. This could indicate that the older the consumer is, the higher his or her lack of risk calculation is, which poses as a new finding using quantitative methods. However, the estimate is not significant. In the second model, column (2), we see that the effect of inconvenience on risk calculation slightly decreases, however the estimate remains positive and not significant, when including the control variable educational level. The same goes for the control variable age. We found that education has a negative impact on risk calculation, but that the estimate is not significant. When including the control variable gender in the third model in column (3), we see that the effect of inconvenience and education on risk calculation decreases, whereas age increases. Moreover, we find that gender has a positive effect on risk calculation, however the estimate is not significant either.

Risk calculation	(1)	(2)	(3)
Inconvenience	0.0819	0.0780	0.0639
	(0.0516)	(0.0531)	(0.0536)
Age	0.0587	0.0558	0.0667
	(0.0483)	(0.0493)	(0.0496)
Education		-0.0421	-0.0482
		(0.124)	(0.124)
Gender			0.137
			(0.0910)
Constant	2.944***	3.080***	2.860***
	(0.135)	(0.423)	(0.445)
Observations	126	126	126
R-squared	0.039	0.040	0.058

Standard errors in parentheses: *** p<0.01, ** p<0.05, * p<0.1

Table 4: Risk calculation with three different models

The above results suggest that inconvenience has a positive effect on risk calculation, which could indicate that the more a consumer inconveniences him or herself the higher their lack of risk calculation is. Moreover, while age and gender showed a positive effect on the lack of risk calculation, education showed a negative effect on risk calculation which could suggest that the higher the consumer's education level is the lower their lack of risk calculation is, meaning the more they calculate risk. However, as the estimates of all three models were insignificant, we are unable to conclude that inconvenience has a strong effect on consumers' lack of risk calculation if any at all.

4.3.3. Subconclusion

Overall, our quantitative analysis of our hypotheses using linear regressions showed that there is a significant relationship between our variables in H_1 and H_3. However, it is important to note that the variables in H_3 hold severe validity limitations. These

results complement our findings from our qualitative analysis. However, as the results of the regression of H_4 showed no significance, we were unable to conclude that the variables of this hypothesis had a significant relationship. As the implementation of the quantitative analysis was not a part of the initial research design, this could explain the lack of significance in H_4, as the questions were not designed for making linear regressions. However, our findings from the regressions have shown that quantitative methods are still applicable for confirming or denying hypotheses like these.

5. Discussion

With the enforcement of the GDPR in 2018, the public debate about data privacy and how consumers can protect their data reached new heights. While it can be argued that consumers today are generally more aware of how their data is being handled and what they can do to protect their privacy online, there is still a great need for improvement of the public knowledge on data privacy. When discussing how data is best protected, there is a important distinction to be made between protecting data that one has already provided and protecting one's data by not producing it in the first place. The findings of this study have shown that consumers protect their data in different ways and for different reasons. While personal opinions as to how data is best protected can be argued to be appropriate to some degree, e.g. in terms of how the individual needs of consumers are best served, there are still some clear facts when it comes to data protection that call for more general best practices for the public. The following sections will elaborate on these distinctions and what they imply as well as provide recommendations for a future framework that responds to consumers' demand for more control over their data.

5.1. Data restriction versus data generation

The findings of this study supports the current statistics stating that a majority of consumers do care about data privacy and do take measures to protect their data online. Moreover, we argue that the majority are generally aware of how data can be

protected by analysing the findings of our survey questions about data sharing and data protection. As mentioned in the analysis, our respondents prefer setting, checking or changing their privacy settings and educate themselves, to protect their data, rather than making use of privacy protection tools and apps or not sharing their data under any circumstances. In the analysis, we stated that the preference for privacy settings over not sharing data at all may be connected to convenience or the lack of awareness about which method is the most optimal. However, this study has not implied a definition of privacy protection as a concept but merely investigated the different ways that the respondent's group might protect their data. Therefore, we found it important to discuss how data protection can be defined and whether consumers are actually aware as to what degree their data is protected when using different protective methods.

First of all, it is crucial to establish that data protection can be separated into two categories: (1) restriction to collection, processing and sharing of ones data and (2) restricting one's overall data generation. When restricting the collection, processing and sharing of one's data it involves both the measures that consumers take and the ones that businesses take to keep personal information private. As our respondents group did not display strong beliefs in adopting privacy protection tools and apps, we will not further discuss these measures. However, we presented anonymization and encryption as two methods of data protection that businesses can adopt for the purpose of making consumers share their data. The respondents group indicated a stronger preference for sharing their data if it is either anonymised or encrypted. As mentioned in the analysis these two methods of data protection are quite different measures and hence we find it interesting to challenge the respondents view on these measures as they view them as the most optimal way of staying private. Despite there being several modes of protecting data available, there are limitations to their effectiveness that the common public does not question. However, several other methods such as pseudonymisation, hashing, tokenization, etc. can be used by businesses to keep their users' data private. Since the enforcement of the GDPR regular anonymization has become more and more challenged as adversarial models (re-identification attacks) have evolved tremendously over the recent years (Enisa, 2019). The model of pseudonymisation is being advocated for as a 'state of the art' protection technology by the European Union Agency for Cybersecurity (Enisa), to

such an extent that it was included in the GDPR under article 32: "*... the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data;...* " (GDPR, art. 32). Pseudonymisation is the processing of personal data where it no longer can be attributed to a specific individual without the use of additional information which is kept separately under technical measures that ensures that identification is not possible (Enisa, 2019). One's identifiable data is thus replaced by a code that replaces that given data. The identifiable data is thus removed and stored separately from the data that is to be processed. Anonymisation on the other hand is the irreversible action of personal data altered in such a way that an individual no longer can be identified directly or indirectly, not even by a data controller or any other party (Enisa 2019). Both methods have become valid options for businesses to handle sensitive personal data while still protecting the individual's data privacy. It has also become an argument in the debate of a European data economy in which data sharing is necessary in order for businesses to drive innovation and develop technologies of crucial importance to humankind, e.g. technologies within the healthcare sector. However, studies have pointed towards the fact that anonymising data does not work for all types of data, as it is still possible to de-anonymise data when compared to public or open data (Narayanan & Shmatikov, 2008; Korayam & Crandall, 2013; Sweeney, 2000). The same can also be said about geolocated data (Gambs, Killijian & Cortez, 2014), as mobility trances of individuals are highly unique hence this data is vulnerable to re-identification attacks (EDPB, 2020). Consumers should thus not seek to believe that the anonymisation or pseudonymisation of their data entails that their privacy is ensured and not at risk. These attacks on data processing, supports the demand for increased consumer awareness but is this even realistic to expect that the consumer will challenge these methods? Have consumers even thoroughly investigated and evaluated their data protection preferences for how their data is processed?

Additionally, the encryption of data - together with anonymisation - was also viewed by our respondents group as the most optimal way of staying private. Encryption, as explained the analysis, entails not just a 'removal' of the personal identifiable data but a complete 'removal' of the entire data such as personal information and the content. One could argue that encryption is more secure as it makes the entire data impossible to read to everyone, including the data controller. The GDPR advocate for encryption

being the best protection during data transferring, however, what encryption technique is implemented is up to the data controller to decide (GDPR, art. 32). It thus protects both your personal data and whatever the generation consists of, such as conversations or browsing historic etc. However, is encryption of data really that secure? Several studies have shown that cryptography (the practise consisting of encryption, encryption analysis and encryption key management) has several issues relating to plain-text disclosure, weak encryption algorithm and keys, and authentication errors (Lazar, Chen, Wang & Zeldovich, 2014). The cryptography of data is in theory a strong protector against invasion of personal and sensitive data, so consumers are not completely off in trusting this method. However, the weaknesses are often related to the human errors made in the production and management of setting up an encrypting system around a product or service.

The point of challenging both the anonymization and encryption belief that our respondents group displayed, is to emphasise the issue of having consumer awareness as a sole solution to privacy concerns. How businesses protect their user's data should not be a concern that should have any weight in consumers decision making of whether or not they should share their data. Data breaches are not unavoidable and they are going to occur, but the GDPR should be able to translate - in an understandable manner - the rights and actions that consumers can take if this happens. Additionally, law enforcement should take firm actions against businesses to display that GDPR is a empowerment to the consumer. As expert Anette Høyrup states: "*One of the challenges is to enforce the new rules for businesses and make them live up to them… it also entails that the data protection agencies in Europe are proactive*." (Appendix 4, line 30-34). She further states that what they try and do is to encourage consumers to file complaints, however is it difficult: "*... it is still very complex and there are many consumers that do not spend time on this [file a complaint] due to the complexity*" (Appendix 4, line 50-51). The issue here is to make it more manageable for consumers to navigate through the GDPR for the sake of their data privacy and remove concerns that should not be present in the first place.

This leads us to the second distinction of data protection which is the restricting one's data generation. We referred to this category as a set of 'proactive' measures to protecting data, which implies that the data protection is best achieved when the individual restricts his or her data generation to not providing data online in the first

place. Of course, this does not entail going off the grid completely, but it generally implies that consumers' privacy is safer when they critically evaluate their data generation online. At the moment, it can be argued that boycotting digital platforms is the only tangible guarantee a consumer can get for the protection of their privacy, however not many consumers are willing to do this due to the loss of personal benefits this may entail. Our respondents group stated that they do not seek to never share their data or taking the extreme measure of boycotting a platform. As we assumed, something could suggest that consumers do accept the premise of not being in complete control over their data as they do experience benefits in the trade-off of data for services. The questions is however, when does it compromise their right to privacy? Our respondents stated that they do not have a choice when it comes to using digital platforms. It can be argued that data sharing in this way is only voluntary to some extent, which suggests that the GDPR is not fulfilling its main task. Consumers do not feel empowered, nevertheless they feel powerless. With the wave of digitalisation, both of the age we live in and with the manifest of the new EU Commission, consumer lives are imbued with technology and everything is getting increasingly digitised these years, so is it even possible to reduce ones data generation? We would argue that it is not. One might be able to reduce the amount of data one generates, however as even the public sector has started to digitalise, a reduction of one's data generation would not be effective enough for protecting one's data privacy. If consumers are to reduce their data generation it would take extensive amounts of resources to ensure that one's data is not publicly accessible. Often by default, some of our data is publicly accessible unless we take active measures to remove it, such as your phone number on www.krak.dk.

This leads us to the discussion on opt-in versus opt-out. What is the best practise? We will not go into depts with the specific technologies, but there are some interesting thought to made here. Both measures entail that consumer awareness must increase. By opting-in the consumer voluntarily agrees to share their data and this entails more control for the consumer. However, opting-out entails a by default agreement, which can of convenience and value to the consumer. However, as the word suggests, opt-out requires an active decision of declining and takes extensive amount of effort to the consumer, contrary to opting-in. Opt-in or opt-out should receive more attention from policy makers, as this also entails that consumers increase their awareness in terms of data sharing by default, and as it should be easy to refuse this in a somewhat

uncomplicated manner. Opting out is a process that businesses have made more difficult to practise in such a manner, that even though the GDPR art. 17 stipulates 'the right to be forgotten' so one's data is erased, consumers are met with negative and complicated challenges in doing so, which should not be a problem. Consumers believe that they have no other choice than to share their data if they seek to use digital platforms. This shows how they obey to intrusion of their privacy for the sake of using online services and becoming a part of an online community. Consumer probably do not adopt strict privacy protection measures, as they have come to the realisation that intrusion is unavoidable nowadays. If this is case, the enforcement and an re-evaluation of the GDPR should be considered.

Data privacy is a subjective matter and it varies from consumer to consumer, however with the continuous demand for more control, we argue that the GDPR has room for improvement. The GDPR has set the bar too low and consumers are left to make the decisions on their own data privacy which they simply are not fully equipped to. The expectations of the EU to demand for EU citizens to be so well-informed and ready to make decisions of such intensity, does not seem fair. Consumers should not have their privacy invaded - voluntarily or involuntarily - and especially not determined by their level of data protection awareness. As put forward in the analysis, consumers might need to know who third-parties are, but as research has shown, this study included, then inconvenience, time and habituation blocks our interest in protecting ourselves. Businesses know more about the consumers than they do themselves, and the current legislation is not protecting them from this exploitation. Hence, it would be wise to question if more legislation, in favour of the consumers, should be adopted. Raising the bar for minimum EU level requirements on data privacy legislation would meet the consumers middle way in their demand for more control. It is crucial also to evaluate if consumers are eligible to be trusted with the amount of control that they demand. The field of data privacy and how to protect it is extremely complex, so to expect that consumers solely are able to rationally evaluate and know about data protection measures, would be a flawed claim. Therefore, it is relevant to raise the question of the fairness in letting the consumer's knowledge determine the level of their data privacy. If privacy is the right to be let alone (Wang et al., 1998), is data privacy then not the right for one's data to be let alone as well? As of now, consumers can only

practise the right to be let alone online, if they do not generate any data because their data is not being let alone. Consumers find it difficult to translate the GDPR intro their everyday lives. As our expert Jan Bauer, Associate professor from CBS stated in his interview: "*[The default idea of it [one's own data] is all mine]... it does not work because the consumer does not have the knowledge, does not have the capacity to make those choices and… it is the consumer… the citizen who should be the first to be protected*" (Appendix 5, line 144 + 158-160). It is also important for us to mention that it is not - and should not - be businesses responsibility to make every single consumer understand the entire matter of data privacy. It is certainly up to the consumers themselves to take responsibility of their actions and to understand and utilise the right to privacy that they have. Businesses cannot ensure that the consumer fully understands the term of using their digital platform, but as mentioned studies have proven that the practise businesses are currently running are nowhere near making it easier for consumer to comprehend the matter either.

We do not claim to know the answer to which distinction of data restriction or generation is better, but we find that is important to underline that consumers' awareness should not determine the individual's level of data protection. As GDPR has been put into force to protect consumers, there is room for improvement when it comes to providing an equally fair framework in which consumers level of data awareness does not determine the level of their data privacy. The bar for EU level legislation protecting consumers first and then businesses, should be raised as a response to consumers' increasing demand for more control over their data.

5.2. Privacy by design

As presented by some of the theories, a possible solution to the privacy paradox and to consumers wish for more control over their data for the sake of their privacy, Privacy by design could be the answer. Our experts also introduced how they see Privacy by design being able to reduce the concerns that consumers hold. Anette Høyrup explained: "*... I do not believe that we can demand of the consumers that they have to take on that responsibility because it is so technically complex… It is difficult and complicated to comprehend for the consumer and to gain control over their data, even*

though it is was legislation contemplate" (Appendix 4, line 54-56 + 60-62). Aside from theory, our experts also do not see that consumer awareness is a sole solution or that the consumer should or is capable of making these decision as to their own data protection. Jan Bauer stated: "*... it is also too complicated for them to comprehend. So I would not rely on the consumer to make the right choices there always.*" (Appendix 5, line 18-19). Jan has been involved in a study that proved that consumers can be manipulated into sharing their behaviour data, solely based on the design of a cookie notice. They came to find that certain types of notices could be designed in such a way that resulted in a 17 percent increase in consumers sharing their data (Appendix 5, line 117-124). Manipulations or triggers like these are what consumers are subject to on a daily basis when using digital platforms. Currently, Privacy by design is mentioned in art. 25 of the GDPR and state that businesses should "*... implement appropriate technical and organisational measures*" that are "*... designed to implement data-protection principles*", hence "*... such measures shall ensure that by default personal data are not made accessible...*" (GDPR, art. 25). The definition of what Privacy by design by law is up for interpretation and the only thing it stipulates is that some measures must be taken to ensure that data is kept private and preferably at a minimum. However, no specific standards are set here and that data minimisation is not a lawfully requirement but merely an encouragement, gives businesses a great latitude.

Anette suggested that by implementing Privacy by design companies can use this as a competitive advantage over the big giants, as data protection agencies can support these companies in advocating these to the consumers. But is this really something that disrupt industries? In Denmark, The Danish Industry Foundation, The Confederation of Danish industries and the Danish Chamber of Commerce have joined forces for a data security labelling scheme (Erhvervsministeriet, 2019). But is this the way to go? If digital platforms are labelled with this data labelling scheme, the consumer still has to obtain knowledge about what the scheme stands for. Moreover, how will the label work in practise when a consumer browses on other European sites which may have their own national labelling schemes? Should they then also know what those national labelling schemes stands for? If the purpose of a labelling scheme is to ease consumers' decision making, then we suggests developing one collective European label across digitalisation technologies that also function cross-boarderly.

This measure will support that consumers are not forced to make decisions that they are simply not equipped to make. Another point to make here, is if consumers even would care about a labelling scheme when they use digital platforms? Will a label really have enough impact on the consumers for them to deviate from their habituation and their convenience pattern?

5.3. The future for data

Before providing some recommendations as a possible solution to accommodating consumers demand for strengthened data privacy, it is relevant to evaluate data privacy from all three sides of the consumers, businesses and the policy makers. As this thesis mainly has viewed the issue of data privacy from the point of view of consumers, this is already extensively elaborated. However, we find it crucial to acknowledge and clearly state that we do not in any matter or form neglect the importance that data has on businesses. We find it relevant to discuss the aforementioned premise of using digital platforms, namely that the consumer is not in full control over their data. Consumers have adopted the prejudice that they can get services for free online. "*When you go to the newsstand and buy a newspaper, you pay money to read whatever is in this newspaper but on the internet you expect to get it for free, the same information…*", says our third expert Dorte Lundin, Programmatic Lead at GroupM (Appendix 6, line 18-21). Is it even a fair assumption that consumers expect to receive services for free just because it is digital? No, of course not. The amount of money it takes to run a service on a utility platform or a interaction network platform, takes enormous amounts of resources which are also put into developing better customer experiences. It is time that we make up with the assumption that 'free' services exist and realise that the premise for using digital platforms is that one trades data for services. By principle it is crucial to recognise that data has become the new currency, however the trading parties should be equally aware of this.

There is still a great deal of evidence pointing towards the fact that it is the digital platforms and businesses that have the upper hand when it comes to data privacy. They have the potential leeway for utilising their users' data for other benefits than societal. As data privacy is the right for anyone to be let alone, also online, it is crucial to distinguish between when the consumer are truly aware of when and what data they

are providing and when data is tracked without their knowledge and consent. We are not claiming that data driven businesses should be shut down, because consumers still derive a lot of value from these services. However, we suggest that legislation increases its focus on restricting the leeway that businesses have within the GDPR for collecting non-consensual or manipulated 'volunteered' consumer data. Dorte explained that she expects that businesses will have to find new ways of making money and this will also affect the consumers, as their previous 'free' service will vanish. She elaborates: "*The consequence is just that we - in the long run - will see that more media bureaus will start taking payment for the content they are producing, and I believe that in the beginning as a consumer, one will see this as negative, but turn it around, in the end it is a business.*" (Appendix 6, line 134-137). If Dorte's forecast is accurate, consumers must be ready for the possibility of swapping their currency of data with money. Perhaps, this concept is not preferred by consumers, but the decrease in legal data collection will affect business models and will bring along change to the 'free' service landscape.

When it considering data privacy legislation, we recognise that policymakers represent various point of views and interest, and that a regulation on data privacy should meet the needs of consumers, businesses and authorities alike. It is a known fact that legislation by default always will be outdated by the time it comes into force. However, now that the GDPR has been in force for two years, and it still has not fulfilled its purpose, it is time for a review. Ursula von der Leyen, President of the EU Commission, has declared that the newly compounded EU Commission serves the goal of making the Single Market fit for the digital age, create an economy that works for people and foremost then the EU must lead the transition of a new digital world that bring people and businesses together (European Commission a, 2019). Cybersecurity is one of the areas in which the EU has to catch up to, hence the consumers demand for more control over their data complement the EU Commission's agenda anno 2020. As mentioned previously, the bar for minimum requirements of data privacy is already set in the current GDPR. However, if von der Leyen is going to reach her goals, the GDPR bar must be raised as the EU citizen still feels powerless.

5.4. Recommendations for altering the GDPR

On the basis of the different arguments we have brought up throughout this entire thesis, we will provide some recommendations for EU policy makers as we believe that these suggestions will be of great relevance and importance when responding to consumers' privacy concerns.

First of all, we recommend that more and stricter regulation is needed in the GDPR. The level of best practises and encouragement for certain practises needs to be clearly formulated and certain measures should be demanded. This means that grey zones must be explicitly determined on how to legislate one's way out of, for the sake of eliminating these. Grey zones ultimately does not favour or empower the consumer. By reviewing and further restrict the current legislation, it will ensure alignment of data protection practises across digital platforms and thus contribute to a less complex framework of procedures that consumers must evaluate. This will simplify the matter of data privacy and ultimately ease the consumers' decision-making process when determining whether a digital platform lives up to one's standards of privacy protection.

Second, we call for a specification of the legal frame of a cookie. As the matter of cookies is only mentioned under recital 30 and as studies have uncovered that consumers are easily triggered by certain designs and phrasings, the design and usage of cookie notices should receive further attention. We recommend not formulating best practises or encouragement. However, an explicit design, phrasing and usage should be legally determined and apply for all businesses. By forcing the consumer to make an active choice between allowing or denying the different cookies in a pop-up window that blocks the view of a website, we believe that this will place more power in the hands of consumer, rather than a thin banner in the bottom of a page that only allows you to agree with the website's cookie tracking. By setting a single practise for how cookie notices should look like, alignment between digital platform will minimise the complexity of its meaning to consumers and ease their decision making process.

Third, we call for Privacy by design to become a legal act. A framework for production of new products and existing product should be subject to a certain scope of minimum

requirements related to Privacy by design. On this matter we acknowledge that the matter of Privacy by design is extremely complex and difficult to manage. However, we do believe that by setting certain privacy standards around the production of new product this will support the goal of making the Single market ready for the digital age in the long run. This measure would be a competitive advantage against non-EU businesses, thus leading the way for a new digital age. When it comes to forcing Privacy by design on to already existing products this involves increased cost of restructuring, however by replacing encouragement or best practises with a minimum requirement this will have a direct impact in reaching the goal of empowering the consumer.

6. Conclusion

The aim of this thesis was to uncover the correlation between consumers' behaviour on digital platforms and their demand for strengthened data privacy. This was done by testing under which parameters people protect or do not protect their data. Derived from literature and through expert interviews, the parameters tested were trust, risk and convenience. The research design of this study included Mixed Methods of qualitative and quantitative analyses of results from our main data source which was a survey on behaviour and beliefs about digital platforms and data privacy. To test the various parameters' influence on consumers' behaviour on digital platforms, hypotheses were developed and analysed qualitatively through theoretical interpretations and quantitatively with linear regressions.

The main findings of this study were that consumers' behaviour on digital platforms is affected by all of the presented parameters. Additionally, our findings showed that consumers' level of awareness has a great impact on their behaviour, hence we adopted this as a fourth parameter. Trust was linked to consumers' wish for more control over their data, which was reflected in their wish to know the purpose of data use and its receiver. This may also be the reason why consumers currently do not trust digital platforms with their data. The parameter of risk showed that consumers do associate risk with using digital platforms, however these did not seem to exceed the

value that the consumers receive. Moreover, we uncovered that certain types of data were associated with a higher disclosure risk, and thus was valued higher than other types. The parameter of convenience turned out to play a crucial role in protecting one's data. It can be concluded that protective measures such as pop-up windows are directly dismissed due to inconvenience, namely that the time and effort demanded disrupts the main purpose of the online behaviour. Lastly, we found that consumers' actual awareness about the complexity around data protection can be questioned. This further entails that the consumers' knowledge of protective measures does not realise their wish for more control. Therefore, we can conclude that consumers' wish for strengthened data privacy does not necessarily entail that they also protect their data likewise. Trust to different stakeholders, the risks involved with digital platforms, online convenience and the consumers' awareness of data privacy and protective measures all affect and to different degrees block the consumers in behaving in accordance to their intentions. By the supplement of linear regressions conducted on three of the four hypotheses, we were able to conclude that there was a significant relationship between the variables in H_1 and H_3. Hence these results indicate that statistical methods can complement findings from a qualitative analysis.

Based on the findings on consumers' awareness on data protection, we discussed whether their level of awareness should determine their level of data protection. It was discussed if the GDPR has empowered consumers as it promised to do. Therefore, we argued that the EU policy makers should raise the bar for the GDPR's minimum requirements. Furthermore, we provided specific recommendations to the GDPR for further regulation on the areas of cookie notices and Privacy by design.

Further research

Further research on consumers' behaviour on digital platforms and data privacy concerns should include an experiment with the respondents group of the survey, in which the different findings of this study are tested. One element could be to test the consumers' intended behaviour on digital platforms versus their actual behaviour. As this study has assumed that the consumers' actual behaviour corresponds to their answers from our survey, it does not account for the fact that consumers might not be entirely rational. Investigating the consumers' intended behaviour would also support theories on the intention-behaviour gap, which dive into consumer irrationality. In this way, we would be able to identify which specific barriers stand in the way of people converting their wish for more control into actions. This would allow for concrete recommendations on how to overcome these barriers.

Another interesting element to further research, would be to test the consumers' perceived awareness versus their actual awareness of data privacy as this study's research design does not account for a divergence between the two. Uncovering the actual awareness on data privacy and protection would provide better grounds for specific recommendation on e.g. cookies and privacy enhancing technologies.

In terms of research design, this study found that it is possible to quantify qualitative data with the purpose of confirming or denying hypotheses. However, this would require including questions surveys that already from the initial phase is focused towards being measured econometrically, in order to obtain the most valid result. Moreover, it should carefully be considered whether a latent concept such as data privacy should be analysed quantitatively, as doing so does not allow for as many interpretations of results.

Bibliography

Acquisti, A. (May, 2004). Privacy in electronic commerce and the economics of immediate gratification. EC ´04: Proceedings of the 5th ACM conference on Electronic commerce, pp. 21-29.

Albaum, G. & Murphy, B. (28 October, 1988). Extreme response on a Likert scale. Psychological Reports, Vol. 63, pp. 501-502.

Albergotti, K. (26 November, 2019). Apple say recent changes to operating system improve user privacy, but some lawmakers see them as efforts to edge out its rivals. The Washington Post. Retrieved 4 April 2020, from https://www.washingtonpost.com/technology/2019/11/26/apple-emphasizes-user-privacy-lawmakers-see-it-an-effort-edge-out-its-rivals/

Böhme, R. & Köpsell, S. (April, 2010). Trained to Accept? A field experiment on consent dialogs. International Conference on Human factors in Computing Systems Proceedings, pp. 2403-2406.

Borneschein, R., Schmidt, L. & Maier, E. (2020). The Effect of Consumer' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices. Journal of Public Policy & Marketing, Vol 39(2), pp. 135-154.

Bowles, N. (12 April, 2018). After Cambridge Analytica, Privacy Experts Get to Say 'I Told You So'. The New York Times. Retrieved 11 April 2020, from https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html

Brown, B. (26 March, 2001). Studying the Internet Experience. HP Laboratories Bristol, HPL-2001-49.

Bryman, A. and Bell, E. (2011). Business Research Methods. 3rd ed. New York: Oxford University Press, pp. 4-711.

Carrascal, J., Riederer, C., Erramilli, V., Cherubini, M. & Oliveira, R. (May, 2013). Your browsing behavior for a big mac: economies of personal information online. WWW´13: Proceedings of the 22nd international conference on World Wide Web, pp. 189-200.

Chen, A. (26 September, 2018). What happens when life insurance companies track fitness data? Verge.com. Retrieved 27 April 2020, from https://www.theverge.com/2018/9/26/17905390/john-hancock-life-insurance-fitness-tracker-wearables-science-health

Cisco (November, 2019). Consumer Privacy Survey – The growing imperative of getting data privacy right. Retrieved 9 March 2020, from https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf

Cisco (2020). Products, Solutions, And Services. Retrieved 14 April 2002, from https://www.cisco.com/c/en/us/products/index.html#~products-by-business-type

Clement, J. (7 October, 2019). Online Privacy - Statistics & Facts. Retrieved 10 May 2020, from https://www.statista.com/topics/2476/online-privacy/

CNIL, (21 January, 2019). The CNIL's restricted committee imposes a financial penalty of 50 Million euros again GOOGLE LLC. Retrieved 8 April 2020, from https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Coventry, L., Jeske, D., Blythe, J., Turland, J. & Briggs, P. (7 September, 2016). Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance. Frontiers in Psychology, Vol. 7, article 1371.

Data Etische Kommissionen (December, 2019). Opinion of the Data Ethics Commission. Retrieved 11 May 2020, from https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3

Datatilsynet (n.d.). Indbygget databeskyttelse (Privacy by design). Retrieved 2 May 2020, from https://www.datatilsynet.dk/emner/persondatasikkerhed/indbygget-databeskyttelse-privacy-by-design/

De Vaus, D. (2002). Surveys in Social Research. (5th ed.) Routledge, London.

Deloitte (2018). A new era for privacy – GDPR six months on. Retrieved 9 March 2020, from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf

Deloitte (2020). Government & Public Services. Retrieved 14 April 2020, from https://www2.deloitte.com/global/en/industries/government-public-services.html?icid=top_government-public-services

EDPB (European Data Protection Board) (21 April, 2020). Guidelines 04/2020 on the use of location data and contact tracing tools in the context of COVID-19 outbreak. Retrieved 8 May 2020, from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

EDPS (n.d.). The History of the General Data Protection Regulation. Retrieved 9 April 2020, from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Egelman, S., Cranor, L. & Hong, J. (April, 2008). You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1065-1074.

Enisa (The European Union Agency for Cybersecurity) (November, 2019). Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions. Retrieved 7 May 2020, from https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

Erhvervsministeriet (31 November, 2019). Nyt mærke for it-sikkerhed og ansvarlig dataanvendelse på vej.Retrieved 7 May 2002, from https://em.dk/nyhedsarkiv/2019/oktober/nyt-maerke-for-it-sikkerhed-og-ansvarlig-dataanvendelse-paa-vej/

European Commission (n.d.). 2.1 Uddannelse. Retrieved 10 May 2020, from https://ec.europa.eu/eurostat/cache/infographs/womenmen_2017/dk_dk/bloc-2a.html

European Commission (June, 2015). Data Protection. Retrieved 9 March 2020, from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

European Commission a (10 September, 2019). The von der Leyen Commission: for a Union that strives for more. Retrieved 9 May 2020, from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_5542

European Commission b (18 September, 2019). How do online platforms shape our lives and businesses? - Brochure. Retrieved 21 April 2020, from https://ec.europa.eu/digital-single-market/en/news/how-do-online-platforms-shape-our-lives-and-businesses-brochure

European Commission (19 February, 2020). White Paper On Artificial Intelligence - A European approach to excellence and trust. Retrieved 11 May 2020, from https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Eurostat (26 June, 2018). File:Age pyramids, 1 January 2017 (% of total population) world18.png. Retrieved 14 April 2020, from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Age_pyramids,_1_January_2017_(%25_of_total_population)_world18.png

Eurostat (June, 2019). Ageing Europe - statistics on population developments. Retrieved 10 May 2020, from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Ageing_Europe_-

_statistics_on_population_developments#Older_people_.E2.80.94_population_overview

Eurostat (February, 2020). Gender Statistics. Retrieved 14 April 2002, from https://ec.europa.eu/eurostat/statistics-explained/index.php/Gender_statistics

Forbrugerrådet Tænk. (2020). About Us. Retrieved 14 April 2020, from https://taenk.dk/om-os/about-us

Fung, B. (16 April, 2020). Apple And Google Want Your Phone To Become A Coronavirus Tracking Device. Can It Really Work? Retrieved 11 May 2020, from https://edition.cnn.com/2020/04/15/tech/google-apple-coronavirus-tracker/index.html

Gambs, S., Killijian, M. & Cortez, M. (2014). De-anonymization attack on geolocated data. Journal of Computer and System Sciences, vol. 80, pp. 1597-1614.

GDPR (2016). General Data Protection Regulation. Retrieved 11 May 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Haggin, P. (31 December, 2019). iPhone Update Reminds User - Again and Again - of Being Tracked; Some app developers are concerned that frequent iOS 13 notifications will scare user away. The Wall Street Journal. Retrieved 4 April 2020, from https://www.wsj.com/articles/iphone-update-reminds-usersagain-and-againof-being-tracked-11577799336

Happn.com (29 July, 2020). Privacy Policy. Retrieved 11 May 2020 from https://www.happn.com/en/privacy/

Harvard University (3 April, 2020). Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks. Retrieved 11 May 2020 from https://ethics.harvard.edu/files/center-for-ethics/files/white_paper_5_outpacing_the_virus_final.pdf

Hunt, P. (12 June, 2016). 9 Types of of Software Platforms. Medium.com. Retrieved 15 April 2020, from https://medium.com/platform-hunt/the-8-types-of-software-platforms-473c74f4536a

Hussain, I. (19 January, 2020). Tile Testifies in Congress Against Apple's iSO 13 Location Tracking Changes. Wccftech. Retrieved 4 April 2020, from https://wccftech.com/tile-testifies-in-congress-against-apples-ios-13-location-tracking-changes/

Ingram, D. (20 March, 2018). Factbox: Who is Cambridge Analytica and did it do? Reuters. Retrieved 11 April 2020, from https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F

Jiang, L., Yung, Z. & Jun, M. (2013). Measuring consumer perception of online shopping convenience. Journal of Service Management, Vol 21(2), pp.191-214.

Kokolakis, S. (10 July, 2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, Vol. 64, (2017) pp. 122-134.

Korayem, M., & Crandall, D.J. (2013). De-Anonymizing Users Across Heterogeneous Social Computing Platforms. ICWSM.

Krasnova, H., Günther, O., Spiekermann, S. & Koroleva, K. (1. October 2009). Privacy concerns and identity in online social networks. Identity Journal Limited, Vol. 2(1), pp. 39-63.

Kristensen, C. & Hussain, M. (2016). Metoder i samfundsvidenskaberne. Samfundslitteratur, (1 Ed.).

Kumar, V., Zhang, X. & Luo, A. (2014). Modeling Customer Opt-In and Opt-Out in a Permission-Based Marketing Context. Journal of Marketing Research, Vol. LI (August 2014), pp. 403-419.

Kvale, S. (2008). Doing Interviews. London: SAGE Publications Ltd., pp.1-161.

Lazar, D., Chen, H., Wang, X. and Zeldovich, N. (2014). Why does cryptographic software fail? A case study and open problems. In Proceedings of 5th Asia-Pacific Workshop on Systems (APSys '14). Association for Computing Machinery, New York, NY, USA, Article 7, pp. 1–7.

Lundin, D. (host) & Jørgensen, M. (co-host) (20 February, 2020). Digital beyond cookies [audio podcast]. GroupM Denmark. Retrieved 5 March 2020, from https://open.spotify.com/episode/6Wbp9KnuALgtxdya2Q1cpF?si=TgvmQDDqRkaY8sFbzBrHUQ

Magde, R. (27 August, 2017). Five loopholes in the GDPR. Retrieved 11 May 2020, from https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b

Milne, G. & Rohm, A. (2000). Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives. Journal of Public Policy & Marketing, Vol. 19(2), pp. 238-249.

Mothersbaugh, D., Foxx II, W., Beatty, S. & Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. Journal of Service Research, Vol. 15(1), pp. 76-98.

Narayanan, A. & Shmatikov, V. (5 February, 2008). Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset). The University of Texas at Austin.

Norberg, P., Horne, D. & Horne, D. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. The Journal of Consumer Affairs, Vol. 41(1), pp. 100-126.

O´Dea, S. (27 February, 2020). iOT Devices in use worldwide 2009-2020. Statista. Retrieved 20 April 2020, from https://www.statista.com/statistics/764026/number-of-iot-devices-in-use-worldwide/

Ölander, F. & Thøgersen, J. (1995). Understanding of Consumer behavior as a Prerequisite for Environmental Protection. Journal of Consumer Policy, Vol. 18, pp. 345-385.

Parez, S. (19 August, 2019). Developers accuse Apple of anti-competitive behaviour with its privacy changes in iSO 13. Tech Crunch. Retrieved 4 April 2020, from https://techcrunch.com/2019/08/19/developers-accuse-apple-of-anti-competitive-behavior-with-its-privacy-changes-in-ios-13/

Patil, S., Lu, H., Saunders, C., Potoglou, D. & Robinson, N. (23 April, 2016). Public preferences for electronic health data storage, access and sharing - evidence from a pan-European survey. American Medical Informatics Association, Vol. 23, pp. 1096-1106.

Phelps, J., Nowak, G. & Farrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. Journal of Public Policy & Marketing, Vol. 19(1), pp. 27-41.

Privacy Affairs (31 March, 2020). GDPR Fines Tracker & Statistics. Retrieved 11 April 2020, from https://www.privacyaffairs.com/gdpr-fines/

Reuters (26 November, 2019). Data firm broke Canadian privacy laws with involvement in Brexit, U.S. campaigns - probe. Reuters. Retrieved 11 April 2020, from https://www.reuters.com/article/canada-aggregateiq/data-firm-broke-canadian-privacy-laws-with-involvement-in-brexit-u-s-campaigns-probe-idUSL1N2860ZE

Rossow, A. (25 May, 2018). The Birth of GDPR: What Is It And What You Need To Know. Retrieved 8 April 2020, from https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#68197f7455e5

S. (11 May, 2016). What is the Kaiser-Meyer-Olkin (KMO) Test? Retrieved 10 May 2002, from https://www.statisticshowto.com/kaiser-meyer-olkin/

Saunders, M., Lewis, P. & Thornhill, A. (2007). Research Methods for Business Students. (4 Ed.), Financial Times Prentice Hall, Edinburgh Gate, Harlow.

Simmons, D. (17 January, 2019). 6 countries with GDPR-like Data Privacy Laws. Retrieved 10 May 2020, from https://insights.comforte.com/6-countries-with-gdpr-like-data-privacy-laws

Sniehotta, F., Scholz, U. & Schwarzer, R. (2005). Bridging the intention–behavior gap: Planning, self-efficacy, and action control in the adoption and maintenance of physical exercise. Psychology & Health, Vol 20(2), pp. 143-160.

Spiekermann, S. (2005). The Desire for Privacy: Insights into the Views and Nature of the Early Adopters of Privacy Services. International Journal of Technology and Human Interaction, Vol 1(1), pp. 74-83.

Stata.com (n.d.). Factor analysis. Retrieved 10 May 2020, from https://www.stata.com/manuals13/mvfactor.pdf

Sweeney, L. (2000). Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh.

Techcrunch (2020). About Techcrunch. Retrieved 14 April 2020, from https://techcrunch.com

Tresorit (24 April, 2019). Trust in Tech Giants is Broken. Retrieved 11 April 2020, from https://tresorit.com/blog/trust-in-tech-giants-is-broken/

Uber.com (30 April, 2020). Uber Privacy Notice. Retrieved 11 May 2020, from https://www.uber.com/legal/da/document/?country=united-states&lang=en&name=privacy-notice

UCLA (n.d.). What does Cronbach's alpha mean? Retrieved 10 May 2020, from https://stats.idre.ucla.edu/spss/faq/what-does-cronbachs-alpha-mean/

UrRahman, T. (29 June, 2019). Cookies, ITP and how it affects your privacy. Medium. Retrieved 5 April 2020, from https://medium.com/swlh/cookies-itp-and-how-it-affects-your-privacy-7ad39c9de46

Virtual College (2 January, 2018). What are the main differences between GDPR and the Data Protection Act? Retrieved 9 April 2020, from https://www.virtual-college.co.uk/resources/2018/01/the-differences-between-gdpr-and-data-protection

Wang, H., Lee, M. & Wang, C. (March, 1998). Consumer privacy concerns about Internet Marketing.Communications of the ACM, Vol. 41 (3), pp. 63-70.

Wccftech (2020). Wccftech. Retrieved 14 April 2020, from https://wccftech.com

Wivagg, J. (2008). Forced choice. In P. J. Lavrakas (Ed.), Encyclopedia of survey research methods, pp. 290-290. Thousand Oaks, CA: SAGE Publications, Inc.

World Health Organization (12 April, 2020). Cornonavirus disease 2019 (COVID-19) Situation Report - 83. Retrieved 11 May 2020, from https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200412-sitrep-83-covid-19.pdf?sfvrsn=697ce98d_4