Customer Data and Privacy in Norwegian Companies

Companies' perspective on user data and the privacy discourse surrounding it

Sophie Katharina Egeberg Nyborg

Masteroppgave i medievitenskap
Institutt for medier og kommunikasjon
Universitetet i Oslo

15.06.2021

Table of Contents

Abstract

This thesis investigates the process of how large Norwegian companies, specifically Telia and DNB, collect and use customer data and how this is conceptualized. Moreover, it investigates the privacy considerations and concerns discussed within these companies. The data in this study has been collected through in depth- interviews and a document analysis. Through the findings, data collection is portrayed as a multifaceted process that happens across various digital surfaces. The findings suggest data use and collection will become increasingly prevalent, and that we are in an age of dataism where the belief in data is central. Furthermore, that the discussion on customer privacy and data ethics is as relevant as ever. The findings show that the companies view the use of customer data as a prerequisite of future success. Additionally, the GDPR has made the use of customer data dependent on customer trust, and this means that customers' confidence in the fact that their data will not be exploited or misused is viewed as fundamental for the companies.

Forord

Jeg vil utrette en stor takk til informantene som har stilt opp og dermed gjort det mulig for meg å skrive denne masteroppgaven. Videre vil jeg takke veilederen min, Marika Lüders, for støtte og forståelse, god akademisk hjelp og motivasjon gjennom arbeidet med denne masteroppgaven. Jeg vil også takke gode venner, familie og kjæreste for motiverende ord, oppmuntring og deres tro på meg gjennom hele prosessen.

1 Introduction

In this thesis I investigate how companies collect and use user data as well as the privacy concerns that are discussed within the companies. Specifically, I investigate how two of Norway's largest companies, DNB ASA and Telia Norway deal with user data and their motivations behind the process of collecting the data and what they use it for. I will also investigate how the companies view customer privacy and what their discussions surrounding customer privacy are like. As Telia and DNB are subject to General Data Privacy Regulation (GDPR), this thesis will also touch on how GDPR affects the process of data collection. The thesis will base its findings on information obtained through qualitative interviews with employees within the two companies, as well as a document analysis conducted on privacy policies and annual reports.

1.1 Background – Critical viewpoint

In the preface of the 2018 annual report of The Norwegian Data Protection Authority (Datatilsynet), director Bjørn Erik Thon, raises the question: "even if what the companies are doing is legal, is this the world we want?" (Datatilsynet, 2018, p. 5). This question begs an interesting discussion. Companies collecting user data has become a normal part of the digital age we are in. The companies who were the most successful, from a financial perspective, a decade ago have had to make way for technological companies. The most financially successful companies across the world all share a commonality, and this commonality is that they have an immense amount of user data. Thon goes on to say that privacy and ethics are important topics of discussion, as the data the companies are collecting and profiting off is data generated by users. The companies are not only wealthy, but they also have a real influence on society, for example, Donald Trump's election in 2016. There is no question that privacy and ethics are, and have been for a few years, very topical and central themes in the public discourse.

Up until recent years companies viewed paying for data storage as a bad investment, whereas today, companies are mostly data-driven and refraining from paying for data storage could be considered the equivalent of throwing barrels of oil down the drain (Sadowski, 2019, p. 1). The issue is, in this analogy, that the private user data are the barrels of oil. Personal data have become the resource on which the new online economy is based (Couldry and Van Dijck, 2015, p. 3). Personal data includes data that are offered freely by users, as well as behavioral data that is obtained without individuals' knowledge. Fourcade and Healy (2017, p. 9) argue that "modern organizations follow an institutionalized data imperative to collect as much data as possible". Because data *is* revenue. The data users generate are worth so much because they contain excessive amounts of information about people which again can be used for targeted advertising and profiling. Essentially, what is happening is a commodification of private human behavior.

Zuboff's book *The Age of Surveillance Capitalism* (2019) heavily criticizes how companies utilize user data. She condemns Google for exploiting human behavior for economic gain and blames Google of being the pioneer of the misuse of user data. Zuboff argues that Google set a precedent for other companies where it is accepted to "feed on every aspect of every human's behavior" (Zuboff, 2019, p. 18). User data is then being sold in what Zuboff (2019) refers to as behavioral future markets, where essentially what is being traded are peoples' future behaviors. This information is very valuable, both to the companies that are selling the data for large amounts of money, and for the companies willing to pay for it. The information can predict individuals' behavior and can be used for targeted advertising and personalization (Couldry and van Dijck, 2015, p. 3). Fourcade and Healy (2017, p. 16) argue that data is perceived as imperative for organizations, which is why companies will collect data even when they lack the capabilities or knowledge on what to do with it. There will be other firms that will successfully extract valuable information from the data that was collected. Data are analyzed and used to build individual profiles aimed at making a profit by commodifying individual behavior (Fourcade and Healy, 2017, p. 16).

1.2 Terms and definitions

Zuboff has a prevalent presence in the critical research and debate on user data and privacy. In her book, Zuboff presents an eight-part definition of surveillance capitalism (p. 8).

> 1. A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales; 2. A parasitic economic logic in which the production of goods and services is subordinated to a new

> global architecture of behavioral modification; 3. A rogue mutation of capitalism marked by concentrations of wealth, knowledge and power unprecedented in human history; 4. The foundational framework of a surveillance economy; 5. As significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth; 6. The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy; 7. A movement that aims to impose a new collective order based on total certainty; 8. An expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty.

Through her definition it is clear that Zuboff views surveillance capitalism as negative and intrusive on the human experience. Through her use of words like "parasitic", "rogue mutation", "threat", "coup" in the definition, she clearly illustrates her dissatisfaction with how these companies have been, and still are, allowed to operate. Furthermore, her definition highlights the financial focus of the process. Zuboff's views and critical research can be considered to be at the very end of the spectrum in terms of being critical as to what these companies are doing. As a prevalent researcher on the topic her arguments and perspective have garnered much attention and discussions on the topic.

Another term frequently used by Zuboff (2019) is behavioral surplus. This is a term Zuboff uses to describe the added traces that users involuntarily leave when using certain platforms (2019, p. 69). Behavioral surplus can be facts about a user's personalia such as gender, age, religion and political views. These involuntary data are turned into individual profiles which are then sold to advertising companies in, what Zuboff calls, future markets. Through this information companies who collect and analyze this data will be able to know peoples' thoughts and feelings (Zuboff, 2019, p. 71). So, the information extracted from behavioral surplus has been transformed for advertisers to target a specific individual with an advertisement that matches their particular interests.

There are several relevant terms in the literature that attempt to criticize the role of data in business. Couldry and Yu (2018) use the term 'datafication' to describe a process where life-processes are turned into data input streams for computer-based processing. Van Dijck (2014) uses 'dataism' and 'dataveillance'. Data is discussed as a commodity (Zuboff, 2019), a currency (Van Dijk, 2014) and a capital (Sadowski, 2019). The common denominator within the terms is they are all data-driven and imply the increasing importance and value of data. The growth of the digital economy is a central factor through these terms and what they describe. The terms recognize the value of data, while also acknowledging the human and private aspects of the value that is being discussed. 'Dataveillance' denotes a focus on surveillance, where datafication and dataism suggest a process. Dataism can be considered to be a form of ideology, almost a religion, where the importance and value of data is at the center of it. So, datafication describes the process of continuous data collection, and dataism can be considered to be the reason behind datafication. In Zuboff's term "surveillance capitalism" the economic aspect of the process is given a larger point of focus through her use of the word 'capitalism' which suggests an economic system. Where terms such as dataveillance and surveillance capitalism introduces an established and uneven power dynamic, datafication and dataism, particularly dataism, denotes a process of change that involves the public society and is not necessarily limited to organizations. What the terms imply or denote may differ slightly, but the definitions all recognize data as the product that makes these developments possible. The various terms portray the diverse utilization of data and suggest that data is perceived as a valuable resource across several industries with different end-goals.

1.3 Research questions

This thesis will attempt to understand to what extent, and how, the companies behind the invisible wall of data processing themselves problematize and/or recognize an issue with something that has become so, as Van Dijck states (2014, p. 197), "nestled into the comfort zone of most people".

I will conduct my research from the perspective of the companies, rather than the customers. I will be investigating the process of data collection and use, as well as attempt to gain a perspective on companies' reasoning and motivation behind the process of data collection and use. Furthermore, I will also investigate how the companies take customer privacy concerns and protection into consideration through this process.

My overarching thesis question is as follows:

How do companies conceptualize data collection and use, and how central is customer privacy in this conception?

My three focused research questions are:

- What is their primary motivation in gathering customer data?
- How is this data gathered?
- What are their main privacy concerns?

1.4 Privacy in the digital age

The Information and Communication Technology (ICT) industry is steadily growing, evolving and increasing in users (Berbers, Hildebrant, Vandewalle et al., 2018, p. 6). In fact, it is now even more widespread than electricity, reaching three billion of the seven billion people on earth (Zuboff, 2019, p. 17). Individuals constantly leave data traces through living their everyday lives (Mai, 2016, p. 192). Through activities like shopping, reading the news, listening to music or communicating with friends and family, personal information is revealed about individuals (Mai, 2016, p. 193). As a result of this, the amount of user generated data is almost inconceivable, furthermore, only a concentrated few big companies own close to all the data (Berbers, Hildebrant, Vandewalle et al., 2018, p. 6). The perspective seems to be that the more data organizations have, the better their services and advertisements will be (Mai, 2016, p. 194). As data is personal information, this knowledge allows organizations to offer customers personalized and relevant advertisements and services (Mai, 2016, p. 193). Hence, companies attempt to collect as much information as possible to offer their customer the best service possible. While the technological advances easily let people share personal information, there is a privacy issue, because once the personal data is shared it is almost impossible to retain control over it (Pelteret & Ophoff, 2016, p. 279).

The private information gathered is not only valuable to companies whose primary motive is financial gain. According to Zuboff (2019, p. 99) the terrorist attack on 9/11/2001 changed how the US government viewed privacy. After 9/11 the US government's focus was no longer on privacy, but on security (Zuboff, 2019, p. 99). The interest in Google was deemed a necessity and in 2002 when the Total Information Awareness program was launched, they relied heavily on Google to provide them with the information they required. If terrorist organizations planned attacks on the US, they would leave digital traces in the information spaces, which is why the US government halted all plans working on regulating the industry. Zuboff's (2019, p. 99) contention is that through the lack of laws and regulations after 9/11 surveillance capitalism was allowed to flourish.

An incident that sparked a public discussion on privacy, in 2013 Edward Snowden, a CIA-analyst, released documents detailing the privacy invasion that was happening that he no longer felt comfortable taking part in (Van Dijk, 2014, p. 197). The whistleblower wished to start a conversation surrounding privacy and personal data through revealing the extent of the government surveillance on the public. Snowden's leak may be a contributing factor to why regulation was put on the authorities' agenda.

Couldry and Yu (2018) argue that discussing personal data as 'raw' material that has no intrinsic value contributes to the naturalization of data. Data are compared to natural occurring materials such as water and oil, because their value occurs through human intervention, and it is the same for personal data (Couldry and Yu, 2018, p. 4477). Collection and use of personal data have potential negative impacts for the autonomy and privacy of the data subjects. The value extracted from the data is based on and generated by persons, their beliefs, behaviors and other personal information (Sadowski, 2018, p. 6). This means that to accumulate data there are invasive methods in place that track and monitor individuals (Sadowski, 2018, p.7). As such, Sadowski (2018, p. 2) argues that a more apt terminology when referring to data mining, which implies that data exists as a natural resource to be discovered, is data manufacturing.

Globalization can have positive effects on humanity, but it can also create issues for people (Romansky, 2019, p. 95). Privacy is recognized as a fundamental human right by many international regulations and documents, among them are the United Nations Declaration of Human Rights (Romansky, 2019, p. 98). The growth and development of technologies that allow the processing of large personal data has led to developments of regulations that attempt to legislate the use of data and ensure that privacy of persons is still upheld and protected. Pelteret and Ophoff (2016, p. 279) state that privacy is difficult to define, not just because it is a complex term in itself, but because it is a dynamic one. Since the basic principle of privacy was formulated, its meaning has been reconceptualized a number of times (Mai, 2016, p. 194). Societal, political and technological developments are changing its meaning (Pelteret and Ophoff, 2016, p. 279). Romansky (2019, p. 104) argues that the traditional view of privacy as “the right to be alone” is changing in the digital age and moving towards viewing privacy as “the right to be forgotten”.

1.5 GDPR as a regulatory framework

As this thesis discusses privacy and data in Norwegian companies who are subject to the General Data Protection Regulation (GDPR), I will include some more background information on GDPR in the theory chapter of this thesis. This is important because what holds true for Zuboff and other critical researchers’ arguments on data use and privacy within companies like Google, Facebook and Amazon might not be transferable in this study as Norwegian companies do not have the same liberties that companies outside of the GDPR do as Norwegian businesses are subject to strict rules and regulations due to GDPR.

The European Union (EU) enforced the GDPR in May 2018 (Zuboff, 2019, p. 378). In effect, the EU’s approach to data activities contrasts to the United States because companies must justify their use and collection of data within the GDPR framework. The regulation attempts to regulate the free movement of personal data. It focuses on regulating individuals’ fundamental rights and freedoms, and especially in regard to their personal data (GDPR, 2016).

1.6 Telia Norge and DNB ASA as case studies

This study seeks to contribute to the existing theory by examining how and why two major companies in Norway collect data. I initially wanted to include Telenor, but the interview eventually fell through, and I ended up investigating Telia and DNB. I will investigate the companies’ primary motivation for data collection and use, as well as gaining insight into what privacy concerns and considerations the companies are discussing. As they are subject to GDPR, looking at companies in Norway is interesting, and this will offer a contrast to the research where American companies are discussed in discourses surrounding data and privacy. In addition to being subject to GDPR, the companies this thesis is investigating, although large Nordic companies, are significantly smaller in size than Google, for instance. The business model is also very different, and data is not the main objective or source of revenue for Telia or DNB. However, both companies are of a significant size and process extensive amounts of customer data.

1.6.1 Telia Norge

Telia Norge is a telecom company and was previously called NetCom, before changing the name to Telia Norge after being acquired by Telia Company in 2016. Telia Norge refers to themselves as "Norway's biggest challenger". Telia Norge has around 3,2 million customers, and thus, Telia has access to large amounts of customer data, which is why Telia is a relevant company to investigate.

1.6.2 DNB ASA

DNB is Norway's largest financial institution. DNB has around 2,1 million customers. As a financial institution DNB has access to extensive amounts of data regarding customers which is why I was interested in conducting an interview with DNB ASA.

This concludes Chapter 1. Chapter 2 will discuss theories and frameworks as well as previous research on the topic. Following from this Chapter 3 will discuss the methods used. Chapter 4 will present the results and analyze the findings, then Chapter 5 will discuss the findings in light of relevant theory. Finally, Chapter 6 will include a summary and conclusion of this thesis.

2 Literature and Theoretical framework

In this chapter I will discuss relevant theory and literature and attempt to point to what has already been researched and what knowledge might be lacking in the area of research I will be investigating.

2.1 Literature review

This literature review will include and explain previous research. This thesis seeks to explain why and how businesses use customer data and as such the relevant articles from a business and managerial side are included in this literature review. Furthermore, as businesses often make decisions with their customers in mind, this literature review will also include research from the user perspective. The literature review is categorized into relevant subchapters.

2.1.1 Big data in business

Big data has been recognized as one of the most important areas of future technology (Raguseo & Vitari, 2018, p. 5206). The way businesses are interacting with big data is changing the way these companies operate (Raguseo, 2018). There are major benefits for data-driven companies. McAfee, Brynjolfsson, Davenport, Patil and Barton (2012) found that companies who actively use the information gained from big data generally perform better business-wise. Management strategies are changing as a result of big data. Data-driven companies can make business decisions based on evidence, rather than intuition and, thus, improve their business. Data allows businesses to gain insight, analyze and measure and in general, know more about their company and their customers (McAfee et al., 2012, p. 4). By analyzing and understanding consumer patterns companies can cater to individual consumers' preferences, and thus, big data also give rise to a new meaning of customer service. Furthermore, an increase in customer satisfaction is often found to have a positive relationship with financial performance (Raguseo & Vitari, 2018, p. 5210). Analyses of the data could increase an organizations' knowledge on their customers through an improved understanding of their customers' needs and wants. This knowledge can be utilized to increase loyalty and create an improved customer experience. From the knowledge accrued by data analyses, organizations can improve their decision-making, customer satisfaction and general performance. McAfee et al. (2012, p. 9) argue that companies who make decisions based on data make better decisions, and that managers who doubt this fact will likely be replaced by someone who will embrace it.

For businesses to benefit from all the data that are being collected they need to develop strategies for maximizing and optimizing the advantageous information that can be found by managing the data correctly (Raguseo, 2018). However, Raguseo (2018) argues that the process of implementing big data strategies can be complex. Raguseo (2018) investigated both risks and benefits for companies implementing big data strategies. She identified four different types of benefits: transactional, strategic, transformational and informational. The four types each have different benefits that are related to it. Through her survey it was discovered that the transactional benefits and motivations ranked the highest by the companies that participated is increased productivity growth, as well as a reduction in operation cost. In terms of strategic benefits, the most recognized benefit is related to improving services and products. The most frequent transformational benefit that was identified by the participating companies was that big data facilitates an expansion of a company's capabilities. Finally, the informational benefit that was ranked the highest related to data management, easier access to data and data accuracy. Businesses also have to take potential risks into consideration when implementing big data strategies (Raguseo, 2018). Through her survey Raguseo (2018) found that privacy and security issues were the two risks that were ranked the highest by companies wanting to implement big data strategies. To successfully implement big data strategies businesses have to invest in new technologies and enhance their general ability to manage big data. Moreover, businesses have to increase their awareness and capabilities of managing the risks that are associated with processing user data (Raguseo, 2018).

Understanding how much value individuals assign to their privacy is important from a business perspective (Acquisti, John, and Loewenstein, 2013, p. 249). Companies can use that information to decide whether it is a strategic business move to invest in systems that enhances customers' privacy and use that as an advantage in a competitive market, and also be aware of the adverse effects of not doing so. Companies often have their own privacy policy and Acquisti, John and Loewenstein (2013, p. 250) also argue that policy makers benefit from knowing how much money is worth putting into consumers' privacy, and the only way to really know this is to know how much individuals value their privacy. Knowing how much individuals value their privacy will aid them in knowing which policy change they should prioritize, and whether the policy change should include increased security at the price of increased administrative costs or not. Essentially, it is important to understand how individuals value their privacy because this will provide companies with clues as to what they should be prioritizing in terms of privacy considerations.

Morey, Forbath and Schoop (2015) argue that companies who are transparent with customers will benefit from this transparency in the long run, as transparency increases user trust. Further, they contend that companies who continue to keep their customers in the dark will eventually lose their customers due to a lack of trust. Their research found that consumers are aware they are being surveilled and that the anxiety levels are high, and consequently customers who are given a choice will go with the companies that lets users gain control over generated data will be more successful in the long run. Morey, Forbath and Schoop (2015) identified three different types of data collected by companies in their analysis: (1) self-reported; information users enter, like email, age and gender etc, (2) digital exhaust; browsing history and location data etc, (3) profiling data; which is data used to make predictions about individuals' future behaviors. Their analysis revealed that customers are the most worried about profiling data, which is a combination of self-reported data and digital exhaust. However, they also found that what the companies were using the data for mattered. They identified three categories: (1) improving a service or a product, (2) facilitating targeted marketing or advertising, (3) generating revenues through resale to third parties. They found that customers feel compensated when their data is used to improve a service. However, customers do not feel it is a fair trade when their data is being used for targeted advertising and especially not when it is sold to third parties. Customers expect compensation for such trades, and companies who sell data to third parties have an especially high bar to clear. They also found that trust is key when dealing with user data; the more trusted a brand is the more willing customers are to share their data. Ultimately, transparency was found to build trust, so best practice for companies would be to build trust with customers through transparency.

2.1.2 How the lack of government regulations promoted surveillance capitalism

Zuboff (2019, p. 92-93) argues that the inability of the government to follow Google's fast paced developments is a "critical success factor" of surveillance capitalism. Google's view on the topic claims that any attempts at regulating the corporations would therefore be deemed a negative force as this “freedom from law” is necessary in the context of technological innovation. Former CEO of Google, Eric Schmidt has spoken about the topic and has been quoted in a 2010 interview with the Wall Street Journal saying Google does not need any government interference or regulations due to its “strong incentives to treat its users right”. In Business Insider in 2011, Schmidt stated that the government really ought not to try and slow them down as they’ll “move faster than any government”. Larry Page, co-founder of Google, was quoted saying “old institutions like the law and so on aren’t keeping up with the rate of change that we’ve caused through technology…” in 2013. He further argued for innovation in “safe places” so new things could be tried out and figure out its effect on society. Zuboff explains their motivation for wanting to be exempt from any law due to such laws being potential threats to the free flow of behavioral surplus. One could argue that Google’s stance sets a dangerous precedent where the public accepts companies’ arguments of them not being able to innovate if they are being held back by governmental regulations. To understand what makes this possible we need to go back to 1996, when section 230 (p. 96-97) was passed. Essentially, it states that websites are not publishers and the sites nor their users can be held accountable as such. Some form of regulation on platforms was encouraged to keep obscenities off the internet, but without the risk of legal sanctions should some inappropriate user generated content circumvent the regulations in place. This provided ample opportunity for self-regulation and Zuboff argues that it was exactly what was needed for the growth of surveillance capitalism to flourish.

2.1.2 Research from a user perspective

An important part of understanding the topic is through the user perspective, as the user perspective is a motivational factor in companies’ business strategy and decision making. Sheng, Nah and Siau (2008, p. 351), identified privacy concerns in users as the biggest obstacle in the adoption of ubiquitous commerce. Ubiquitous commerce refers to “anywhere, anytime” commerce (Sheng, Nah & Shau, 2008, p. 344). Personalization allows businesses to offer customers products and services based on their interests, identities and preferences and has been identified as a key factor in ubiquitous commerce. By having information that lets businesses understand their users the business can be more successful in predicting what the user is interested in buying and produce more successful and relevant sales for customers. Sheng, Nah and Siau (2008, p. 364) state that although personalization can benefit the user, their privacy concerns increase with the use of personalization as the users recognize the sacrifice of personal information that personalization is contingent on.

Barnes (2006) investigated young individuals' apparent lack of privacy concern on social networking sites (SNS). She found that young people do not necessarily realize that they are participating and sharing private information in a public space, as they lack the ability to recognize when something is private and when it is not. She argues that it will require a collective effort from parents, education facilities, legal policies, as well as making an individual effort to learn about how to correctly protect one's privacy.

Andrejevic (2014, p. 1685) findings show that people feel powerless against the big data companies. Users lack information that allows them to comprehend the processes surrounding data collection and use, and thus, feel frustrated as they do not feel as if they have a choice. One study found that if an individual were to read the privacy policies they encountered over a year, they would have to spend 8 hours over 76 days (Sadowski, 2018, p. 7). As a result, people often click agree and consent to data collection even though the consent is not likely to be meaningful or informed. Acquisti, Brandimarte, and Loewenstein (2015, p. 509) question whether individuals are capable of managing their own privacy in a rapidly evolving landscape in the information age. As data collection in the digital age is happening through less obvious and covert methods, individuals lack awareness on how much information on them is collected. Following this argument one can logically assume that when people lack general knowledge on how their data is acquired, they do not fully comprehend how to protect or prevent their information from being collected. As Andrejevic (2014) findings point out this lack of knowledge results in frustration from the users, which supports Morey, Forbath and Schoop's (2015) contention that companies and users would benefit from transparency.

Benisch, Kelley, Sadeh and Cranor (2010) found that the less complex peoples' privacy settings were, the more likely they are to protect their privacy and share less. They state that this is due to the fact that when the privacy settings are simple people tend to be more cautious and restrict sharing to be safe. Whereas, when met with more complex privacy settings, individuals can accurately restrict their personal privacy concerns. This would allow users to deny sharing some information they find particularly sensitive and allow sharing for other information they might not view as a concern. Different persons are likely to have different privacy preferences. Therefore, Benisch et al. (2010), state that it would be beneficial to companies to present users with more complex and accurate privacy settings as a way of encouraging privacy-sensitive users to share more.

Personalized systems have become a massive focus for businesses with the rise of technology. The personalized systems analyze consumer behavior which lets businesses provide customers with products, advertisements and offers that are targeted to a specific user and their preferences (Teltzrow & Kobsa, 2004, p. 1). There are benefits to personalization, such as users experiencing a more relevant product display catered to their personal preferences (Knijnenburg et al., 2012, p. 442). However, while personalization is commonly accepted by users, some users do not enjoy it and might discontinue an internet behavior when faced with an offer to get more personalization at the price of giving away more data (Zhu, Ou, van den Heuvel and Liu, 2017, p. 427). Teltzrow and Kobsa (2004, p. 2) stated that finding the right balance between privacy and personalization is a challenge. There are varying privacy concerns between users, and Kobsa (2003, cited in Teltzrow and Kobsa, 2004, p. 13) proposes an individualized method of data collection where different users are allowed to change their privacy settings to match their own privacy preferences. This has been implemented in some capacity in the implementation of GDPR, where users can more easily opt out of certain types of data collection. Teltzrow and Kobsa (2004, p. 13) also demonstrated that user privacy concerns have a direct impact on the adoption of personalization systems. This is because some users will refrain from online activities, such as online shopping if their privacy concerns are too high. Privacy concerns in users and their subsequent behaviors are also dependent on the situation or the domain in question (Menard & Bott, 2020). For example, studies have shown perceived benefits to neutralize privacy concerns in cases where the perceived benefits are high and can override the perceived privacy loss. This neutralization of privacy concern is found to be higher in the Internet of Things (IoT)- domain. This might be explained by the fact that adoption of smart-home appliances is generally perceived as more beneficial than internet related benefits.

Paul, Scheibe and Nilakanta (2020), investigated users perceived privacy risks, specifically in regard to fitness wearables, and the effect of GDPR on users perceived privacy risks. The results showed that users who view privacy policies as effective experience an increased control over their online privacy (Paul, Scheibe and Nilakanta, 2020, p. 4394). Thus, the more information a user is given about data collection, processing and use, the less the perceived loss of privacy control is. Essentially, GDPR compliance results in a decreased perceived privacy risk by the user.

2.1.2.1 The Norwegian public's views on privacy and knowledge of GDPR

To offer some background and understanding on how the Norwegian public view privacy, I will include results from a survey conducted by the Norwegian Data Protection Authority. The Norwegian Data Protection Authority released a survey where they mapped out the Norwegian public's knowledge of GDPR and their opinion/attitude of privacy. The data was collected between the 15th and 28th of November 2019 and published on the 11th of August 2020. Through their research the Norwegian Data Protection Authority found that two out of three people were aware of the new regulations. However, they found that this number was significantly lower for people with lower socioeconomic status. Furthermore, people have more trust in public companies over private businesses. The survey also revealed that half of the people included in the survey have refrained from using a service due to being worried that their privacy is compromised. Furthermore, the survey revealed that close to seven out of ten do not feel they are in control of their privacy information online and lack knowledge on how it is being stored and collected. There is also a consistent negative attitude towards the business model that the internet services are based on. Very few people (eight percent) are positive to targeted advertising, whereas three out of four people are negative. Eighty-four percent of the participants are negative to Google and Facebook's entrance into the financial sector and do not like the idea of giving them their financial information. Furthermore, the IoT allows technological devices that are on the same network to "communicate", and half of the participants were skeptical as to how smart-house devices collect and store information in a way that protects the user's privacy. 'Social cooling' is a term coined to describe the negative effect that big data can have on our behaviors. The results from the survey found that a large amount of the participants engages in self-censorship online due to skepticism and distrust towards governmental surveillance, self-censorship being an example of social cooling.

The results from the survey conducted by the Norwegian Data Protection Authority are important because they could, in fact they should, impact on how companies communicate their privacy policies. The results imply that individuals are more likely to trust public companies over private companies is interesting and perhaps an increase of transparency from private companies could improve this. Furthermore, half of the participants have refrained from using a service due to privacy concerns. This information is also something I would assume companies would be interested in, so they can implement strategies that can decrease the users’ privacy concerns. The fact that seven out of ten do not feel like they have enough knowledge on how their information is collected, stored and what it is used for should act as a sign for the companies to be more public and explanatory to the general public on this topic. Especially companies who promote transparency as something they focus on should take the results of this survey into account.

2.1.3 The effect of GDPR

As previously mentioned, the GDPR attempts to give users more control in the process of data collection and the consequent distribution and use of such data (Sørensen & Kosta, 2019, p. 1590). As the GDPR covers any business that collects or distributes data on EU citizens irrespective of the location of the organization its effects can be seen worldwide (Zaeem & Berber, 2020, p. 1). The EU’s regulatory response to recent Big Data scandals has been progressive with the launch of GDPR (Andrew & Baker, 2019). They argue that it is viewed as the new ‘gold standard’ on data protection laws. GDPR will impose fines for companies who do not comply. The privacy regulations in Europe stand in contrast to the US. However, the effect of GDPR crosses European borders, as all companies who track or provide services to European citizens are subject to GDPR (Bonatti and Kirrane, 2019, p. 7). As a result, businesses across the globe had to make changes to their process of data collection and distribution (Zaeem & Berber, 2020, p. 2).

Prior to the GDPR, which came into effect in 2018, there had been made no changes to regulations regarding data protection since 1995 and the Data Protection Directive (Andrew & Baker, 2019, p. 570). As a consequence of having no changes made since 1995 the new regulations meant quite a big change for every business that collect and/or use private data. A big reason for the creation of GDPR was to limit the largest players in the Big Data market. Basically, the GDPR requires the data collectors (it assumes data collectors wish to collect and process personal and identified data sets) to follow four principles that are in place to protect their data subjects (Andrew and Baker, 2019, p. 571). The first two relate to data collection, and the second two to data processing. The first principle: data minimization simply means that when collecting data sets it is limited to the data that is necessary for what it is purposed to. In essence, collect as little data as possible. It is worth noting that GDPR categorizes “normal” personal data, which is data that includes “name, location, ID numbers, IP address, and economic information” differently to what is termed “special categories of personal data”, such as data that “reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life”. The more special, or sensitive, data is generally prohibited from being collected except for very specific and controlled circumstances that involve explicit consent from the user. A common method for obtaining that consent is through a pop-up window where a user should be given options of what information they consent to being collected (Machuletz & Böhme, 2020, p. 481). Machuletz and Böhme (2020, p. 494) found that these pop-up windows often are deceptive in their presentation and that this can trick the users to agree to more data collection than was intended.

Sanchez-Rola et al. (2019) found that GDPR had made a global difference in website behavior. However, they found that tracking remains ubiquitous, and that cookies could identify users when visiting more than 90% of the websites in their sample. The study also revealed that many websites are deceitful in their presentation of information, making it difficult for users to avoid being tracked. Furthermore, they found that few websites provide users with a possibility of opting out from tracking. Zaeem and Berber (2020) investigated the impact of GDPR after its implementation by comparing privacy polices before and after GDPR. They (2020, p. 18) found that the effects of GDPR have generated progress in data protection and regulation, but that further work is necessary. One particular area that privacy policies can improve is granting users the right to edit, update and delete their data so as to fully be in compliance with the GDPR (Zaeem & Berber, 2020, p. 18).

Sanchez-Rola et al. (2019, p. 10) speculate that websites which are not in compliance with GDPR are aware that the revenue loss they could face from allowing users to easily opt-out is larger than the possible fine they could receive. As many websites earn most of their income from advertising, the potential fines from incompliance with GDPR do not act as a method of prevention as the loss of revenue they could face if they did comply with the GDPR. However, the financial aspect is one factor, another important factor to recognize is the potential harm of reputation that businesses who do not comply with GDPR guidelines may experience.

Paul, Scheibe and Nilakanta (2020, p. 4389) identified privacy policies as one of the best ways for corporations to address a user's privacy concern. However, for this to be true, the privacy policy needs to be comprehensible and transparent. Furthermore, they found that GDPR acts as a mitigating factor and reduces the perceived loss of privacy control as the GDPR safeguards users' fair and transparent data management (p. 4394). This means that users are more likely to trust companies who are subject to governmental regulations such as GDPR.

Many companies rely on personal data analyses as a means of generating a big part of their revenue, and the task for them after the implementation of GDPR is to maximize the usage of user data within the limits of GDPR (Bonatti and Kirrane, 2019, p. 7). As the GDPR by default states that personal data shall not be processed and it encourages the use of anonymous data, Bonatti and Kirrane (2019, p. 7) state that companies whose revenue benefitted from the use of personal data are now looking at the legal basis that allows them to continue using and processing personal data. One such legal basis is explicit consent from the data subject. By obtaining explicit consent from users, companies would still be allowed to use personal data under GDPR.

2.1.4 Research gap

There is quite extensive research on the topic of big data in business. There are many research articles investigating the benefits and potential risks of using data in business. However, I wish to contribute to the existing research literature by investigating how Norwegian companies view data use and how they protect and discuss their customers' privacy while simultaneously building data driven companies. On one hand, companies like Telia and DNB cannot really be compared to companies such as Google, because the business model of Google relies on user data to generate income. Through advertising revenue, data is essentially how Google makes money. Telia and DNB have paying customers who expect to be delivered good services and products, and their business model is still primarily based on customers paying for a product. However, I thought it would be interesting to look at companies who have extensive amounts of data, and a lot of sensitive information about their customers, and to investigate what they are doing with these data as well as what ethical questions are being discussed in order to safeguard customer privacy. Furthermore, GDPR has further promoted a discussion on user data and it is interesting to see how that has affected the companies use of customer data. Why are they collecting it, what are they using it for and do they have any privacy concerns regarding the use and collection of customer data?

2.2 Theoretical framework

The theoretical framework discusses relevant literature on the topic and will provide a theoretical framework for my discussion.

2.2.1 Critical views of surveillance capitalism

Zuboff (2019, p. 83-84) paints a bleak picture of the current digital age we are in. She contends users are no longer subjects, nor are they products, but rather, objects. Objects from which raw material is being extracted and taken to be used in prediction factories. She blames Google for being the pioneer of surveillance capitalism, and that they set a precedent for other companies handling user data and how to generate revenue from it. Silverman (2017, p. 149) argues that human objectification is at the center of this new paradigm. He states that while businesses and authorities have become increasingly opaque, individuals have become more transparent. This suggests that while businesses and authorities gain increasingly more information on individuals, people know increasingly less about the processes and motivations of the businesses and authorities.

Zuboff (2019, p. 18) argues surveillance capitalism revives Karl Marx' idea that capitalism is the vampire that feeds on manual labor. Moreover, she states it is even worse as surveillance capitalism preys on every aspect of the human experience. This might be because the surveillance even penetrates the most intimate private spheres, as phones and other gadgets are always carried and tracks people's physical movements, as well as digital ones like shopping patterns and search history. Silverman describes the smartphone as a personalized surveillance device that is constantly gathering personal information (2017, p. 153). Information that is highly valuable because it allows marketing companies to target their advertisement specifically to the individual.

As previously mentioned, there are various terms that have commonalities and many that have researched the effect of commodifying personal, private data. For example, van Dijck (2014, p. 204) refers to the movement almost as a religion or an ideology which she calls dataism. Dataism can be described as a religion or ideology where the belief is placed in data, rather than a deity. Van Dijck (2014) uses dataism to explain the, perhaps naïve, trust that the population inhabits in their governments and the private corporations that collect their data. Through dataism, much like surveillance capitalism, behavioral data is viewed as raw material waiting to be analyzed and processed into predictive models and algorithms about future human behavior (van Dijck, 2014, p. 201). According to van Dijck (2014, p. 202) dataism relies on user trust to further its paradigm and persuasive logic. There are various actors with a belief in big data that value the data differently. While some large corporations view big data as a way of generating revenue, governmental institutions see the value of surveillance that data collection permits, and researchers see big data as a method of learning more about human behavior (van Dijck, 2014, p. 203). A second part of dataism, van Dijck (2014, p. 204) argues, is the trust and belief that technological companies and government agencies who collect data will protect the data from exploitation and misuse. Through the success of dataism as a belief system, datafication grows. Dataism can be viewed as the thought and reasoning behind the process of datafication.

Sadowski (2019, p. 6) argues that the process of collecting data is closely related to surveillance and refers to it as dataveillance. The data that is collected contains information on people; their behaviors and their beliefs, so through the process of collection one gains access to people. Dataveillance is a more appropriate term as it is the act of surveillance through personal data. Furthermore, Sadowski (2019, p. 6) criticizes the use of terms such as ‘data mining’, because it implies that data is a resource waiting to be discovered, such as oil. He suggests a more accurate term is data manufacturing because it acknowledges that data is created and valorized by people using technology. Sadowski (2019, p. 4) argues that data can be viewed as a capital in its own right, albeit with its roots in economic capital. He argues for its distinction from economic capital as its primary motive is not necessarily monetary. Sadowski (2019, p. 7) argues that when data is perceived and treated as capital, the primary motive becomes to collect as much of it as possible through any means possible. He argues that the extensive collection of data influences business models, political governance and technological developments. Recognizing data as a form of capital, Sadowski (2019, p. 1) argues, can conceptualize it and impact on the way it is understood and researched.

Fourcade and Healy (2017, p. 26) discuss how data can be interpreted as truth when it may be much more complex. To illustrate, data are not able to present the complexity behind choices or reasons for behaving a certain way online. Fourcade and Healy (2017, p. 26) use the example of missing or making a bill payment. Someone may miss this payment due to an unforeseen circumstance, for example an accident or a familial crisis. Whereas someone else may be able to pay it due to having parents that are financially able to help pay their bills. Data do not differentiate, and a case of a missing bill payment will only be coded as someone being financially wise or not, because data do not reveal the reasons behind the outcome. Data can be used as an indication of a person's character, when in fact, a person's character and their reasoning for behaving a certain way are often highly complex. As such, it is important to acknowledge and be aware of the limits that exist in data and the analyses.

Couldry and Yu (2018) highlight the ethical issues that may arise through datafication. Datafication is the constant collection and processing of data through everyday life streams and transactions and the transformation of those into quantifiable data (Van Dijck, 2014, p. 198; Couldry and Yu, 2020, p. 1). Mejias and Couldry (2019, p. 3) argue that two vital elements of data production are, firstly, the external infrastructure from which the data is collected, processed and stored. Secondly, the process of generating value from the data. Essentially, the process combines the transformation and quantification of human life and the valorization of those data. Couldry and Yu (2018, p. 4474) explain that attempts to regulate the use of personal data, for example GDPR, may not be protective enough in regard to the collection of said data. Further that regulatory frameworks', such as GDPR, effectiveness is limited where consent to data collection has already happened or where there is a contract in place where data collection is necessary to meet the terms of the contract. Couldry and Yu (2018, p. 4475) point out that situations where people have to agree to data collection to gain access to a service are permeating larger and larger areas of people's lives. Furthermore, they (2018, p. 4486) argue that the collection of personal data is in contrast with basic human autonomy and democratic processes. Couldry and Yu (2018, p. 4487) argue that it is necessary to deconstruct the current discourse on data collection. The current discourse on data collection views data collection as something natural, when in fact, perhaps it should not be. The discourse on data collection has identified data collection as natural through referring to data as “raw material with value” (Couldry and Yu, 2018, p. 4476). Therefore, they argue, that if it is at all possible that continuous data collection infringes on individuals’ right to autonomy and privacy, there needs to be a discussion on the topic.

2.2.2 Privacy

Kokolakis (2007, p. 123) distinguishes between three aspects of privacy, (1) territorial privacy, which is related to the privacy in the physical space surrounding an individual, (2) privacy of a person, which is related to protecting individuals from unwarranted interventions, and (3) informational privacy, which is related to how personal data is collected, managed and distributed. This thesis delimits the term privacy to the aspect of privacy regarding informational privacy as that is the relevant definition.

2.2.2.1 Privacy paradox

Efficiency has been described as the “holy grail” of surveillance capitalism (Silverman, 2017, p. 153). This points to the efficiency privacy trade-off where people might recognize that some of their privacy is being compromised, but they are willing to let go of it to maximize and streamline efficiency in their day-to-day lives. Privacy concerns among the population have consistently been found to be high. However, the following actions across the population do not match the expressed privacy concerns (Hoffman, Lutz and Ranzini, 2016). So, there is a discrepancy between the apparent attitudes and observable behaviors. This has been called the privacy paradox, and it alludes to the issue of caring about privacy until it starts being inconvenient. The technological advances are making it very easy for people to give up a lot of private information, in order for them to have an easier and more convenient life. The privacy paradox describes a personal battle between efficiency and privacy concern.

Kokolakis (2017) conducted a review on the current research done on the privacy paradox. He found that the two important factors in the privacy paradox, privacy concern and privacy attitudes, are fundamentally different. Further, he makes an important distinction between privacy intention and privacy behavior. This is because the intention to protect one’s privacy, does not equate behaving in a way that protects one’s privacy. Some of the studies included in his review have investigated privacy intention, not privacy behavior. Acquisti (2004, p. 27) presents a model where he partly explains the privacy paradox by using the human bias of immediate gratification. He proposes that the immediate benefits of overlooking one's privacy are greater than the potential future privacy risks. Acquisti (2004, p, 23-24) also describes that individuals' faced with a privacy decision are met with three problems, (1) incomplete information, this relates to the potential lack of information surrounding the complex concept of privacy (2) bounded rationality, which begs the question of whether an individual is able to calculate all the parameters related to the choice, and finally (3) psychological distortions, which details the many biases humans may fall victim to. Put simply, humans lack all the necessary information to make an informed decision, and even if the information was available individuals might struggle to process it, and finally, even so humans tend to often behave in a way that directly opposes their better judgement. Kehr et al's., (2015, p. 626) findings similarly suggest that the privacy paradox, often referred to as a gap between intention and behavior, might be more precisely described as a gap between intention and attitude. Kehr et al's., (2015) findings suggest that the privacy paradox can be explained through biased intention forming. Although people may have pre-existing privacy attitudes, an individuals' privacy intention is often determined by situational cues, such as affective thinking, when met with a privacy-decision making process. These situational dependent cues can override the pre-existing privacy attitude and directly influence their actual privacy behavior. Kehr et al., (2015, p. 624) also state that a person's ability to behave rationally when met with a privacy decision making process is limited by psychological limitations. Acquisti (2004, p. 27) concludes, by stating the solution to the privacy problem is a combination of policy regulations, awareness and technology.

Dienlin and Trepte (2014) were able to eliminate the privacy paradox when operationalizing the term in a new approach that differentiates between social, psychological and informational privacy, and by investigating privacy attitudes and privacy intentions as well as privacy concerns. Their findings suggest that online privacy behaviors are directly influenced by privacy attitudes (p. 45). Rather than concluding that their findings explain the privacy paradox and why it exists, such as Acquisti (2004) and Kehr. et al (2015) did, Dienlin and Trepte (2014, p. 45) conclude by stating that the privacy paradox is a relic of the past.

2.2.2.2 Privacy in organizations

Organizations who process personal data should be interested in the impacts of privacy, as user privacy concerns can ultimately have an effect on the success of a company (Bélanger and Crossler, 2011, p. 1029). Making a decision on privacy can be as difficult for an organization as it is for individuals (Pelteret & Ophoff, 2016, p. 291). Moreover, how companies view privacy differs between organizations. While some companies provide users with significant amounts of privacy protection, other companies may not view that as equally important (Bélanger and Crossler, 2011, p. 1029). An organization's view of privacy is likely to be a multifaceted process of which factors like ethical and legal issues as well as information management determine the outcome (Pelteret & Ophoff, 2016, p. 291). The continuous legal, technological and societal developments also affect the organizations as they have to continuously inform their privacy management.

As there are multiple issues that can arise from sharing personal information, privacy concerns in users will impact on their decision-making process when deciding to share or not share their private information (Pelteret & Ophoff, 2016, p. 284). Trust allows consumers to feel safe being vulnerable, as there is an expectation for the company to not behave opportunistically and in a way that contradicts that trust (Mou, Shin & Cohen 2017, p. 257). Martin (2018) found that consumers experienced a decrease in trust in firms who violated privacy expectations. This decrease in trust is not necessarily easy to build back up, as the integrity of the firm is diminished. Furthermore, Martin (2018) found that the more experienced technologically consumers are, the more they tend to care about privacy factors. As Andrejevic (2014) and Acquisti, Brandimarte, and Loewenstein (2015) point out there is an asymmetry between the methods companies use to collect data and the knowledge of these methods within the public, this discrepancy leads to consumers feeling frustrated. This frustration can lead to customer dissatisfaction which can have a negative impact on the organization. Maintaining a positive relationship with customers is important for company success.

Establishing a trustworthy privacy culture can benefit organizations (Pelteret & Ophoff, 2016, p. 292). By being more transparent with how data is used and more careful about how a company expresses their privacy attitude users will be able to make more informed and conscious privacy decisions. The organization is also likely to benefit as the users will feel less frustrated the more knowledge they have. Companies can also benefit from their customers’ trust, especially in cases where competitors might not be seen as trustworthy by their users (Pelteret & Ophoff, 2016, p. 292). Building trust, thus, may lead to a competitive advantage for the companies.

2.2.3 Why government regulations matter

Through reading the literature review I can draw some conclusions to create a conceptual model that will help explain why governmental regulation is important. Firstly, it has been established that data can be viewed as valuable assets or commodities for businesses. Secondly, it has also been established that users are constantly leaving data traces whether they wish to do so or not. Finally, the literature describes how users do not necessarily act in a way that would suggest that they care about their privacy. Even in situations where privacy is identified as important to a particular individual, their online behavior does not necessarily reflect that. It seems like as long as users feel like they are receiving benefits that outweigh the disadvantages of giving up some of their privacy, they are willing to do so. The literature also suggests that there are complicated brain processes and biases that stand in the way of an individual making a privacy decision behaving in a way that matches their privacy intention or attitude. In very simple terms, data are valuable resources, users are data, and users are not able to protect their own privacy in a satisfactory manner. I would argue that this means some form of unbiased governmental regulation is necessary. Without it, companies could collect, analyze, use and sell user data without a negative consequence. Data from online users will be collected and used regardless of governmental regulation, but regulatory frameworks, such as GDPR, are there to safeguard and encourage businesses to do so in a way that protects and respects user privacy. Users’ online privacy behaviors have been shown to not accurately represent their level of privacy attitudes, which means they need something in place that can take better care of their privacy than they themselves are able or willing to. Furthermore, the research suggests that if companies are transparent with data processing and dissemination, they have a privacy policy and they are subject to governmental regulations like GDPR, customers are more likely to trust the companies. As such, governmental regulations seem to be important and beneficial, both for companies and for their users.

3 Methods

This chapter will identify what methodological approach was used, explain why it is the appropriate approach, and describe how it was used. This thesis will use a qualitative approach to methods. It will include two qualitative interviews with employees at DNB ASA and Telia. My thesis will also use document analysis to obtain more information on how companies collect and use user data. Telenor, DNB and Telia's privacy policies and parts of their annual reports were included in the document analysis.

3.1 Interviews

Conversations have been a method of obtaining systematic knowledge for a very long time (Brinkmann & Kvale, 2018, p. 27). The term interview denotes an interchange of views between people. Qualitative interviews have been recognized as a research method in their own right and are extensively employed as a research method in the social sciences. Interviews are a structured conversation in which the interviewer determines the structure of the conversation (Brinkmann & Kvale, 2018, p. 30). Thus, the interview transcends everyday conversation, it is a professional and systematic interaction that involves careful listening and questioning.

This thesis employs interviews as a research method because interviews allow for conversations with people who inhabit in-depth knowledge. Interviews as a qualitative research method is popular in the social sciences (Brinkmann & Kvale, 2009, p. 11). Qualitative interviews are interviews that are not devoted to quantify the results, but to gain knowledge and insight into a topic that is spoken in normal language (Brinkmann & Kvale, 2018, p. 36).

Interviewing participants with knowledge on the specific topic of this thesis will be vital in order to obtain the information that this study is interested in. Qualitative interviews are central in the social sciences, and some have argued it has become the most central resource through which society engages with topics that concern us (Brinkman, 2013). People talk to people to gain perspectives on how they feel, how they act and how they think; it is an arena in which people interchange views. The interviewees I will be speaking to will have information and perspectives that this thesis will find valuable. However, the objective of the interviews is not to gain entrance into my participants personal views or feelings, but to get unique information that they have through their employment.

3.1.1 Interview Selection

The participants in the interviews were chosen based on their employment and position within the companies this thesis is interested in. The interviewees both work with, and thus are likely to have knowledge on, customer data. As this thesis was interested in specific information that is not available to everyone, this was not a random selection of participants. I experienced varying difficulties with gaining access to employees at the companies who were willing to be interviewed. Establishing a date and time for the interview with Telenor proved to be difficult and it never happened, although their initial response was positive. DNB's response was positive, and I managed to set a date and time for an interview, even though this process took some time. Telia was the last company I contacted and the first I interviewed, so this process went very quickly. Essentially the three companies I contacted had three completely different approaches.

I contacted the participants by email. I initially contacted Telenor and DNB, and sent an email to a specific person in Telenor who was listed as a privacy officer. As DNB did not have a specific person listed as privacy officer I sent the email to an email address listed as one to use if you wanted to reach a privacy officer. The first email was sent on the 29th of October, 2020. None of the two companies replied to my first email, but I received positive replies after I sent them a follow-up email. From there I tried to establish a date and time for an interview. At first, I did not think it would become as hard as it proved to be due to positive responses from both companies. However, pretty quickly my contact at Telenor became very unavailable, and eventually completely ignored my attempts at setting up a time and date for an interview. Due to the lack of response from Telenor, I realized I would have to contact Telia and abandon Telenor. Thankfully, Telia were extraordinarily quick to reply and agree on a date and time for an interview and by far the easiest to gain access to. The interview with Hågen Ljøgodt from Telia was conducted on the 4th of February, 2021. DNB also agreed to an interview and the interview was conducted with Ine Oftedahl on the 10th of February, 2021.

I managed to secure two interviews, and while that may be a low number of interview participants, the interviews I conducted were highly informative. I specifically wanted to interview large Norwegian organizations who process a vast amount of customer data, and thus, there were a limited number of companies that were relevant to contact. Generalizability is not an objective in a case-study, but I hope my research can be built upon and researched further and that it offers a valid and qualitative contribution to the existing research. Crouch and McKenzie (2006) argues for the benefits of small sample sizes. They (2006, p. 495) contend that a small number of interview participants in a qualitative study allows the researcher to keep the total results from the interviews in their mind throughout the project. Furthermore, they argue that for depth to be achieved, the research has to be intensive and focused, rather than aiming at being extensive and convincing through a large sample size (Crouch & McKenzie, p. 494). Smaller sample sizes can more easily achieve depth and from an intense focus on a few interview participants the research is more conceptually persuasive, and a larger number of interview participants is not necessarily an effective way of increasing the quality of a research study.

3.1.2 Preparing for ‘elite-ish’ interviews

As my interviews are not, as Brinkman (2013) focuses on, conducted to gain knowledge on the interviewees’ personal perspectives or feelings towards my topic, but rather their knowledge and their company’s perspective, it is important to discuss the aspect of elite interviews. My interviewees do not necessarily fall into the category of elite interviews, but it is important to recognize that they do share similarities and characteristics of elite interviews. Harvey (2011) states that there is no specific definition of what constitutes an ‘elite’ within an interview setting (p. 432). For example, Zuckerman (1972, cited in Harvey, 2011, p. 432) proposed the term ultra-elite to describe interviewees who hold a significant amount of power. Harvey (2011, p.433) defines elites as people in senior management positions, or board level positions within organizations, however, his definition does not mention the scale of the organization. Both my interviewees are employed in largely powerful corporations, but are not board members or senior management. However, they are a big part of a new and innovative focus area of their respective companies. Ine Oftedahl from DNB ASA is the director for data transformation, and Hågen Ljøgodt from Telia Norge is both a data protection officer and a privacy lawyer.

Oftedahl describes her job to have changed from increasing DNB’s competence and expertise on data internally, to now being responsible for DNB’s analyses on how the pandemic has affected Norwegian households, society and businesses. Ljøgodt describes his job as mainly giving internal legal advice and informing on what is legal and not in the processing of personal data. None of them were interviewed for their personal views or feelings on this topic, but rather their professional opinion and knowledge. Mikecz (2012) describes that gaining access and trust to elite interviews is a time-consuming process, and it can prove difficult as elites can deny access to the information that is needed. Natow (2020) argues for the importance of triangulation when conducting elite interviews. Triangulation can mean relying on different research methodologies in addition to the interviews (Natow, 2020, p. 161). This is so the information provided in the interviews can be verified by other sources of information. Natow (2020, p. 169) found that the most common form of triangulation in combination with elite interviews is document analysis. This thesis will also include a document analysis.

Mikecz (2012, p. 485) also highlights the issue of getting the “real” story and not the “public relations” version of the story. Thomas (1993) also relays this as an issue describing that after finally gaining access, the researcher might not get the answers they are looking for, but a pre-determined narrative that suits the interviewee. When I decided to write my thesis on user data and how big companies collect and what they use it for, I knew it was possibly a “sensitive” subject matter. However, the companies are outwardly focused on transparency which is visible in their privacy policies and annual reports.

3.1.3 Interview guides

Oftentimes too much time is spent on interviewing, and too little spent on preparations (Brinkman, 2013). Brinkman (2013) states that necessary preparation is vital in order to gain relevant information about the topic in question. I spent considerable time developing my interview guides. This thesis was reported to Norsk Senter for Datainnsamling (NSD) and a draft of the interview guides had to be completed for the thesis to be properly evaluated by the NSD. As a result of this the interview guides were almost complete when the thesis was approved by the NSD. However, as the questions could be edited slightly, I kept improving them up until my meeting interviewees. At the time of receiving approval from NSD my main contenders for companies I wanted to interview were Telenor and DNB, so these are the interview guides I prepared. Telenor proved difficult to gain an interview with, and I eventually interviewed Telia. So, the interview guide for Telia had to be written at a quicker pace than the previous two. However, as I had already spent time writing and researching how to write a good interview guide, I did find that it was easier the third time around. Furthermore, the questions were mostly identical, except for the questions relating to the individual companies or their privacy policies. I wanted to keep them as similar as possible as I think that is the fairest way of gaining information.

My interview questions were formed from my research questions. Brinkman and Kvale (2009, p. 132) show how to generate good interview questions from your research questions. As I also wanted to conduct a document analysis, I had thoroughly read the companies' privacy policies and a few questions during the interview related back to the privacy policies. Had the interviews had completely different questions they would not be as comparable to each other. The questions asked during the interview were a mix of open and specific. Open-ended questions are helpful because I wanted a semi-something interview so that I could ask follow-up questions if the respondents said anything where I wanted to dig deeper to better gain an understanding or if they mentioned something relevant to my study. Harvey (2011, p. 435) points out that, especially when interviewing elites, they prefer open-ended questions because close-ended questions may feel restricting to them. The interview guides (see Appendix B and C) were separated into three sections so it would be easier for me to control the interview as well as making it easier when analyzing the information received later. The sections were based on my three research questions.

3.1.4 Conducting the interviews

Two interviews were conducted, one with Hågen Ljøgodt at Telia Norge and one with Ine Oftedahl from DNB ASA. The interview with Ljøgodt was on February 4th, 2021 and lasted for 45 minutes. Oftedahl's interview was conducted on the 10th of February and its duration was 31 minutes.

Due to the pandemic the interviews were conducted digitally through Zoom as home office was mandatory for everyone when possible. Holt (2010, in Harvey, 2011, p. 435) argues that phone interviews are not to be seen as the second-best option and are as good as an in-person interview. As the interviews were conducted through Zoom with video on, it is possible to argue that it can be considered a level up from traditional phone interviews. I also believe that as a result of working from home for close to a year at the time of the interviews my participants are used to meetings on Zoom. This, perhaps, allowed the digital method of interviewing to feel more comfortable and “normal” than prior to the pandemic. Nonetheless, the literature suggests that face-to-face interviews generally allow for better data (Harvey, 2011). But, as this was not possible due to the pandemic, a digital interview over Zoom was the best option. In my experience, the digital aspect of the interviews did not interfere negatively with the interview. As the topic of my interviews are not of a particularly sensitive or personal matter to my respondents, I do not think they would have found it any easier if the interview was conducted face-to-face.

3.1.4.1. Digital Interviews

Prior to conducting the interviews, I made sure to find a suitable place at home with good lighting so that was not a distracting factor, as well as to test my microphone and camera by conducting a test-interview. Through this test-interview I made sure everything technical was in working order so I could minimize the risks of technical issues during the interviews.

Had the interviews been conducted face-to-face it is likely that I had recorded the sound from the interviews to be able to transcribe the interviews, but I would not have recorded a video of the interviews. However, Zoom does not allow for exclusive sound recordings, which meant that in order to record the interview for transcriptions the interviews were recorded both with video and sound. My participants were informed and consented to the recording of the interviews.

3.1.5 Analysis of interviews

The researcher should have an idea about analysis even before conducting the interviews (Brinkmann & Kvale, 2018, p. 136). In the interview situation there are opportunities where the researcher can push the conversation in the direction of what will be useful and relevant when analyzing the interviews later. Brinkmann and Kvale (2018, p. 137) argue that it is favorable for a researcher to identify if the research is framed inductively, deductively, abductively or as a combination. I approached my thesis from an inductive perspective.

I transcribed the interviews straight after they were conducted. The transcriptions were written in Norwegian, as that is the language the interviews took place in. As I was writing the analysis, I included the quotes that I found were the most relevant and translated those quotes to English. I sorted the different quotes into thematic categories that were identified through my research questions. There does not exist a magic solution to find meaning in interviews and transcripts, that is the researcher's job (Brinkmann & Kvale, 2018, p. 139). However, Brinkmann and Kvale (2018) provide some useful tools.

As the primary focus of my interviews was to gain knowledge into how the organizations process user data and their view on privacy, I transcribed the interviews verbatim and my analysis was purely descriptive. I did not attempt to analyze the interviews looking for hidden agendas or hidden meanings in body or verbal language. I simply tried to communicate exactly what my interviewees had said and to the best of my ability make their arguments and accounts as correct as possible.

After I had completed my descriptive analysis of the interviews, I sent the interview chapter by mail to my respondents. This was so they had the opportunity to correct or adjust any misunderstandings and change any factual errors, and to give them the opportunity of withdrawing their consent. Only minor corrections were made by both respondents, which indicates that the interviewees were satisfied with how their meanings and statements were portrayed and that it was probably close to their experience of the interview.

3.2 Document analysis

Document analysis is often part of research, whether as a focal part of the research investigation or as an addition to the research (Karppinen & Moe, 2019). Compared to other research methods that might be costly or difficult to access, documents are often readily available and a stable form of research material. Bowen (2009, p. 27) defines document analysis as a "systematic procedure for reviewing or evaluating documents- both printed and electronic material". Karppinen and Moe (2012, p. 3) state that there are many definitions for a document within the social sciences. John Scott (1990) has a popular definition of a document as: "an artefact which has as its central feature an inscribed text" (John Scott, 1990, in Karppinen and Moe, p. 3). Syvertsen (1998, p. 5) whose research is more based in media studies, has a definition that explicitly includes both audio-visual and written texts. She (1998, p. 5) defines document analysis as a “systematic analysis on written or audio-visual stories not generated or produced by the researcher themself”. Bowen (2009, p. 29) argues that document analysis as a method is especially appropriate in qualitative case studies.

Karppinen and Moe (2012) discusses documents as texts or sources. Documents as sources are primarily used where the interest is to use them as ‘sources intended to document a process’ (Skogerbø 1996: 50; also Østbye et al. 2007: 47 in Karppinen & Moe, 2012, p. 9). Essentially, the documents are used as sources to uncover the facts behind the documents. The documents in this research can have a descriptive function, where the researcher is interested in finding the facts and provide an accurate description of the documents’ content. To illustrate, research where this is used can be, for example, systematic studies of recent media policy developments (Karppinen & Moe, 2012, p.10). Karppinen & Moe (2012, p.10) state that studies like these are useful for increasing the public knowledge of communication policy. Documents can also be analyzed exclusively as texts. In this way they are viewed as important and consequential in and of themselves, irrespective of the authors’ intentions (p. 11). Documents are analyzed by looking into metaphors and narratives that exist within the text. The focus shifts from describing the truth, to finding hidden assumptions behind policy-making. As all documents are influenced by the conditions of their production, it is important for the researcher to acknowledge this fact and place them in the proper context in an analysis (Karppinen & Moe, 2012, p. 15). In this thesis I will look at documents as sources, and conduct a more descriptive analysis where the focus is to describe the documents’ factual content, rather than the documents own consequential importance.

Syvertsen (1998, p. 16) warns that documents do not necessarily offer an objective and truthful account of how an organization operates, but rather, that they act as an opportunity for self-presentation for the company. While annual reports’ intended audience is usually the organizations’ stakeholders, different parts of the document may be intended for different audiences (Syvertsen, 1998, p. 17-18). In terms of my document analysis, I am primarily interested in the parts of the annual reports that are relevant to customer privacy, transparency and use of customer data, in general, the organizations privacy culture. I would argue that these specific parts pertaining to privacy are likely to be more relevant to the public and the organization’s customers, rather than their stakeholders.

The document analysis offers insights that the interviews might lack, and it is also a method of triangulation. Triangulation is the combination of two or more methodologies and is a way of corroboration and convergence (Bowen, 2009, p. 28). Natow (2020) looked at the benefits of triangulation in combination with elite interviews. Natow (2020, p. 161) argues that because elite interviews present a risk of being inaccurate, triangulation can be a way of obtaining a more accurate picture of the topic being investigated. The method that was most popularly used in combination with elite interviews is a document review (Natow, 2020, p. 169). Documents can offer background, context and supplementary data to a study (Bowen, 2009, p. 31).

This thesis conducted a document analysis on privacy policies and the parts of the annual reports that were relevant to this thesis. The privacy policies and annual reports belonged to Telenor, Telia and DNB. This thesis analyzed the most recent version of the documents that are available online as of May 2021.

Wolford (n.d) has created a template for privacy policies and what needs to be included so I used that source as a reference point when analyzing the privacy policies.

3.3 Research Ethics

Research ethics include a wide variety of norms and values that exist to ensure a moral and ethical approach in research projects (NESH, 2016). The National Committee for Research Ethics in the Social Sciences and the Humanities (NESH) provide advisory guidelines that promote responsible research. The guidelines are based on general ethics in science, which again are based on the morality in society (NESH, 2016). They do not act legislatively, but, rather, exist as a tool for researchers to use and refer back to as they describe important areas of relevance that researchers should keep in mind through the entirety of a research project.

Brinkman (2013) states that it is important to not think of ethics as a “check-list” approach that can be finished even before really starting a research project. Ethics in qualitative interviews is likely to be a constant conversation, and it is important to be open to these questions as my thesis progresses and recognize that ethical questions can arise suddenly.

Brinkmann and Kvale (2018, p. 47) state that moral issues concern both the means and the ends of an interview. The means refer to the interview situation and how this affects the interviewees. By the end, I would assume, Brinkmann and Kvale (2018, p.47) refer to the potential consequences that the interviewees might experience as a result of a published research study.

Brinkman (2013) recognizes the difficulty in obtaining informed consent. In a research project the focus might change, and if so, the researcher will have to ask their participant for renewed consent. Hopf (2004, in von Kardorff, Flick & Steinke, 2004) discusses the principle of damage avoidance, which states that the participants should not be at a disadvantage as a result of the research, and if the possibility that they might be damaged, in any way exceeding normal life, exist, they have to be well informed of that possibility.

My research project was reported to the Norwegian Centre for Research Data (NSD), where a description of my project, information on any interviews I wanted to conduct as well as a draft of the interview guides were included. In addition to this, NSD gathered information on where and for how long I would store the data that I obtained during my research project. Informed consent involves informing the informants about the research objective and the purpose of the study (Brinkmann & Kvale, 2018, p. 51). Furthermore, informed consent should make participants aware of any potential risks and benefits that may occur by participating. I obtained informed consent from participants prior to conducting the interviews (see Appendix A). NESH (2016) states that the researcher is obligated to inform the research participants and obtain their consent. The consent must be freely given, informed and in an explicit form. I obtained the informed consent by giving my participants an information letter depicting the intentions behind the project, reasons I desired their participation as well as their privacy rights. It also explicitly states their right to withdraw from the project at any time after giving their consent without any negative consequences. The information letter was based on a template provided by the NSD. The participants read through the document and sent an email back to me stating that they consent to participating. As my research happened during the Covid-19 pandemic their consent was obtained digitally, had the circumstances allowed for an interview face-to-face it likely would have been obtained through a signed physical document.

In Chapter B of NESH's (2016) guidelines it states that respect for individuals is an important part of conducting an ethically responsible research project. The researcher is responsible for protecting personal integrity, preserving individual freedom and self-determination, respecting privacy and family life, and safeguarding against harm and unreasonable strain. Acknowledging that publishing research can harm and threaten human dignity is an important part of conducting ethically responsible research. Therefore, it is vital that human dignity remains a focus for the researcher through the reporting and publishing of research results.

The participants involved in this thesis are not anonymized, and this was a conscious decision that was made. The participants in my project would probably be easily identifiable even if I had anonymized their names, furthermore, had I anonymized their role and companies my thesis would not have been as relevant as their employment in their respective companies are what my research is based on and is what gives the project substance. The participants were of course given the information that their identities would not be anonymized. The informed consent was given with the knowledge that their identities would be known.

NESH (2016) Chapter C Section 9 describes how researchers must respect the legitimate reasons companies have for not wanting their private interests to be published. Although Telenor did not get back to me and disclose those reasons, I respect their decision for not wishing to be a part of my research project. Companies are under no legal obligation to disclose their information with the public.

3.3.1 Reliability and Validity

Reliability relates to consistency and how reproducible the findings in the study are (Brinkmann & Kvale, 2018, p. 161). In interviews, this is related to whether the interview objects would have the same answers if asked the same questions at a later date and by other researchers. Furthermore, issues pertaining to reliability are also discussed in instances where different transcribers and analyzers might produce different sets of transcriptions and analyses. The transcriptions and analyses were conducted by me, so this is not a reliability issue relevant to this study. I would argue that my thesis is reliable, and that other researchers would get the same results and replies had they asked my interviewees the same questions. With regard to answering the same questions in the same way at other times, there are constant changes and new developments in the industries which might result in completely different answers had the same questions been asked two years from now. However, I would not identify that as an issue of reliability, more as a consequence of investigating a fast-paced industry in a continuous process of change.

Validity refers to whether a research project investigates what it means to investigate (Brinkmann & Kvale, 2018, p. 162). Is the method that was used be seen as sufficient and effective in answering the questions the study intended to answer? Validity is an important concept that the researcher should keep in mind throughout the entire research process, and it rests on the quality of the researcher. As I conducted interviews there will always be a consideration to take pertaining to objectivity because no human is completely objective. The informants were also selected due to their employment and spoke on behalf of their organizations so there is a possibility that it is in their interest to promote a certain message. However, this was not my experience during the interviews, and I, as a researcher, have been cautious and attentive not to let my subjective human nature influence my descriptive analyses of the interviews.

4 Analysis

In this chapter I will present my findings. As this thesis conducted two in-depth interviews with employees from DNB and Telia respectively, this is where most of the information was gathered. This thesis also includes a document analysis of privacy policies as well as relevant sections of the annual reports which offers further insights and acts as a method of triangulation. The privacy policies and annual reports that I investigated belong to Telenor, Telia and DNB.

4.1 Document analysis

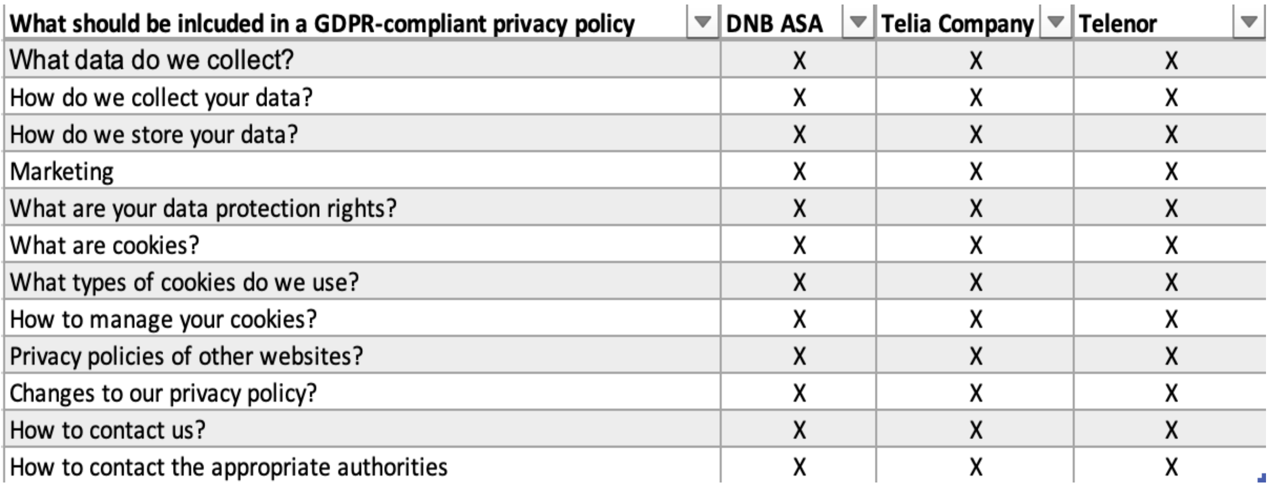
The document analysis that was conducted provides information about how and why the relevant companies gather and use customer data, the companies' stance on privacy and transparency, as well as how that is communicated to the readers.

4.1.1 Privacy policies

The terms privacy notice and privacy policy are interchangeable. The GDPR provides details of what should be included in a privacy notice in articles 12, 13 and 14 (Wolford, n.d). As Ljøgodt from Telia explained during his interview, this is to benefit the customer, but may also provide the customers with a less concise privacy policy as there are certain things that may be confusing that need to be included according to law. However, it is the companies' responsibility to explain and define anything that may be less clear to their customers and the privacy policies are updated quite regularly.

The three privacy notices are relatively similar, and this might be due to the legal requirements in what has to be included in a GDPR compliant privacy notice.

DNB's privacy policy is the longest of the three, with 11 pages, while Telenor's one is 8 pages, and Telia's is 6 pages long. Seen from a user perspective a shorter privacy policy might be seen as more approachable. However, as there are strict laws pertaining to what needs to be included in a GDPR compliant privacy notice, this can be a challenge to execute in an effective manner.



What should be inlcuded in a GDPR-compliant privacy policy	DNB ASA	Telia Company	Telenor
What data do we collect?	X	X	X
How do we collect your data?	X	X	X
How do we store your data?	X	X	X
Marketing	X	X	X
What are your data protection rights?	X	X	X
What are cookies?	X	X	X
What types of cookies do we use?	X	X	X
How to manage your cookies?	X	X	X
Privacy policies of other websites?	X	X	X
Changes to our privacy policy?	X	X	X
How to contact us?	X	X	X
How to contact the appropriate authorities	X	X	X

Figure 1. *What should be included in a GDPR compliant privacy notice.*

These are the topics that should be included in a GDPR compliant privacy notice. As shown in Figure 1, the three companies' privacy notices and its contents are all compliant with the GDPR guidelines. The X represents that the topic is included in the privacy policy.

4.1.1.1 Data collection

This part of the document analysis will look at the sections surrounding data collection in the privacy policies.

How the collection occurs is described quite vaguely across all the privacy policies. DNB ASA privacy policy states that they collect user data from third parties and through cookies. Further the privacy policy describes scenarios where and how this happens. For example, cookies are described as small text files of data that are stored locally on the user/visitor's technological devices and allows DNB to collect information on how their website is used. This information is then used to offer a secure and functional website, personalization, analytics, and to market their products and services. DNB ASA's privacy policy goes on to describe how a user can turn off certain aspects of the data collection through cookies, and the user can easily turn off or on features while reading the privacy policy. The features the user is allowed to turn off or on is tracking online behavior and statistical analysis. It is also stated that the user needs to repeat this process for all devices. Telenor and Telia's privacy policies do not offer their customers the opportunity of opting out directly within their privacy policies, but details how a customer who wishes to opt out of their statistical analyses can do so.

Some of the information in the privacy policies on how data is gathered is probably not surprising, for example the collection of customers name, email addresses, payment details, demographic data and so on. However, some of the other data that is collected may come as a bigger surprise to some. Other avenues the companies collect data from is through the information that is generated when they are using their services. For example, Telia's privacy policy details how they collect information on viewer history, technical devices, traffic data, internet connection, screen sizes, navigation and menu selections, location data. Telenor also mentions that they gather information on what website the user visits after visiting theirs (p. 3).

4.1.1.2 Data use

Telia Company's privacy policy states that the collection of data is primarily used to deliver services, improve services and user experience, profiling, targeted advertising, ensure information safety and prevent misuse of services or when there is a legitimate interest to do so (p. x). These are the same overarching uses that Telenor describes in their privacy notice (p. 4), and it is the same for DNB (p. x). In addition to this, DNB ASA also uses data for customer authentication.

DNB's privacy policy includes a subsection on 'legitimate interest'. In the subsection it states that "DNB can process personal information if necessary to safeguard a legitimate interest that carries more weight than the consideration for the individuals' privacy". Following this are examples of data processing related to a legitimate interest and one of the three examples is "customer analyses based on profiling for marketing purposes". Essentially, their privacy policy claims that 'profiling for marketing purposes' is more important than their customers' individual privacy, which is not necessarily true, but that is what it is reading as.

In Telia's privacy policy each section of the document starts with either how, what, when, who or where. That string of words would often include a 'why', and this is probably something Telia could include in their privacy policy that the readers would benefit from. The privacy notice includes what data Telia collects, additionally, it might be relevant for customers to know why these data are collected.

It is clear that data collection and use is an important part of many aspects of the organizations, such as delivering services, billing, security, customer identification and for legal reasons. However, there is also data use that is not necessary, but that happens for profiling, marketing, personalization, statistical and analytic purposes.

These uses can be seen as the companies' motivations for collecting user data.

4.1.1.3 Protecting customer privacy

All the three privacy policies include a short introductory written text where it is stated that customer privacy is something they as a company take very seriously, and that their customers should feel safe in knowing their personal data are being protected. The introductory text also states that the personal data is processed in accordance with applicable and current privacy laws.

The privacy policies describe how the data that is collected is kept secure. Telenor (p. 6), details how there are physical, technical and administrative measures in place to protect customer data. These include access cards, strict confidentiality measures for the employees, encryption, and regular privacy and risk analyses. Telia and DNB also describe that there are technical and organizational measures to protect customer privacy and that they are committed to the safeguarding of customer privacy.

4.1.2 Annual reports

The annual reports provide a more overarching and conceptualized view of the privacy discourses in the companies compared to the privacy policies.

4.1.2.1 Dataism

The increasing flow of data produces new ways of doing business. Van Dijck (2014, p. 201), describes dataism as a belief in big data as a way of quantifying human behavior and a belief in the potential of user data and its information. Essentially, dataism is a belief in data.

Dataism involves trust in companies from users who experience that a larger part of their life is being moved online (van Dick, 2014, p. 202). Through the annual reports it is clear that the companies look to customer data as a key factor for future success.

Telia (Telia Company, 2020, p. 15) writes how data enables new business models, such as use-based payments. Telia's annual report also describes how the demand for real-time data is increasing, and how that can help with smarter and more sustainable city planning and transportation. Digitalization also increases the need for developing smarter and more secure networks and solutions, as cyber-attacks and security threats have become a part of a digitized society (Telia Company, 2020, p. 15). Furthermore, data analytics have become a method of improving user experience and personalization through massive data sets. It attempts to improve user experience and create a smarter use of resources (Telia Company, 2020, p. 15). Telia's annual report states that Telia will accelerate their "data and analytics capabilities to enhance products, decisions, and customer interaction in real time" (Telia Company, 2020, p. 17).

DNB's annual report (DNB-konsernet, 2020, p. 41) touches on the value of user data, specifically transaction data, and details how that data in conjunction with customer data is an important part of how customers communicate with the bank. The analysis of the data allows for valuable insights into what the different customers might need, and the knowledge from the analyses is a way for DNB to continue to be a competitive and proactive banking offer for customers. Data analysis is identified as a critical area that DNB will continue to improve and develop their competence and expertise (DNB-konsernet, 2020, p. 45).

Telia Company's annual report describes how the company provided the European Commission with their Crowd Insight solution when met with a request to do so as a method of fighting the pandemic with the help of data (Telia Company, 2020, p.66). The report mentions certain risks (misuse or overuse of the data) of complying with the request, and how the request was examined in detail before it was approved.

Telenor's annual report (2020, p. 13) describes that to deliver personalized and engaging customer experiences they will continue to develop and utilize new opportunities within digitalization, data and analytics. Furthermore, Telenor's annual report (2020, p. 20) describes how their app, MyTelenor, is developed to increase customer interaction and consumption.

This is done so Telenor can offer increased personalization, which again will drive customer loyalty (Telenor Group, 2020, p. 20). Telenor's services have also proved useful to stop the spread of Covid-19 (Telenor Group, 2020, p.64). The company provided aggregated and anonymized data to the Norwegian Institute of Public Health, as well as provided mobility data to health authorities in Pakistan, Malaysia and Bangladesh.

The way data are discussed throughout the annual reports is an attest to how much value is put on customer data. For example, the way Telia's annual report describes how improving their data and analytics will enhance products, processes, decisions and customer interaction (Telia Company, 2020, p. 17). Additionally, Telia (2020, p. 31) writes that "to deliver customer value, we need to understand and be able to predict customer's expectations and requirements". This phrasing denotes that without predicting customers' expectation and requirements it would be impossible for Telia to deliver customer value. This customer insight is produced from customer data. These are examples of how highly data is valued and illustrates how dataism is present in the annual reports. There seems to be a general understanding in the annual reports, that to improve customer experience one has to know as much as possible about the customers. The information will improve the business' understanding by increasing their knowledge of their customers, and allow them to meet customers with personalized services, which in turn will increase customer satisfaction and loyalty.

4.1.2.2 Transparency

Increased transparency has been found to lower customer privacy concerns (Morey, Forbath and Schoop, 2015), as it reduces frustration from lack of knowledge.

Telia's annual report mentions the company's commitment to transparency. Furthermore, how Telia has published the information on what requests they have gotten and their response throughout the pandemic. The commitment to and promotion of transparency is reiterated throughout the report and is mentioned as a way of ensuring their customers freedom of expression and surveillance privacy (Telia Company, 2020, p. 65). Moreover, Telia Company are a member of the Global Network Initative (GNI) who work to support freedom of expression and privacy.

Similarly, to Telia, through their annual report DNB ASA demonstrates a goal to be transparent and trustworthy with their data use and collection (DNB-konsernet, 2020, p. 42). DNB’s annual report explicitly states that they need to be transparent about the process of using customer data (DNB-konsernet, 2020, p. 92). DNB’s report describes that, as a competitive organization, they are reliant on customer information in order to deliver the best products and services. However, access to that information is dependent on customers’ confidence and trust that their data will not be misused. Essentially, treating customer privacy with respect and transparency is vital for DNB when using customer data. Their customers’ lack of confidence in DNB’s ability to use and protect customer information and privacy can impact negatively on DNB’s reputation and business opportunities. Transparency is a way of keeping customers updated and informed, and will increase trust in the organization.

4.1.2.3 Customer privacy considerations

As all three companies process a large amount of personal customer data it is important that they protect customers’ data and privacy.

In their annual report Telia Company identifies customer privacy as a risk and outlines the potential impact of the risk, as well as describes mitigating factors (Telia Company, 2020, p. 84). In the description of customer privacy as a risk, it is stated that massive amounts of data are generated in and through the services they provide and their networks, and that the responsibility to protect the data from harm and misuse lies with the company. Further they write that “new ways of connecting as well as data driven business models increase the complexity of understanding and retaining control over how data is collected and used”. An example of the mitigating factors described are continuously reviewing GDPR compliance within the company. Examples of potential impacts of risks mentioned are financial penalties, loss of customer satisfaction, and thus, a loss of reputation that may become harmful to the business. Increased digitization and connectivity also increase demands for customer privacy and ethics management (Telia Company, 2020, p. 15). Maintaining and gaining customer trust is seen as important. Telia’s annual report also mentions customer privacy in their chapter on human rights (Telia Company, 2020, p. 54). Customer “privacy compliance when using customer data for advanced business insights” was identified as the most salient issue in terms of customer privacy.

Telenor’s annual report also identifies privacy as a risk (Telenor Group, 2020, p. 23), similarly to Telia’s annual report. However, the risk is linked to the possible financial penalties should Telenor not keep on top of the laws and regulations, not necessarily the potential harm the customers might experience. Telenor Group’s annual report (p. 24) states that there is a continuous focus on ensuring the human right to privacy and freedom of speech. Furthermore, that there is a focus on ensuring their customers’ privacy, because if customers experience a lack of privacy protection, they might not share their data with Telenor (Telenor Group, 2020, p. 71). The consequence of customers not feeling safe in trusting that Telenor can protect their data, would limit the opportunities for Telenor to deliver data-driven services (Telenor Group, 2020, p. 71).

DNB also describes how the fast-paced digital development increases the need for advanced handling of data and that customer privacy is an area which will continue to be a focus for DNB ASA moving forward (DNB-konsernet, 2020, p. 93). DNB’s annual report refers to the results of the Norwegian Data Protection Authority Report that showed that a majority of people have refrained from using a service based on privacy concerns (DNB-konsernet, 2020, p. 92). DNB’s report states that this shows how businesses run the risk of losing customers if customers lack the necessary trust in how DNB processes their personal data. It further describes the importance of safeguarding customer privacy to build and maintain trust. The annual report identifies customer trust as an obvious prerequisite if DNB is to reach its financial goals and create the best customer experiences (DNB-konsernet, 2020, p. 93). Thus, customer privacy will continue to be an area of focus for DNB moving forward.

4.1.3 Conceptualized summary of the document analysis

By looking at both privacy notices and annual reports the companies all seem to be focusing on improving customer privacy and transparency, as well as reducing the risk associated with customer privacy. However, it is necessary to keep in mind that some of these documents may be intended as a method of promoting the companies to customers and stakeholders. This does not mean there are falsehoods or misrepresentations in the documents. I do not think organizations like Telenor, DNB or Telia should be afraid to discuss their commercial interests in data more transparently. The documents read as an explanation for how, what and when the companies process personal data, but there is not one sentence that explicitly states that they also collect and use this information because they have commercial interests in doing so. Big organizations like Telia, Telenor and DNB depend on revenue and the use of customer data allows for another avenue of income generation as well as increases their customer insight. However, the importance of safeguarding customer privacy while using their data to improve their business has to be made explicitly clear. In general, the documents suggest that customer data and customer privacy are two areas that are viewed as significant for the organizations. There is also a sense that this will continue to be important in the future. Furthermore, the annual reports promote the importance of customer data, the insight it offers and illustrate how dataism is present within the companies.

4.2 Interviews

The interview chapter is categorized into subchapters based on my research questions, as well as conceptualizations and themes that were discovered through the analysis of the interviews.

4.2.1 Why do companies gather user data?

Ljøgodt stated that the main motivation for collecting user data is to deliver the services they offer. To illustrate, without data collection Telia would not have enough information to set up the call, nor to bill their customers for that call. So, some form of data processing is necessary for the delivery of services and products:

> The main motivation is that we collect user data to deliver the services. When our customers call each other, we need to set up that call, purely from a technical standpoint, and we also have to save information about the call taking place so we can bill for it. So, to deliver the service we have to process personal data.

Ljøgodt goes on to say that they also have data that is used for marketing purposes, product development, statistical and analytical purposes. But he adds how “that is kind of something we do as a consequence or result of having this information”. Data generated by the use of Telia’s services, traffic data, are exclusively used to deliver the service and for billing purposes. Whereas for marketing purposes only basic personal data is utilized.

Oftedahl makes an important distinction between data collection and data utilization. Data collection has been happening for a long time, but to actually use it and analyze it instead of just storing it in a vault is the more recent development. Large amounts of the data collection is necessary due to legal requirements. Oftedahl spoke on DNB's motivation as a way of wanting to meet customers personally in a less personal digital world. As DNB becomes increasingly digitized and the number of physical offices decreases, DNB has to maintain contact with their customers through other avenues. The data generated by customers is a way to listen to their customers in a digitized world. Oftedahl describes how their customers are speaking to them every time they use their cards or visit their website. Through the analyses DNB is listening and creating the best possible offer for their customers by adapting products and services and communicating more efficiently to meet specific customer needs. Oftedahl, DNB:

> And this is just going to be more prevalent in the future. It's also a process of maturation, the customer must understand that we have a lot of data, we use a lot of data, but we do it so we can give them the best possible banking offer.

Oftedahl also describes that the customers need to come to terms with the fact that their data are being used and collected, but also understand that the motivation behind that is so that DNB can offer them the best possible service. Oftedahl says that, other than the data that they are required to collect, the main use of customer data is to make data driven business decisions, and to personalize and improve services for their customers.

> Other than the data we need to collect due to legal reasons, we collect data, 1. to make business decisions, and 2. to personalize and optimize products, services and communication with our customers. That is overall, in my head, the main reason.

Ljøgodt explains that the information Telia has pertaining to their customers' invoice can be used to recommend services or subscriptions plans that might be a better fit for that particular customer. A customer might be paying for more data than they use, or a customer is paying for less data than they use and are therefore having to buy extra data packages on a regular basis. Information retrieved from a customer's invoice is used by Telia to ensure that they are offering the best possible plan for that specific customer.

> If we see that a customer uses much more data than what is included in the subscription and constantly has to buy data packages and, thus, comes out worse financially then we

> can recommend a subscription that matches the customer's use better. This also applies to broadband and in the television area, we can give recommendations for new series that match the TV habits of the customer. It will also benefit the customer that we can use information on how our services are used to make our services better. Whether it's purely technical, where should we set up a new base station to make our network better, or to make them more in line with what customers expect about modern services.

Furthermore, what benefits the customer will eventually benefit the company, and so the interests of the customer and the company usually overlap. In the example of a customer paying too much for what they are using, they might shop around for better subscriptions that are a better match to their needs. This would mean that Telia lost a customer to a competitor. While the customer’s and company’s interests usually coincide, there are some cases where customer data is used mostly for Telia’s benefit. For example, in cases where the information is used to compare Telia to their competitors.

> It’s a bit coincidental because if the customer has a subscription that does not meet the customer's needs, he or she will quickly be able to look around for competitors because the customer experiences that it is too expensive. So usually, we have overlapping interests. At the moment we’re, for example, using information for marketing and it’s not a given that the customer has any interest in receiving e-mails from us with advertising, but it may be of interest. Therefore, the customer has the opportunity to say no to it. But we also use customer data for statistical purposes, analysis. We also use it to ensure the security of our network, we use certain sets of information. Then we probably also use information perhaps to compare ourselves to competitors, it’s probably typically only in our interest not in the customer's interest. But a lot of what we do, I really think, Telia and the customer have overlapping interests.

In their privacy policy, Telia Company writes that their users will receive a more relevant user experience if their advertisements are targeted at their specific needs and based on their personal information. However, the report from The Norwegian Data Protection Authority showed that 3 out of 4 view the use of targeted advertising negatively. Ljøgodt was asked if he had any thoughts on this specific matter. Ljøgodt explains that Telia, like most others, advertises online. He also says he believes that a personalized experience when visiting the Telia website, receiving ads that are relevant to that specific customer would be beneficial to them. To illustrate, a young adult private customer who is receiving advertisements for services that Telia offer their business customers would probably feel more interested if the advertisements were of services that are relevant to them. Advertisements targeted at business customers will probably not be experienced as relevant to private customers. He also describes a different effect of targeted advertising where a person doing research on the best Telia mobile subscription plan is likely to receive Telia advertisements for weeks after as a consequence of their search history. He acknowledges that the experience might be annoying, but that is probably the reality of advertising today. Furthermore, for a visitor to Telia.no it should be relatively easy to change their cookie settings so the Telia advertisements will not follow them around. Ljøgodt argues that opting out of cookie collection should have become easier than it currently is, and that many websites are probably not in compliance with GDPR guidelines. After GDPR was implemented, websites have to inform visitors that they are collecting cookies, and the visitor can then click accept, deny or make changes to the cookie settings. On Telia.no the user has to give consent to cookies used for marketing purposes, and the default is setting is no. However, some websites do not let their visitors change the cookie settings.

> It should also be easier for consumers to change settings now, when you visit a webpage, you should be able to change the cookie settings. I don’t think the way this has been solved and regulated has been particularly good, because you just get bored and most of us just want to get rid of them [pop-ups] and press ok on everything

4.2.2 How do companies gather the data?

Both Ljøgodt and Oftedahl had quite superficial knowledge on how the data is collected, however, as the technical aspect of collecting the data is not the primary focus of this thesis, their knowledge and the added information from the document analysis will provide enough insight into the process for this thesis.

Ljøgodt gives an example, if a customer is paying for access to watch Premier League on demand, they could technically be able to fulfill the necessary billing without registering what games you are watching or what episode you are up to on a certain show. However, they register that information so that the next time you want to keep watching an episode, you can easily tell what episode is up next, and when a customer has finished watching a show Telia can offer a similar show to the one they were watching based on the customers' viewing history. Essentially, the user experience would decrease if companies only collected the bare minimum. Almost all streaming services know where you were when you left off and will offer customers other shows they might like. If people are used to having that level of user experience, it might be annoying to suddenly not have that function anymore. Telia's main sources of collecting user data is through their customers' use of the services they provide, market research and cookies.

> [user experience] is one reason, it should be easy for the customer to quit a movie and resume from where she left it. But then we also look at, maybe how popular this movie is and then promote maybe similar movies and so on. So, it is through the use of our services that is our main source [of data collection]. And we also use market research where we measure the effect of our ads, and then we have cookies. Those are the main ways I can think of.

Oftedahl did not have in-depth knowledge on how exactly data is collected, but describes it as a multifaceted process similar to what Ljøgodt portrayed. The different platforms, website surfaces and apps all are ways DNB is gathering customer data. There are many technical surfaces and also every time customers draw their card, or use it to pay for something online. Effectively, the process of data collection is based on the customers' use and engagement with their services and products.

> It's very different, and I [Oftedahl] know the most about the method we use, so we have data warehouses where everything is stored, across platforms, so if we're talking about card data that is where we get it from. But we also have a lot of new platforms, we have a platform called Celebrus, that is only related to clickstream data, all the different websites and surfaces, our mobile bank and apps where data is collected from. And then others that are more relevant for the online bank and so on, so yes, quite a few technical surfaces that I sadly do not have enough knowledge on other than superficially.

I asked Ljøgodt if he could elaborate further on what happens to the data after it has been collected, and if it is being sold, how it is anonymized. Telia sells a small part of the data they collect, a product called Crowd Insight. Crowd Insight provides information on how many people are in a certain area and how they move in that area, and this is the only data Telia sells. The regulations are very strict about what you can call anonymized data. If information is classified as anonymous it should be completely impossible for both the company and anyone else to figure out or guess the identity of the data. Ljøgodt said that with the appropriate data skills that is something that is relatively easy to do, so before data can be referred to as anonymous it goes through a comprehensive process.

> So, to be able to call data anonymous, there is a thorough process, I'll be a little reticent, I was not involved in that work, but I'm very sure that it's fully anonymous, the data we refer to as anonymous. Excluding that [Crowd Insight] we sell little to others, but as I mentioned, we advertise online and have so-called third-party cookies on our website, which are based on active consent from the user. And so an exchange of information happens that is not anonymous, like if you've been on Telia.no and agreed to the third party cookies you might receive an ad for Telia the next time you go online… Other than that we are careful with third parties, that is, we are sometimes required to share information with the police, but that is completely different.

I asked Ljøgodt to explain what happens after the data from the third-party cookies are shared or sold and if they retain any control over it after this exchange. He explains that Telia relies on the advertisers' privacy policies and that they do not retain control, but that there is a thorough examination before they enter into a cooperation with other companies. As they are dependent on the trust of their customers, they do not give just anyone access. The only information any advertisers would have is if someone accessed Telia.no, no other information or information that could be perceived as sensitive is shared.

> So, what we [Telia] have of a more sensitive character, you could obviously tell a lot about a person from who they communicate with and where they are at all times. We also have content data, but this is information we wouldn't dare to use, or share with advertisers. So, the online marketing, it can be annoying to receive Telia ads for three weeks after choosing your phone subscription, but after all it's not scarier than that. And if we are the source, it is based on consent.

Telia's privacy policy states that they take special precautions to ensure subcontractors act in accordance with Telia's privacy policy, I asked Ljøgodt to explain what those special precautions are. He explains that there is a due diligence process where they ask the suppliers to ensure that they have procedures in place that protects personal information and that they meet the legal requirements. He further describes how they also make sure that the suppliers again do not use subcontractors where they run the risk of misusing the personal data. A data processing contract is signed where the subcontractors agree to meet Telia's requirements. The contract states that should they breach the agreement Telia can hold them accountable for the breach. GDPR has made the location of where the information is being treated highly relevant, and Telia prefers data to be processed within Europe where GDPR applies. So, while there is a part of the process that is based on trust, there is extensive vetting of the companies involved when data is shared with third parties and measures in place to ensure that trust is not broken.

Oftedahl explains that for DNB, the processes of aggregation, anonymization, pseudonymization and storing are different depending on what the purpose of the data is. There are different rules and guidelines depending on if it is being used for statistical purposes or advertisement. Relatedly for Telia, in terms of anonymization of user data, Ljøgodt explains that firstly it is aggregated so the data is never in a smaller group than ten people. In some cases, that can be too small of a group and then it is aggregated to a larger group. And then the cord that determines it is personal information is cut. For example, an IP-address that identifies who accessed a website is combined with a random series of digits and then the IP-address is fully removed from the digits so essentially what is left is a random series of digits that is not connected to an individual and the information is anonymous. Ljøgodt explains that at times there are attempts to anonymize data that he then has to tell the organization that it is not actually anonymized. For example, perhaps name and date of birth has been removed, but the customer identification number remains. A customer identification number can easily be connected with a name, so this is not considered anonymous information. In these situations, there are processes in place to ensure that this information is assessed before it is publicized, and the issue is solved internally before it is released or further developed.

4.2.3 What privacy concerns and company ethics are discussed?

Both of my interviewees had similar lines that would not be crossed when discussing personal information that they would never use the data of. Both banks and telecom companies have a very large set of sensitive data, as banks know exactly what and where you spend your money, granted when paying with your card, which, the pandemic has made using cash even less popular. Telecom companies know who you call and where you are, and sometimes those calls can reveal sensitive information that customers might not be comfortable with being used and shared. In general, anything that might be viewed as sensitive data for customers is off limits as it is not beneficial to customers.

An example of sensitive data that they both mentioned would be ethically wrong to use was any type of data related to personal health. Ljøgodt identified traffic data; who is in contact with whom, and location data; where individuals are located, as data that he would have ethical issues to use and sell to third parties. This is because customers are in contact with health specialists and abortion clinics, and it would be wrong for Telia to take that information and analyze why they were at this location and why they went to this location next. That is something that would be highly unethical for Telia to sell to advertisers. Customers also make calls that reveal sensitive information about the individual. For example, helplines can reveal something about an individuals' health status. Calls can also reveal infidelity, and clients who are in contact with their lawyers, or journalists who are in contact with their sources. There are a lot of examples and scenarios where both location data and traffic data can reveal highly personal and sensitive information about customers.

> Traffic data, that is, who is in contact with whom, location, I [Ljøgodt] think, I'd have major ethical issues to sell that. Because people visit health specialists and abortion clinics, and we are not going to analyze who that is and why she was there and went there after.. selling that information to advertisers would be highly unethical, I think. And as for who we speak to [on the phone], I mean it can present innocently enough, but we are in contact with helplines, and there might be health issues and infidelity and yes, there is a lot of information that can be uncovered with these data, clients who are in contact with their lawyers and journalists who are in contact with their sources.

Telia is responsible for ensuring the protection of their customers sensitive and personal data. Access into this data is only given to emergency services and police, and even then, there are procedures in place to safeguard that the access is necessary. In an instance where there is a legitimate emergency the emergency services will be given the necessary information, but this information will not be shared with anyone else.

> So, we [Telia] have to protect that information. Obviously. Only the police and emergency services can get that information. The police during an investigation, although we have procedures in place, we can't give them anything. And the emergency services, if there is a real emergency they will of course gain access to the whereabouts of a person, but nobody else will have that access.

> Our [DNB] internal guidelines are stricter than laws and regulations, so that means we stay away from industries that may be experienced as sensitive by customers, anything health related. There are enough customers so we could potentially deliver those data, but it would not benefit our customers and it would most likely be perceived negatively by the public.

The interviewees recognize that the professional reputation of the organization would be at risk if they were to use data that can be considered to be sensitive to the customers, and furthermore, that the customers would most likely not benefit from this particular data being used in any way.

DNB is part of a project with Stanford University that investigates ethical and responsible use of user data. Oftedahl states that there are many international organizations who are much larger than they are who are also a part of the Stanford University project, like Visa, Mastercard and Deutsche Bank who have come further in the process. Oftedahl explains that DNB is going to be the frontrunner of this development in Norway. It is clear that they wish to be perceived by customers as treating this seriously, but also that they really want to do this "the right way" and in no way do they want to step over their customers boundaries. There are many ethical and privacy related concerns to keep in mind when dealing with customer data. Oftedahl explains some of the thought processes behind being ethically responsible when asked if they consider the ethical implications.

> Yes, we are part of a project with Stanford University, that is about ethical and responsible use of data, kind of one step above GDPR, I mean yes it's technically legal, but should we? Is it right? Will it add value to our customers? Will our customers think

> it’s the right use of their data? And it’s also the considerations we take, we are not going to publicly discuss “vinmonopolet” or if people went to the doctor, or go deep, even if GDPR legally allows it, going so deep that people can think oh but I’m in that data set and feel bad about it.. There’s a fine line between being perceived as relevant and personal, and being perceived as creeps. So, there is a limit to how personal we should be.

Here, Oftedahl poses the same questions as The Norwegian Data Protection Authority director Bjørn Erik Thon did in 2018.

Ljøgodt explains that the more data is normalized and used the more important it will become for them to be transparent with customers and that they have a responsibility to ensure that their customers understand why they are getting recommended this movie, or why they got an advertisement for a different subscription plan in their email. Ljøgodt says their customers probably expect that making changes to their personal privacy settings should be relatively easy.

> This is something we must be completely open about and we must also be able to offer the customer the opportunity to say yes or no. So, a part of the customer's expectation is probably to be able to easily do these settings. To understand why they get these recommendations for example, so I also think that customers are becoming more and more concerned about their own privacy so then our job is to be clear on what we do and why we do it, and give the customer easy choices. To not have such long terms of use with lots of pages, like a 10 pages long privacy policy that the customer never understands and does not bother to read, but make it simple and easy to understand and user-friendly.

Oftedahl does not necessarily think their average customer is aware of how to opt out of statistical analyses based on customer data. She guesses that those who have made the decision to opt out and refrain from being a part of those analyses have a clear intention and know they do not want to participate and have found the option of opting out through looking for it. She thinks that if asked about their knowledge about their choice of opting out of statistical analyses, their average customer would shrug and say they never thought about it. So, she says it is easy for those who actively go looking for it and want to find it, but not in a way where most customers are aware of this decision. However, in 2019 updated information and opt out possibility was sent to all customers in the Internet bank. She further says that she does not see any immediate problems with the lack of awareness from their average customers, as long as customers have an easy way to find both more information and the opt out possibility if interested.

> I think how my team work with it [customer data] today you have to be very interested in not participating in any kind of statistics for it to make any sense, as you are anonymous and we are at such an aggregated level it will not really.. it has no implication for you.

GDPR is not necessarily more restrictive than its predecessor, in fact, Ljøgodt explains that it has opened up a few doors and allows for creativity and interpretation. He points out that the temptation of using information is bigger due to developing better tools. However, same as with DNB that does not mean that Telia engages with everything that is allowed, but that they hold the company to standards that exceed those of GDPR. Ljøgodt was asked whether GDPR has changed the way user data is processed and describes how GDPR has put user data on the agenda and that they are more aware of it than they were previously. Furthermore, GDPR has led to an increase in work processes before any type of product release to ensure that the requirements of GDPR is met and that there is no risk of being fined or breaking any rules.

> Firstly, user data is higher up on the agenda and we are more aware of it. We have also introduced multiple work processes that we have to go through before anything can be released so we can ensure that the requirements of GDPR are met, that the solution is safe enough so we don’t end up breaking the law which would be very expensive. So we are probably more restrictive now, and also after GDPR the temptation to use the information is maybe, because of the competitive situation and better tools and one can use the information more creatively now, but it is also increasingly important to do things correctly and in line with the law because the consequences breaking it has become tougher.

Ljøgodt was asked to explain how Telia works to ensure that the data they collect does not exceed more than they need for that purpose and how they avoid collecting unnecessary data. Telia conducts what is referred to as the GDPR as a data protection assessment, which they are legally required to do any time the company processes information that can be perceived to have a high privacy risk.

> We carry out what the GDPR calls a data protection impact assessment, the law says that you have do this every time you start doing something that has a high privacy risk. We always carry it out, but in cases where there is a very low risk we conduct a sort of light version of that process. But you have to ask yourself the questions; what is the purpose, do we have a valid legal basis, for example consent, legal authority, necessary to fulfill the contract, and is it limited to what we strictly need, how long can we sit on them, do we have a deletion routine etc.? So, we ask ourselves the questions throughout the process that must be carried out in connection with all development and releases. So, it is quite time consuming, and it is also quite costly because there are quite a few who have to be involved, and it delays us and so on, so this is a direct consequence of the GDPR. Many of these principles applied before, but I do not think, one probably did not have routines to follow up that those questions were asked then.

Ljøgodt says his experience is that customers are more aware of their privacy rights than they were before GDPR was implemented. There are more customers who utilize their right of access and request a copy of their personal information than there were before GDPR, even though this was always something customers had the opportunity and right to do.

4.2.4 The future of data use

The interviewees both theorized that data will become even more important in the future and that its role would expand. I asked both respondents about their theories on data in the future, and what the possibilities of data are. Oftedahl is convinced the use of data will become increasingly prevalent. She highlights that the increased use of data will benefit the customers.

Analyzing data in a productive way can contribute to being ahead in a competitive market. Ljøgodt describes customer insight as knowing exactly what customers are using their services and products for, as well as understanding what customers need and might be missing. Being able to properly analyze those data will be a crucial factor for companies that want to stay relevant and competitive in the future. The market and industry they are in is tough and competitive, and there are big actors who Telia will not be able to compete with unless they utilize the information productively. Comprehending and continuously being aware of the most effective way of employing this data so that it will benefit both the organization and the customer simultaneously will have a big impact on their future relevance. However, this development will not happen at the expense of customers' privacy or trust.

> And we [Telia] are also in a tough market, there are other big actors who we're competing with so we're completely dependent on being able to utilize the information we have so we can have the upper hand in the competition. And that's where my position comes in, because we rely on our customers trust and we don't want to misuse the information, and we also have strict legal requirements which we of course need to follow.

Oftedahl says that DNB has to be at the front of the trail, and because DNB is a large bank that can be challenging. Anything that can be streamlined will help DNB be quicker on their feet. Customer insight is creating a better customer experience for customers who might not be able to say exactly what they are missing, that is where utilizing that data will be able to point to what customers want, even before they are aware of it themselves. These are big analyses where DNB is not looking at a single customer, they are automatic analyses where everything will be aggregated and anonymized and the results will reflect a larger part of their customers' needs.

> Streamlining, catching what the customer actually needs, preferably before they can think of it themselves. There is a difference in what we [DNB] can see with all that data versus what the customer would come and tell us in a bank office. Oftentimes if the customer doesn't know what's best for them, or what they need or don't need, that's probably where the biggest opportunities are for us, better customer experience.

Ljøgodt exemplifies what a possible next step in this data driven direction might look like for Telia. They are looking into solutions that require customers to give consent to process their information before companies are legally allowed to use it for marketing purposes. At the time, using a customers' location data for marketing is off limits, but should the customer give consent for this information to be processed, marketers could use that information to target ads based on the location of an individual:

> So that's why we're looking into solutions where we get customers' consent to process information that the law does not allow without a consent. For example, we can't follow a customer's location and use it for marketing, I don't think we've considered exactly this scenario either, but if a customer wanted to then they could accept that location data was used so marketers could target ads based on your location. But that would require consent [from the customer].

While it is nothing new that customers are increasing their online presence, it is clear to Oftedahl that DNB customers really are online centered now. The changed customer behavior will ultimately change the bank and how it operates on an everyday basis. Oftedahl also states that as the customers are changing behaviorally and moving online, DNB is becoming aware of different types of competitors than before. Although the novel competing banks are different banks to DNB, they can just as easily meet their customers' needs. She says it is a fast-developing industry and that in an environment where the distance to customers is already increasing, it means that it will be even more difficult to keep customers with DNB. Ultimately, Oftedahl predicts, being a bank will change.

In terms of customers, Oftedahl stated that there will be a developmental process where customers will need to get used to the idea of data collection and use. It is important for them to not rush the customers in this process, but rather, walk with them through it. This way allows DNB to find out what their customers feel is acceptable use of their data, and where to draw the line for what is not acceptable. Since the beginning of the pandemic DNB has publicized transactional data more than 250 times in the media. After every time there is a perception at DNB that their customers are calmer and understand more about the processes involved.

> I would say it's a process of maturation, for example, we've been in the media 250 times with transactional data, and the more times we are in the media people seem to calm down, so it's kind of like, we have to walk with the customer and agree where to draw the line.

The customers have to adjust to this new reality and learn more about how it is happening and what it is being used for. DNB wants to make that adjustment as comfortable as possible for its customers.

4.2.5 Data driven business

I asked the respondents about the business aspect of data, and how data is impacting on their business strategy. Oftedahl speaks to how DNB is working on becoming a data-driven bank where the important strategic business decisions are being made based on data.

> We have said many times we are going to be a data driven bank, and it might be a little hard to put a finger on exactly what that will mean. In my mind it means that the big important strategic decisions are going to be made based on data.

DNB is working towards becoming a data-driven bank, where business decisions are made based on trends they see in the data. She theorizes that this is likely to change the competitive market in banking. Whereas before, a manager would be hired and business decisions would be mostly made based on the manager's gut feeling and by estimating what the customers would want. Using data in this way allows for products to be released before it is perfect, as the data they will get from a new release will imply what changes are necessary and what the customers want to be improved. This will then be updated and the customers will have had an influence on the final product. Essentially, it is a feedback loop where DNB will push products out faster to fill a need they think customers have, and then use the feedback from that to further improve on their service and deliveries to their customers. Oftedahl refers to it as a "fail fast, fail harder" type of approach, and says it is likely that customers will see a faster development of everything. Ljøgodt has the same idea of the future of data and how it is impacting on their business strategy. Ljøgodt explains that having information on exactly how the products and services are being used by the customers is vital to develop their services in the direction that will benefit the customers. Data is important for product development as well as pricing and meeting each customer with the best offer for them, in a competitive market it is a necessity to keep customers from fleeing to competitors.

> We [Telia] have a department working on business development and analysis, I think it’s an area of focus for everyone in the industry. How to develop our services so they target the customer’s needs, and the actual use of our services, information about the actual use of our services is extremely valuable so we can develop our services in the right direction.

They both mention the incentive of wanting to be ahead, wanting to better understand and see their customer’s needs, almost before they even realize they are missing it. Oftedahl also points to the impact data has on their business strategy and how many of the business decisions that previously were made on a “hunch” are now being made from solid evidence they find in their data analyses.

When I asked Ljøgodt what the discussions surrounding privacy and anonymization include, Ljøgodt says the discussions arise from a business perspective where there is an opportunity for more money to be made. The discussion within the company then turns to whether or not this is within the privacy regulations, as well as whether the customers would feel comfortable or react negatively. The task is to weigh those two considerations up against each other. Ljøgodt describes the GDPR as “quite detailed” but a little ambiguous and that there are many decisions that have to be made. Parts of the GDPR are open to interpretation, he says, because it states that processing personal data is legal as long as there is a legitimate interest to do so that does not negate the person’s privacy. So, there is a constant need to weigh the legitimate interests up against the customers’ privacy to find out what will benefit the customers and the company.

In regard to doing business with third parties, there is an extensive due diligence vetting process of the companies they are in business with, but at the end of the day they are at the mercy of those companies and rely on them to treat the data with the same care that they would. If the other companies do not follow the same careful and safe process that Telia would, Telia can penalize them later by having added a fitting punishment into their contracts.

Ultimately, both companies want to make as much money as they can without compromising the privacy of, and relationship with their customers, as well as their reputation in the public. Both Oftedahl and Ljøgodt propose the only way to do that is to always put the customers’ needs first. Oftedahl states that DNB ASA’s new focus is data ethics, and tells me that after landing in GDPR, what is ok what is not, they are now approaching it from a perspective of ok, even though this is legal, should we be doing it? Where does DNB as a company want to draw a line. That is what they are trying to find out through their new data ethics focus.

> We have a separate division that only works with data ethics. So, it’s kind of the new area of focus. We are in control over laws and regulations and everything we have to do, and now we can start looking at what we shouldn’t be doing even if it’s legal.

Oftedahl speaks of how DNB has a whole division that is exclusively working with data ethics. She says that now that they have gotten used to the new framework and are aware of what is legal and have the necessary procedures in place, they can start thinking about what might be legal, but unnecessary. Where does the line go where something is legal, but it could still harm their customers or be regarded as insensitive. That is what DNB is focusing on, finding where that line needs to be drawn. And that is something DNB hopes to do together with their customers. As Telia provides services to business customers like the Norwegian Armed Forces, the Norwegian Police Service, and the Norwegian Parliament so it would not look good if they were to breach any GDPR requirements. They do not take many risks so anything that could be perceived as a breach of trust, insensitive or illegal is not something they would go through with.

5 Discussion

Through this thesis I investigated three specific research questions; What are the motivational factors behind collecting user data? How does data collection happen? What are the privacy concerns that are discussed within the companies?

In the discussion chapter I will discuss the findings from the document analysis and the interviews in light of relevant theory and my research questions.

5.1 Motivation

The motivation behind collecting customer data is varied. Firstly, there is data collection that needs to happen on legal grounds, as well as data collection that is necessary in order for the services and products to function and for the companies to bill the customer correctly. Furthermore, a motivation behind collecting customer data is optimization of services and products and, in general, being able to be the top choice for customers in their respective industries. From my interviewees, there seems to be a general understanding that collecting and utilizing customer data efficiently is important in order to be successful in the competitive industries.

McAfee, Brynjolfsson, Davenport, Patil and Barton’s (2012) idea that data-driven companies make decisions based on evidence found in the data is exactly what Oftedahl described in her interview. Oftedahl spoke on how DNB ASA will become even more data-driven in the future, and is looking to increase the role of user data and that it plays a big role in decision-making on future plans for the company. Oftedahl and Ljøgodt touched on how data have a huge impact in their business strategy discussions. Decisions that before were being made by a CEO who had gotten the job due to their business instinct is now superfluous, as the data can tell what the customers are missing or needing, and instinct does not need to play a major role in business decisions anymore. Ljøgodt also touched on how he thinks data will play an even bigger role in the future, and that aggregated user data represent an excellent tool to improve services and customer satisfaction. Following McAfee, Brynjolfsson, Davenport, Patil and Barton’s (2012) conclusion it seems inevitable that data will continue to be an important part of improving business.

Oftedahl further mentions how data is viewed as a communication method with customers, and this was also present in the annual report of DNB (p. 41). Data are perceived as a way of listening to what customers want and need, and so, DNB and Telia are able to use the data to see what the customers are lacking. Customer insight is mentioned both by my interviewees as well as in the annual reports of Telia and DNB. The data can provide valuable insights in terms of product development, but also societal developments that extend beyond their customers. In terms of societal developments Ljøgodt mentions Telia's Crowd Insights, which for example, allows city planners to gain insight into how people use the city by monitoring movements. The data make for valuable insight as knowing how a city is being used can aid in the optimization of city planning, public transport, shopping and more.

Morey, Forbath and Schoop (2015) stated that many companies collect user data where there is no urgent use for it, and their reasoning being that it may be valuable someday. Further, that companies usually ask for forgiveness rather than permission. Due to the GDPR the companies this thesis investigated are not legally allowed to collect data that is viewed as unnecessary and that they do not have use for. By collecting unnecessary data, the companies run the risk of being fined. Regarding the contention of Morey, Forbath and Schoop (2015) that companies will usually ask for forgiveness rather than permission, this thesis' findings suggests that this strategy is not optimal, nor is it GDPR compliant, and companies would rather ask permission than forgiveness as the opposite could harm their business reputation.

Thus, the motivations behind collecting customer data are varied, but the most important factors are the improved services and improved customer communication and understanding.

5.2 The process of data collection

Data is collected through a multitude of different surfaces. This includes, but is not limited to, cookies, apps, websites, customer service. In the survey conducted by the Norwegian Data Protection Authority (2020) they found that seven out of ten participants feel they lack control of their online privacy and lack knowledge on how it is being collected and stored. Companies who process and use customer data would likely earn customer trust if they increased their transparency. Furthermore, the survey found that on average, people trust public companies over private ones. By being transparent, private corporations such as Telia and DNB, could probably increase customer trust.

The privacy policies offer insight into how and when data is collected, and the legal requirements and restrictions that are in place to ensure customer privacy. The privacy policies also describe how a customer can opt out of certain methods of data collection. As Ljøgodt states in his interview, should a customer be interested in restricting Telia's data collection and use on their personal online behavior it is relatively easy to opt out. Both Ljøgodt and Oftedahl state that customers who opt out of, for example, having their data included in the analytical and statistical uses will automatically be separated from those who have not opted out and, thus, be excluded from company statistics and analyses.

Data collection is a complex process, and the avenues of data collection seem to be increasing. My interviewees revealed that most of the data that is collected happens through utilization of the services. Customers who are interested in exactly how data are gathered can easily access privacy policies and gain some knowledge into what processes are involved. A privacy policy is not exhaustive and the extent of the information in a privacy policy may not be satisfactory to some. However, included in the privacy policies are ways of contacting employees who may give more extensive information on the topic.

Increasing awareness and knowledge into how data is gathered, stored and used will likely benefit both users and the companies. My interview with Oftedahl revealed that DNB wants to walk with the customers to find a way where data use benefits both parties. They do not want to cross over their customers' boundaries, but rather, use data in an efficient way without compromising their customers' privacy.

Companies that are subject to GDPR need to justify why the processing of customer data is necessary, and there needs to be a legitimate interest behind the utilization of the data.
One thing to note in the privacy policies is that marketing and analytics is considered as much of a legitimate interest to the companies as fraud management. This is because a financial gain is identified as a legitimate interest in the GDPR because generating revenue is a legitimate business objective. However, as Ljøgodt explains, although marketing is a legitimate interest, the companies are still responsible for the protection of customer privacy and economical gain does not surpass the privacy considerations that need to be in place before data processing can happen.

5.3 Privacy concerns

Both Oftedahl and Ljøgodt expressed a desire for transparency with their customers. The focus on transparency is reiterated in the annual reports and the privacy notices included in the document analysis. Morey, Forbath and Schoop (2015, p. 5) found that letting customers understand the exact privacy trade-offs they are making so they are able to make an informed decision on whether the benefits outweigh the trade-offs is considered best practice. This also supports Andrejevic's (2014, p. 1685) findings that the concern over possible harm is less than the frustration of feeling powerless and uninformed about what companies are actually doing. Oftedahl's thoughts on wanting to walk together and find out where to draw the line together with their customers as their use of data increases seems to be a positive suggestion. She illustrates this with an example where they noticed that they received a decreasing number of queries into data collection and use the more times DNB publicized transaction data during the pandemic.

One could argue that the increased visibility of how customer data is being used seems to have a desensitizing effect on customers. Perhaps customers get used to the publication of data as it is perceived as increasingly more normal for every time data is publicized. However, while it may be the result of customers having to get used to the idea, another possibility is that the customers realize that their personal data is not at risk of being misused, that their data is well protected, and that anonymization is satisfactory. Perhaps the increased awareness around how customer data are used results in increased customer trust towards the companies. Martin (2018) found that consumers experienced a decrease in trust in firms who violated privacy expectations. This decrease in trust is not necessarily easy to build back up, as the integrity of the firm is diminished. Furthermore, Martin (2018) found that the more experienced technologically consumers are, the more they tend to care about privacy factors. As a result, if Telia and DNB wish to be seen as relevant and trustworthy organizations by technologically competent customers, they also need to cater to customers with technological knowledge who are likely to care more about the companies' privacy policies and data protection practices. Establishing and maintaining a relationship with customers is important for firms and its future success. Mou, Shin and Cohen (2017) findings also suggest that trust is very important for customers who are making a privacy decision. My document analysis also showed that customer trust is important for the companies and something they are highly aware of. DNB stated that maintaining and building customer trust is imperative for the success of DNB moving forward. Due to the customers having the option of opting out of data analyses, the companies are essentially at the mercy of the customers trusting them enough with their data and feeling safe enough to not opt out.

Research conducted on user privacy preferences and concerns point to transparency as a way of increasing customer trust and decreasing privacy concerns. The more a company is transparent about the process of data collection, data use and customer privacy protection, the more likely customers are to experience a decrease in their privacy concerns. The survey from The Norwegian Data Protection Authority found that seven out of ten participants did not feel like they have enough knowledge on how companies use and collect their data. I would argue that there is an opportunity for companies to increase the public awareness on data collection and use that will benefit both the companies and the customers. According to Morey, Forbath and Schoop (2015), increased knowledge on the processes and security measures that are in place at the companies to ensure privacy protection and prevent misuse of data is likely to decrease customers' privacy concern. Additionally, Paul, Scheibe and Nikalanta (2020, p. 4389) found that GDPR compliance in companies mitigates users' privacy concerns. For companies such as Telia and DNB; that are GDPR compliant, that have stricter internal regulations and that value customer privacy highly, the outcome of being transparent is likely to increase customer trust.

Raguseo (2018) identified the risks and benefits for companies implementing big data as a business strategy. The highest ranked risks that were identified were in terms of security and privacy issues, this is also mentioned as a risk in the annual reports of both Telenor and DNB ASA. As the amount of data increases, the companies have to continuously update their security measures to ensure the safety of customer data.

In her interview Oftedahl poses the same questions as director of The Norwegian Data Protection Authority, Bjørn Erik Thon. When discussing DNB's participation in a study with Stanford University she speaks on the ethical questions that arise; even though what we are doing is technically legal? Should we do it? Will it add value for our customers? Will our customers think it is the right thing to do? This is an important discussion and one I think will stay relevant in the future. For companies who have exploited their customers' personal data there is a tendency to hide behind the fact that what they are doing is within the laws and regulations. However, this does not mean companies should be exempt from criticism or hard-hitting questions about their practice and how it impacts on their users. From my interviews, both Telia and DNB are aware of their moral and ethical responsibilities and how their misuse of customer data could potentially affect those concerned. Ultimately, it is the companies' responsibility to ensure the right processes are in place to safeguard that their customers' right to privacy is upheld. Perhaps this discussion should invite customers to speak on their preferences on this topic so businesses and users can come up in a way that is satisfactory for all parties involved. After all, it is the customers' data and privacy that is at the heart of the discussion.

5.3.1 The limitations of data use

Fourcade and Healy (2017) discussed the limitations of data analyses. Oftedahl also mentions how the data does not offer the whole story of what is happening, it represents facts, but not reasons behind potentially complex decisions or situations.

Oftedahl discussed that it was important for them to not be perceived as creepy by their customers. She mentioned an example where data can be used to help customers who leave their application for a loan unfinished for a period of time. DNB can see, in real time, if a customer is having issues completing their loan application. However, the customer might not be struggling to understand the loan application at all, they may be interrupted by something or someone, dinner might be ready, or maybe they have kids they need to put to sleep. There are so many various situations that might be going on in their real life, but these situations will present themselves similarly in the data; the loan application is incomplete. This was also mentioned by Fourcade and Healy (2017, p. 26) where they stated that data does not have the ability to present the full picture. Where, for some customers, if a little information box or a bot asking if a customer needs help completing their application would be considered very helpful, other customers might find that to be unnecessary, annoying, or worse, creepy. Some customers might even experience a situation where a "do you need help" pops up as if they are being surveilled and that their privacy is being infringed on. It is difficult to please every individual customer as their personal views and preferences on privacy are bound to differ.

5.4 GDPR and its effect

While companies are subject to laws and regulations these are likely to change, as Ljøgodt stated in his interview some of the regulatory framework is already being discussed as being too strict. Through this thesis it has been established that customer trust builds customer satisfaction, Morey, Forbath and Schoop (2015, p. 10) argue that customers who lack knowledge and insight into companies' privacy processes are less likely to trust them, as they do not know what is actually happening. From this I could make the assumption that if customers know their personal data is well protected, they would be more likely to trust a company with their personal data. However, the companies would have to grant the customer access to this information through increased transparency. So, if companies educate their customers about the laws, but also about the strict internal guidelines these companies follow, they might be less worried about their privacy not being protected.

Laws and regulations can act as a way of ensuring that the processing of data is happening safely, and people's privacy is being protected. Having an independent body being able to impose sanctions on businesses or organizations who do not comply with the laws in place is also a way of minimizing the privacy concerns from the users. Furthermore, it holds businesses accountable in cases where user privacy was not sufficiently protected.

Previous research suggests that companies being subject to GDPR mitigate user privacy concerns. Paul, Scheibe and Nilakanta (2020, p. 4394) found that if companies provide a GDPR compliant privacy policy to users, their users experienced an increased control over their online privacy. The more effective the privacy policy was perceived, the greater effect it had on reducing user privacy concern.

Ljøgodt spoke on how the implementation of GDPR had changed how Telia operated. He mentioned that GDPR has led to increased focus on customer privacy, and that its regulations have added several work processes before anything is decided and released in terms of customer data. The risk of not being GDPR compliant has made it even more important for Telia to ensure that their customers' data are protected. He also mentioned that GDPR has increased their interest in customer data and how Telia can best use it as an advantage in the industry. While I think GDPR is a necessary step in ensuring customer privacy and preventing data misuse, it is also clear that the implementation of GDPR has increased awareness on customer data both in companies and in customers. In a way, the implementation of GDPR seems to have confirmed how valuable customer data is, and in that, encouraged the use of customer data, albeit with respect to individuals' privacy. Ljøgodt portrayed an increase of security measures, but also a sense of newfound creativity around the possibilities of customer data.

Critical researchers like Couldry and Yu (2018, p. 4474) have questioned whether the GDPR sufficiently protects individuals from the potential harms of continuous data collection. As the GDPR only regulates the use of personal data, not the collection of it, they (2018, p. 4487) argue that there needs to be a debate surrounding the ethical and moral basis for continuous data collection. For humans there are certain basic rights that have been established in many international regulations and documents, one of which is the United Nations Declaration of Human Rights. The right to privacy is identified as a human right. I would argue that as data use is likely to become increasingly important for companies, and the collection of data is likely to continuously increase, there needs to be further discussions on whether the current laws and regulations are satisfactory in protecting the human right to privacy.

5.5 Dataism and Datafication in Telia and DNB

The companies I investigated view continued use of customer data as a key success factor for the future. This perception of data can be considered an example of dataism and how it has spread as an ideology. Van Dijck (2014, p. 197) refers to dataism as an ideology, conviction and a secular belief that measures its success in how many people trust their personal data to large corporations. I would also argue that van Dijck's (2014) argument that a part of dataism is how people trust their data to large companies has progressed to also include how companies now rely on customers' trust. This argument is specifically relevant to GDPR compliant companies. This can be seen as a consequence of GDPR and stricter privacy laws. As customers gain more control over their personal data, companies now have to earn customers' trust in order to ensure the use of customer data. Dataism represents a mindset where data is the solution to success. Datafication can be seen as the process of turning data into valuable information, whereas dataism can be described as the ideology behind this process. As many people do trust their personal data with companies it is safe to say that dataism is a very successful ideology and is becoming more prevalent and spreading at a fast pace. In terms of organizations, I would argue that dataism also penetrates the companies themselves. By this I mean that the companies have almost made themselves victims of the ideology. Through my document analysis and my interviews, the companies are convinced that it is impossible to stay competitive and relevant in their industries without using customer data as a way of getting ahead. Regulations like the GDPR, which allows customers more control over their data, has changed the execution of datafication, and the companies have made themselves rely on customer trust to collect and use customer data. There are multiple examples both in the document analysis and through my interviews which point to how they view data processing and collection as something that will become increasingly important in the future. Businesses view data processing as a way of getting ahead, or even just staying competitive. By not utilizing data there is a sense of falling behind and not being experienced as relevant to customers or competitors.

Zuboff's (2019, p. 8) definition of surveillance capitalism includes the words "parasitic", "rogue mutation", "threat" and "coup". DNB and Telia's collection and use of user data is very different to what Zuboff describes as surveillance capitalism. However, both DNB and Telia are participating in the process of datafication. Datafication is the process in which people's everyday life streams and transactions are being transformed into quantifiable data (Van Dijck, 2014, p. 198). Although the way Telia and DNB use these data is not necessarily harmful to the individual customer, they are using aggregated customer data to further their business. Fourcade and Healy (2017, p. 13) describe how Facebook, and other digital firms, run tests on their users to see whether users prefer one layout to another, or whether a service or a product works well, both for the company and the customers. One test was especially criticized for experimenting with the emotional lives of their users. Telia and DNB both use data to improve services and products, Oftedahl describes how through data they can have a more "fail fast, fail harder" approach to the release of products and services. Through analyzing customer data their customers will essentially tell them what is working and what could be improved. It is important to recognize the possible impact these "tests" may have on their customers and ensure these are conducted in an ethical manner that will not interfere negatively with their customers' lives.

Even though customers of Telia and DNB are paying for a service and receiving the product they are paying for, that service continues to create value for the companies even after it has been paid for, this value is generated through data collection that occurs within the use of this service. Sadowski (2019, p 7) exemplifies this through the smart fridge. A smart refrigerator, in addition to keeping its contents cool, has added services like letting its user see what is in it from anywhere. Traditionally, a fridge is a commodity that is paid for and that single payment is all the value the company that sells it will receive. In contrast, a smart fridge continuously collects data on the user and this data is then turned into valuable information for targeted advertising companies who will now know what brands they should include to create an effective personalized ad. While DNB and Telia are not exactly selling fridges, and their payments are not a one-off, but rather subscriptions, this analogy holds true for them too. The services their customers are paying for, through the use of them data is being generated. This data is valuable to the companies and continues to provide value as long as their services are being used.

The findings from the interviews suggest that data has become a commodity of some sort, both Ljøgodt and Oftedahl recognize the impact data have on business decision-making as well as on their business model. They both mention how data is used as a form of communication to see what the customers want, in terms of products and services. As such, it is a valuable commodity for the companies to provide the best possible service. Providing the best service is how the companies keep their customers from 'turning' in a competitive industry.

However, the data processing and use have limits. Not only does GDPR have an impact on what the data can be used for, but Telia and DNB do not want to use customer data for purposes that may be harmful or perceived as "creepy" by their customers.

5.6 The future use of data

The increasing use of data in business decisions and service development is not likely to decrease in the near future. The term dataism is descriptive of how Telia and DNB view the use of data today and in the future. There is a sense of awakening and realization around the future possibilities with data. In her interview, Oftedahl discussed how DNB is a part of a project about ethical and responsible use of data, and talks about how Deutsche Bank, Visa and MasterCard have gotten further into the process compared to DNB. This is an example of how dataism can be seen as an ideology that has nestled its way into industries and is now viewed as something highly important, almost necessary, to be successful. My informants both discussed how data is an important tool to maintain their position in their industry, and that an effective way of using and analyzing data to maximize the benefits is essential.

Digital technologies have created a space where companies who do not educate themselves on the use of data are unlikely to survive in a competitive market. However, customers of companies who collect and use their personal data should also make an effort to be educated on the topic. Keeping the companies accountable and ethically responsible in a rapidly changing environment will be vital for both the companies as well as for the consumers. As Andrejevic's (2014) findings suggest, transparency can be a solution for companies to avoid customer frustration, dissatisfaction and distrust. Both my interviewees and the document analysis suggest that transparency will continue to be an area of focus to increase customer knowledge on how their data is used. Especially in terms of future use, which is likely to look a little different than today as new and innovative ways of use are constantly being developed.

In his interview, Ljøgodt gave an example as to what the future of data use would look like for Telia. He said that as GDPR puts limitations on what can be used without explicit consent from customers, Telia might be looking into what getting that explicit consent from a customer would mean for future use. Bonatti and Kerrani (2019) proposed an approach to consent management. They use an example where location data would need to be analyzed in order to improve the services of a smart watch. Ljøgodt gave an example of using location data which would allow targeted advertising based on an individual's location data. For the purpose of this discussion, I will use Ljøgodt's own example from his interview, but he did say that this just is an example, and he does not even think that Telia has looked into this particular scenario. Using Bonatti and Kerrani's (2019, p. 14) approach and Ljøgodt's example Telia would have to obtain consent for the 'analysis' of 'location data' for the purpose of 'personalization of ads based on your location'. Telia would then be able to conduct data mining on the datasets belonging to the customers they obtained consent from. The customer would then get relevant advertisements based on their location, and Telia would be able to profit off of those location data. Bonatti and Kerani (2019, p. 14) recognize that there are issues that need to be considered, such as the difficulty of preventing the analysis to lead to other insights not permitted by the consent policy. However, should Telia find a way to execute this legally and safely, this is an example of what data use could look like in the future.

Zhu, Ou, Van den Heuvel and Liu (2017, p. 435) found that it is imperative for businesses who offer personalization to do so in a way that is in line with specific customers' privacy concerns. They found that for some users, personalization may prevent users from engaging with certain websites or companies as they are strongly against companies collecting and processing their personal data. As such, companies like Telia and DNB should allow personal privacy concerns into the privacy preferences, and this would allow the companies to offer a generic and non-personalized experience for the customers who do not wish personalization. Like Ljøgodt and Oftedahl discussed, customer insight is very important because it means they can see what their customers want. By allowing their customers to easily opt out of any personalization they can even make those customers feel seen. Hence, it is important to quantify customers' privacy concerns in an effective way.

There is no doubt that the collection and use of data can lead to a world where privacy and autonomy can be considered a luxury of the past. The most appropriate example here is probably China and their data and surveillance-based society. On the other hand, data can also be used for betterment. For example, by optimizing products and services, ensuring the safety of services, minimizing waste and optimizing operations (Pelteret & Ophoff, 2016, p. 284). Ljøgodt mentioned how the government was interested to know how people's movement in society changed during the pandemic, and Telia was able to provide aggregated location data that could indicate to what degree citizens were following the guidelines provided by the government. Had the data showed that citizens were not following the recommendations proposed by the government, they could modify their recommendations or tone of voice to reflect the situation that was portrayed by the data. In the annual reports all three companies wrote about how their data analyses had acted as a tool in the fight of the pandemic. However, it is vital to acknowledge that the use of data can also be misused and infringe on the privacy of individuals (Pelteret & Ophoff, 2016, p. 284).

5.7 Critical research and how Telia and DNB are different

Although the companies that were looked at in this study cannot directly be compared to companies such as Facebook and Google, this study offers insight into large Norwegian companies who have extensive amounts of data. Zuboff's critical view of data use as a method to predict human behavior was the starting point of this thesis as her book and contention is what got me interested in the topic. However, it is important to discern between the type of regulated companies this thesis looked at and the type of unregulated and exploitative companies that Zuboff mentions in her book. The most obvious difference between the companies that are described by critical research on user data and privacy and the companies this thesis has explored is the fact that companies such as Google and Facebook rely solely on user data as their source of income. Data is their entire business model as they do not have customers paying for their services, other than advertisers. Google and Facebook offer their services for free, so the payment of the user is their private data. Fourcade and Healy (2017, p. 16) present the notion that Google and Facebook essentially are advertising companies, as advertising revenue makes up over 90% of their income. Furthermore, Google and Facebook are not in a competitive market where they are fighting to keep users loyal to their services. Contrastingly, companies like Telia and DNB have paying customers and their business model is centered around offering their customers the best services as their customers are free to change their service provider at any time. Their reputation is important, and keeping customer data secure is vital for creating a space where customers feel secure and taken care of. DNB and Telia did not start out as a free service, they have paying customers who hold the companies to a certain standard.

5.8 Future research and limitations

This thesis is an introduction into investigating the process of collecting and using customer data at two Norwegian companies, it also investigated their view on user privacy. Future research should further investigate the potential benefits of transparency surrounding user data. This thesis investigated the topic from the companies' perspective, and my analysis shows that the customers' privacy is very much a consideration for the companies. Therefore, research from the customers' perspective would also be very interesting and relevant to look into. As this thesis only managed to gain access into two companies, it would be preferential to further investigate larger companies in Norway/the Nordics who have access to large amounts of user data. This thesis was focused on larger companies who process an enormous amount of customer data, and my analysis suggests that business reputation plays a big role in deciding how careful to be when using customer data. Future research could investigate differences between smaller and larger companies to see if there are any differences in how well customer privacy is protected and/or discussed. The document analysis was a descriptive analysis and only included the most recent documents available. Future research could investigate how GDPR has changed companies views on privacy, how the process of data collection and use has changed and how companies' conceptualization of customer data and privacy differ from before the implementation of GDPR. Furthermore, as data collection and use will likely increase and continue to impact society and businesses, looking at how the fast paced digital and technical developments will impact on business strategies and citizens privacy will be exciting. While I did not experience that my interviewees provided falsehoods or misrepresentations, I acknowledge that they both spoke on behalf of both themselves and their company and therefore might have unconsciously altered their responses accordingly.

6 Conclusion

Through this thesis I hope to have opened up the conversation surrounding user data further, specifically in Norway. The findings of this thesis suggest that the use of customer data is likely to increase, and it will likely have a big impact on both businesses and customers in the future, but not necessarily at the cost of user privacy. I hope my thesis has made how and why businesses collect, use and process user data a little clearer. Moreover, I hope my thesis can encourage companies to be more transparent with customers in the future and perhaps include customers to be a bigger part of the privacy discussions.

6.1 Motivation for data collection

Excluding the data that have to be collected due to legal reasons, Telia and DNB, collect and use customer data mainly to stay competitive in a tough industry and to be able to offer their customers the best possible offer and service they can. Using data to conduct analyses that are able to tell them what their customers want is important. Furthermore, the data is collected so the companies can become more data driven. The large business decisions should be made based on evidence found in the data analyses, not based on a gut feeling. As society turns increasingly digital, the way customers communicate with companies is mainly through data. There is a monetary motivation to collect user data, but the findings suggest that the main motivation is to keep customers from turning by offering the best possible service. Paying customers is how these companies generate most of their revenue, and they want to keep building their customer base. Without using customer data, it would be difficult to have an upper hand, or even to stay relevant in a competitive and rapidly developing industry.

6.2 How does data collection occur

Data collection is a multifaceted process. The main data collection happens through the utilization of the products and services. Using the mobile bank, using a streaming service, accessing an app, contacting customer service and many more avenues. Moreover, cookies when visiting the website is also a way of gathering data, and this is why visitors of the websites may see advertisements for Telia or DNB weeks after visiting their website. Data is also collected through explicit information customers give when contacting customer service or just signing up for a service. Essentially, data collection happens across platforms and the use of services and products.

6.3 Privacy concerns

Ethics and privacy are two important topics and areas of focus for these companies. Not only is it important because breaking the law would mean a large financial fine, but because trust and reputation are important for customers. DNB are participating in a project with Stanford University, and the results suggest that DNB are asking questions and trying to find out where to draw the line on what data they should be using, and what data they should not be using even though it is legal. Both of the respondents were adamant that they would never use or sell data related to health and preferably avoid anything that could be perceived as sensitive data by their customers. The companies recognize and are aware of their responsibility of protecting customer privacy.

6.4 How companies conceptualize the collection and use of customer data, and how central customer privacy is in this conception

In conclusion, companies conceptualize the collection and use of customer data through a belief in customer data as a prerequisite for future success. The companies portray how dataism, an ideology where the belief in data is at the center, is growing. The growing use of customer data does not happen at the expense of customer data. Companies view maintaining customer privacy and trust as an essential part of the continuing use of customer data and are focusing on finding out how this can benefit both parties equally, while ensuring the protection of customer privacy.

References:

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

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

Acquisti, A., John, L.K. and Loewenstein, G., 2013. What is privacy worth?. *The Journal of Legal Studies*, *42*(2), pp.249-274.

Andrejevic, M., 2014. Big data, big questions| the big data divide. *International Journal of Communication*, *8*, p.17.

Andrew, J. and Baker, M., 2019. The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics*, pp.1-14.

Barnes, S.B., 2006. A privacy paradox: Social networking in the United States. *First Monday*.

Bélanger, F. and Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, pp.1017-1041.

Benisch, M., Kelley, P.G., Sadeh, N. and Cranor, L.F., 2011. Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, *15*(7), pp.679-694.

Bertino, E., Merrill, S., Nesen, A. and Utz, C., 2019. Redefining data transparency: A multidimensional approach. *Computer*, *52*(1), pp.16-26.

Bonatti, P.A. and Kirrane, S., 2019, July. Big Data and Analytics in the Age of the GDPR. In *2019 IEEE International Congress on Big Data (BigDataCongress)* (pp. 7-16). IEEE.

Bowen, G.A., 2009. Document analysis as a qualitative research method. *Qualitative research journal*.

Brinkmann, S. (2013). *Qualitative interviewing*. Oxford university press.

Brinkmann, S. and Kvale, S., 2018. *Doing interviews* (Vol. 2). Sage.

Coffey, A., 2014. Analysing Documents. *The SAGE handbook of qualitative data analysis*, pp. 367-379.

Couldry, N. (2017). Surveillance-democracy. *Journal of InfSormation Technology & Politics*, *14*(2), 182-188.

Couldry, N. and Van Dijck, J., 2015. Researching social media as if the social mattered. *Social Media+ Society*, *1*(2), p.2056305115604174.

Couldry, N. and Yu, J., 2018. Deconstructing datafication's brave new world. *New media & society*, *20*(12), pp.4473-4491.

Crouch, M. and McKenzie, H., 2006. The logic of small samples in interview-based qualitative research. *Social science information*, *45*(4), pp.483-499.

Datatilsynets årsrapport (2018) https://www.datatilsynet.no/om-datatilsynet/arsmeldinger/arsrapport-for-2018/

Dienlin, T. and Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, *45*(3), pp.285-297.

DNB- konsernet, 2020. Årsrapport 2020: Resultater som teller. Accessed at: https://www.ir.dnb.no/sites/default/files/DNB_ASA_arsrapport.pdf

(European) General Data Protection Regulation (GDPR) (2016) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. *Official Journal of the European Union*. Available at: http://ec.europa.eu/justice/data-protection/ reform/files/regulation_oj_en.pdf

Fourcade, M. and Healy, K., 2017. Seeing like a market. *Socio-Economic Review*, *15*(1), pp.9-29.

Hoffmann, C., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox.

Karppinen, K. and Moe, H., 2012. What we talk about when we talk about document analysis. *Trends in Communication Policy Research: New Theories, Methods and Subjects. Bristol: Intellect*, pp.177-193.

Karppinen, K. and Moe, H., 2019. Texts as data I: Document analysis. In *The Palgrave handbook of methods for media policy research* (pp. 249-262). Palgrave Macmillan, Cham.

Kehr, F., Kowatsch, T., Wentzel, D. and Fleisch, E., 2015. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), pp.607-635.

Knijnenburg, B.P., Willemsen, M.C., Gantner, Z., Soncu, H. and Newell, C., 2012. Explaining the user experience of recommender systems. *User Modeling and User-Adapted Interaction*, *22*(4), pp.441-504.

Kokolakis, S., 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, pp.122-134.

Kvale, S. and Brinkmann, S., 2009. *Interviews: Learning the craft of qualitative research interviewing*. sage.

Lamoureux, E. (2016). *Privacy, surveillance, and the new media you* (Vol. Volume 96, Digital formations). New York.

Machuletz, D. and Böhme, R., 2020. Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(2), pp.481-498.

Mai, J.E., 2016. Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), pp.192-199.

Martin, K., 2018. The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research, 82,* pp.103-116.

McAfee, A., Brynjolfsson, E., Davenport, T.H., Patil, D.J. and Barton, D., 2012. Big data: the management revolution. *Harvard business review*, *90*(10), pp.60-68.

Mejias, U.A. and Couldry, N., 2019. Datafication. *Internet Policy Review*, *8*(4).

Menard, P. and Bott, G.J., 2020. Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers & Security*, *95*, p.101856.

Morey, T., Forbath, T. and Schoop, A., 2015. Customer data: Designing for transparency and trust. *Harvard Business Review*, *93*(5), pp.96-105.

Mou, J., Shin, D.H. and Cohen, J.F., 2017. Trust and risk in consumer acceptance of e-services. *Electronic Commerce Research*, *17*(2), pp.255-288.

Natow, R.S., 2020. The use of triangulation in qualitative studies employing elite interviews. *Qualitative Research*, *20*(2), pp.160-173

NESH (2016). Guidelines for Research Ethics in the Social Sciences, Humanities, Law and Theology. Oslo: The National Research Ethics

Paul, C., Scheibe, K.P., & Nilakanta, S. (2020). Privacy Concerns Regarding Wearable IoT Devices: How it is Influenced by GDPR? *HICSS*.

Pelteret, M. and Ophoff, J., 2016. A review of information privacy and its importance to consumers and organizations. *Informing Science*, *19*, pp.277-301.

Raguseo, E., 2018. Big data technologies: An empirical investigation on their adoption, benefits and risks for companies. *International Journal of Information Management*, *38*(1), pp.187-195.

Raguseo, E. and Vitari, C., 2018. Investments in big data analytics and firm performance: an empirical investigation of direct and mediating effects. *International Journal of Production Research*, *56*(15), pp.5206-5221.

Reigstad, J., & Bye Skille, Ø. (2019). DNB vil tjene penger på kundene - videreselger data om handlemønster. *NRK*. Retrieved from https://www.nrk.no/norge/dnb-vil-tjene-penger-pa-kundene---videreselger-data-om-handlemonster-1.14711810

Romansky, R., 2019. A Survey of Informatization and Privacy in the Digital Age and Basic Principles of the New Regulation. *International Journal on Information Technologies and Security*, *1*(11), pp.95-106.

Roulston, K., 2014. Analysing interviews. *The SAGE handbook of qualitative data analysis*, pp.297-312.

Roulston, K. & Choi, M. (2018). Qualitative interviews. In Flick, U. *The sage handbook of qualitative data collection* (pp. 233-249). 55 City Road, London: SAGE Publications Ltd doi: 10.4135/9781526416070

Sadowski, J., 2019. When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, *6*(1), p.2053951718820549.

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.A. and Santos, I., 2019, July. Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (pp. 340-351).

Sheng, H., Nah, F. F. H., & Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, *9*(6), 15.

Silverman, J. (2017). Privacy under Surveillance Capitalism. *Social Research,84*(1), 147-164.

Syvertsen, T., 1998. Dokumentanalyse i medievitenskapen: Tilgang, kildekritikk, problemstillinger. og webkilder. *Arbeidsnotat, Institutt for medier og kommunikasjon, Universitetet i Oslo*.

Sørensen, J. and Kosta, S., 2019, May. Before and after gdpr: The changes in third party presence at public and private european websites. In *The World Wide Web Conference* (pp. 1590-1600).

Telenor Group, 2020. Årsrapport 2020. Accessed at: https://www.telenor.com/wp-content/uploads/2021/05/Telenor_Arsrapport_2020_ii.pdf

Telia Company, 2020. Better Connected Living: Annual and Sustainability Report 2020. Accessed at: https://annualreports.teliacompany.com/globalassets/pdf/telia-company--annual-and-sustainability-report-2020.pdf

Teltzrow, M. and Kobsa, A., 2004. Impacts of user privacy preferences on personalized systems. In *Designing personalized user experiences in eCommerce* (pp. 315-332). Springer, Dordrecht.

Turner, F. 2018. The arts at Facebook: An aesthetic infrastructure for surveillance capitalism. *Poetics*, *67*, 53-62.

Van Dijck, J., 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & society*, *12*(2), pp.197-208.

von Kardorff, U., Flick, E., & Steinke, I. (2004). *A Companion to Qualitative Research*. London: Sage Publications.

Yu, J. and Couldry, N., 2020. Education as a domain of natural data extraction: analysing corporate discourse about educational tracking. *Information, Communication & Society*, pp.1-18.

Zaeem, R.N. and Barber, K.S., 2020. The effect of the GDPR on privacy policies: recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, *12*(1), pp.1-20.

Zhu, H., Ou, C.X., van den Heuvel, W.J.A. and Liu, H., 2017. Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management*, *54*(4), pp.427-437.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Vedlegg A- Informasjonsskriv

Vil du delta i forskningsprosjektet

«Customer Data and Privacy in Norwegian Companies; Companies' perspective on user data and the privacy discourse surrounding it»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke hvorfor og hvordan selskaper benytter seg av brukerdata. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva en deltakelse vil innebære for deg.

Formål

Studien gjennomføres som del av Sophie Katharina Egeberg Nyborgs masteroppgave ved Institutt for medier og kommunikasjon, Universitetet i Oslo (UiO). Formålet med studien er å finne ut mer om motivasjonen som ligger bak det å samle inn brukerdata, prosessen videre og hvordan selskaper ivaretar kundenes personvern. Metoden som vil bli brukt for å samle inn data til prosjektet er intervjuer.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Oslo er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Din posisjon og kompetanse rundt personvern og/eller brukerdata gjør at jeg svært gjerne vil gjennomføre et forskningsintervju med deg om dette.

Hva innebærer det for deg å delta?

Deltakelse i studien innebærer et forskningsintervju. Intervjuet er anslått å vare i ca 45-60 minutter. Det vil være opp til deg om intervjuet blir gjennomført ved å møtes fysisk eller over Zoom eller lignende. Dersom du takker ja til å stille på intervju vil vi be om å få bruke opptaker for å på den måten sikre korrekt gjengivelse av intervjuet. Intervjuene gjennomføres av masterstudent Nyborg.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Det er kun masterstudent Nyborg som vil ha tilgang til intervjumaterialet. Intervjuene transkriberes av Nyborg. Dataene vil bli lagret på maskinvare tilhørende UiO med adgangsbegrensning for andre enn Nyborg.

Når materialet er analysert, vil det kun bli brukt i Nyborgs masteroppgave. Ved publisering kan ditt navn og din tittel fremgå, men alle sitater fra deg – både når du er sitert direkte og der ditt navn fremgår indirekte – skal godkjennes av deg før bruk. Dato for når intervjuet ble gjennomført vil alltid fremgå, slik at konteksten for dine sitater kommer klart frem.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Lydfiler og transkriberte intervjuer slettes når prosjektet avsluttes, noe som etter planen er senest 31.12.2021.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Oslo har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Marika Lüders, veileder, på epost marika.luders@media.uio.no eller telefon 99525206,
- Sophie Nyborg, student, på epost: sknyborg@student.media.uio.no eller telefon 97041999
- Vårt personvernombud: personvernombud@uio.no

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Sophie Nyborg

Samtykkeerklæring

.

Jeg har mottatt og forstått informasjon om prosjektet *[sett inn tittel]*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

□ å delta i intervju
□ at opplysninger om meg publiseres slik at jeg kan gjenkjennes (se informasjonsskriv)

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

----
(Signert av prosjektdeltaker, dato)

Vedlegg B- Intervjuguide Telia

TELIA INTERVJUGUIDE

Introduksjon

Hei, tusen takk for at du stiller på intervju.

Er det ok at jeg tar opp intervjuet? Alle sitater i den endelige oppgaven, både direkte og indirekte, skal godkjennes av deg på forhånd. Prosjektet er registrert og godkjent av Norsk senter for forskningsdata.

Informasjonsskriv

Innledning

Kan du fortelle meg din stillingstittel og navn?

Hvor lenge har du jobbet i Telia? Har du hatt andre stillinger i selskapet tidligere?

Kan du fortelle litt om hva din stilling og rolle innebærer? Gjerne litt om ansvars- og arbeidsoppgavene dine?

Motivasjon:

Hva er hovedmotivasjonen deres for å samle inn brukerdata?

På hvilken måte kan brukerdata utnyttes på en måte som gagner kunder?

På hvilken måte kan brukerdata utnyttes på en måte som gagner dere som selskap?

Hva ser du og Telia som de største mulighetene med brukerdata fremover?

Tenker du at analyser av brukerdata vil bli enda viktigere i tiden fremover? Hvordan/hvorfor?

På hvilken måte vil du si at brukerdata påvirker forretningsgrunnlaget for Telia? (eventuelt for hele bransjen de representerer)

I personvernserklæringen nevner dere hvordan dere bruker personopplysninger, blant annet: lage kunde/bruksprofil for å tilby personlig tilpasning av tjenester

Kan du si litt om motivasjonen bak det å ville tilby personlig innhold til kundene og hvordan en slik kundeprofil blir laget?

Prosessen:

Kan du beskrive hvordan brukerdataen samles inn?

Hva er hovedfunksjonen til brukerdataen?

Hva skjer med brukerdataen etter den er samlet inn?

Vet dere hva informasjonen dere selger blir brukt til eller hva som skjer med den etter den er solgt?

I personvernærkleringen står det at personlig informasjon blir samlet inn automatisk når en benytter seg av feks mobilnettet til å ringe, eller besøker nettsiden deres? Er denne typen innsamling av personlig data noe man kan reservere seg mot? Og hva slags personlig informasjon er det snakk om?

På hvilken måte blir det en mer relevant brukeropplevelse av en nettside dersom annonsene på den nettsiden er basert på kundens personlige informasjon, Datatilsynet feks har en undersøkelse som viser at 3 av 4 er negative til bruken av målrettede annonser? Har du noen tanker rundt dette?

Hva vil det si å «vaske» kontaktinformasjon mot kunderegistre?

Kan du beskrive/gi et eksempel på de «særlige forhåndsreglene» som tas for å forsikre om at underleverandører opptrer i samsvar med personvernsærklæringen?

Personvern:

Hvordan sikrer dere anonymisering av brukerdata (i tråd med GDPR og retningslinjer fra Datatilsynet)?

Hva blir lagt mest vekt på i diskusjonene rundt brukerdata og personvern?

Hvordan har GDPR forandret måten brukerdataen blir behandlet?

Ser du/dere noen (etiske) problemer rundt å samle inn og selge brukerdata? Hvorfor/Hvorfor ikke?

I henhold til GDPR: Hvordan jobber dere med at dataen dere samler inn og behandler er i henhold til det den skal brukes til? Og at det ikke blir for mye eller unødvendig data som blir samlet inn?

Jf. «it should be adequate, relevant, and limited to what is necessary for the purpose (‘data minimisation’). It’s your company/organisation's responsibility as controller to assess how much data is needed and ensure that irrelevant data isn’t collected[1].”

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

Opplever dere at dere at kundene deres er mer opptatt av spørsmål knyttet til brukerdata og personvern enn tidligere (før GDPR). [Hvis ja:] Hvordan kommer det til uttrykk? Hva lurer kundene på?

Avslutning

Er det noe du vil legge til som jeg ikke har spurt om, eller som du synes det er viktig at jeg får med meg?

Er det noen andre i Telia du tenker jeg burde snakke med?

Tusen takk for at du stilte på intervju!

Vedlegg C- Intervjuguide DNB

Generell intervjuguide for DNB:

Introduksjon

Er det ok at jeg tar opp intervjuet? Alle sitater i den endelige oppgaven, både direkte og indirekte, skal godkjennes av deg på forhånd. Prosjektet er registrert og godkjent av Norsk senter for forskningsdata.

Informasjonsskriv levert på mail

Innledning

Kan du fortelle meg din stillingstittel og navn?

Hvor lenge har du jobbet i DNB? Har du hatt andre stillinger i selskapet tidligere?

Kan du fortelle litt om hva din stilling og rolle innebærer? Gjerne litt om ansvars- og arbeidsoppgavene dine?

Motivasjon:

Hva er hovedmotivasjonen deres for å samle inn brukerdata?

På hvilken måte kan brukerdata brukes på en måte som gagner deres kunder?

På hvilken måte kan brukerdata brukes på en måte som gagner dere som selskap?

Hva ser du/ DNB som de største mulighetene med brukerdata fremover?

Tenker du at analyser av brukerdata vil bli enda viktigere i tiden fremover? Hvordan/hvorfor?

På hvilken måte vil du si at brukerdata påvirker forretningsgrunnlaget for DNB? (eventuelt for hele bransjen dere representerer)

Kan du si litt om motivasjonen bak det å ville tilby personlig innhold til kunder?

Prosessen:

Kan du beskrive hvordan brukerdataen samles inn, ulike plattformer?

Hva er hovedfunksjonen til brukerdataen?

Hva skjer med brukerdataen etter den er samlet inn, kan dere si noe om hvordan dere anonymiserer informasjonen?

DNB har tidligere opplyst om at dere selger statistikk basert på kundedata til både private og offentlige aktører. Kan du si noe om hvilke hensyn som tas før dataen selges? Spesielt da personvernhensyn?

Vet dere hva informasjonen dere selger blir brukt til etter den blir solgt?

Hvordan blir det en mer relevant brukeropplevelse av en nettside dersom annonsene på den nettsiden er basert på kundens personlige informasjon?

I personvernsærkleringen skriver dere at dersom man velger å ikke tillate cookies kan noen nettlesere ikke fungere optimalt, feks dnb.no-

På hvilken måte reduseres brukeropplevelsen av deres egen nettside dersom man velger å blokkere alle informasjonskapsler?

Når opptak av samtaler med kunder blir gjort, skriver dere at de «kan lyttes til eller se på annen kommunikasjon i kvalitetskontrolløyemed»-

Hva betyr kvalitetskontrolløyemed her? Blir samtalene anonymisert før de skal lyttes til, isåfall hvordan og av hvem?

DNB vil bruke personopplysninger for å oppfylle oppgavene og forpliktelsene de har tatt på seg for kunder, samt kundeadministrasjon og fakturering.

Hva er kundeadministrasjon og fakturering her spesifikt? Og på hvilken måte bidrar personopplysninger for å oppfylle oppgaver og forpliktelser?

Det står at uten samtykke kan nøytrale opplysninger om kunder brukes til markedsføring. Eksempler på nøytrale opplysninger er; navn, kontaktopplysninger, fødselsdato og hvilke produkter/tjenester man har avtale om. (DNB)

Hvordan definerer dere nøytrale opplysninger og på hvilken måte blir de brukt til markedsføring?

Personvern:

Hvordan sikrer dere anonymisering av brukerdata (i tråd med GDPR og retningslinjer fra Datatilsynet)?

Hva blir lagt mest vekt på i diskusjonene rundt brukerdata og personvern?

Hvordan har GDPR forandret måten brukerdataen blir behandlet?

Ser du/dere noen (etiske) problemer rundt å samle inn og selge brukerdata? Hvorfor/Hvorfor ikke?

Hvordan jobber dere med at dataen dere samler inn og behandler er i henhold til det den skal brukes til? Og at det ikke blir for mye eller unødvendig data som blir samlet inn?

Jf. «it should be adequate, relevant, and limited to what is necessary for the purpose ('data minimisation'). It's your company/organisation's responsibility as controller to assess how much data is needed and ensure that irrelevant data isn't collected[2]." https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

Opplever dere at dere at kundene deres er mer opptatt av spørsmål knyttet til brukerdata og personvern enn tidligere (før GDPR). [Hvis ja:] Hvordan kommer det til uttrykk? Hva lurer kundene på?

Avslutning

Er det noe du vil legge til som jeg ikke har spurt om, eller som du synes det er viktig at jeg får med meg?

Er det noen andre i DNB du tenker jeg burde snakke med?

Tusen takk for at du stilte på intervju! ☺