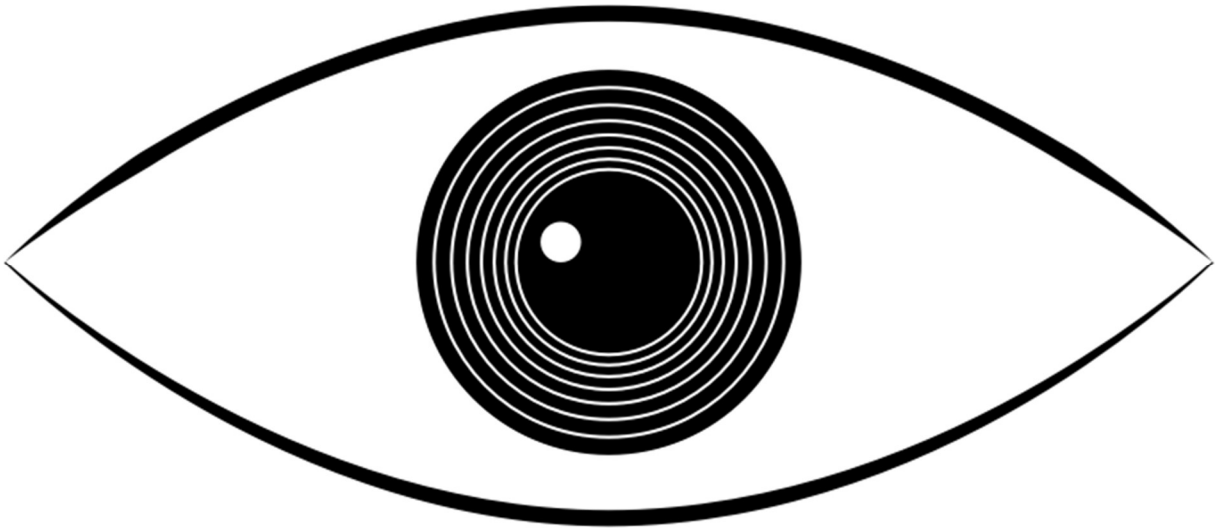
Big Brother is Watching You, Welcome in Walden Two's Brave New World



Jasmijn Boeken

S4709101

30/07/2020

Specialization Political Theory

Supervisor: Prof. Dr. M.L.J. Wissenburg

Nijmegen School of Management

Radboud University, Nijmegen, The Netherlands

Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master in Political Science (MSc)

In the vastly changing world of consumer privacy, laws that protect citizens from the data hunger of companies are of the utmost importance. While the GDPR does protect consumer privacy in a certain way, it is based on a very limited conception of privacy. This paper examines the dominant paradigm in privacy law and shows that there are other ways to conceive of privacy. This will be done by looking at three components: (1) what is privacy, (2) what is privacy behaviour, and (3) why is privacy important. I labelled the current paradigm as the liberal conception of privacy. It contends that privacy is having control over information, that privacy behaviour is determined by rational choice and that privacy is important because it is a prerequisite for autonomy. This paper shows that the meaning of privacy could also be the right to be let alone, or more broad conceptions of control over information. Furthermore, privacy behaviour is not as straightforward as the privacy calculus model makes it seem, behavioural economics and social theory provide us with different understandings of privacy behaviour. Finally, when it comes to the value of privacy, republicanism showed the importance for democracy, relationship theory indicated its role in the development of love, friendship and trust, and critical theory explained the power of surveillance and how losing privacy is losing our humanity. This study concludes that the liberal paradigm provides a very limited way of looking at privacy and consequently, current law does not accurately protect consumer privacy.

Contends

Introduction

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinised.

(Orwell 1949, 4-5)

George Orwell's prophecy in his famous book *1984* did not come to him as in a vision. Surveillance is something of all times, used in times of peace and war and against enemies and friends. Because surveillance is not a new phenomenon, laws that control it are also not new. The very first law prohibiting wiretapping was signed in California in 1862 (White 2018). Nevertheless, Orwell was right that things are changing: where surveillance was a labour-intensive process of following specific individuals in the past, it has developed into an automatic, large-scale operation at present. And with the development of new techniques for surveillance, regulations to protect citizens' privacy have also developed.

The European Union has responded to this development with the introduction of the General Data Protection Regulation (GDPR), the goal of which is to protect personal data in the possession of private companies (GDPR 2016). The text itself states that the right to privacy is not an absolute right, since the gathering and use of personal data has positive impacts on society. Therefore, the right to privacy must be balanced, so that other fundamental rights will not be weakened. According to Julie Cohen (2012), privacy is always on the losing side of this balancing game. Time and again subjects like national security, innovation and efficiency are (mis)used to act as a counter for privacy rights. The statement that data collection is good for humankind (GDPR 2016) might sometimes look evident. Netflix knows what we like to watch when we log in at a certain time, Facebook knows when a women is having her period and wants to spend more money on shopping (Rajagopalan 2019), and Google knows what information I am looking for. In these ways data gathering creates profit and saves us a lot of time. It shows us what we want to see because our personal data is freely available. But although it might seem evident that these are good things, there are also multiple downsides to all of this; including the loss of privacy.

Looking further into what has been written about the GDPR, we can see that it has had its share of critics. Edward Snowden proposed that the law was looking in the wrong direction: while its focus is on data protection, it should have been on data collection (Swant 2019). One of the main points of criticism is that it is mainly focused on a "notice and consent" system. Notice and consent policies follow two logics. First, they see privacy as having control over information, second, they use the logic of the free market, where to make a free and rational purchase, you need full information (Nissenbaum 2011). As will become apparent throughout this paper, the notice and consent system comes with its very own view on the different aspects of privacy. It sees privacy as having control over information and believe that people can calculate their costs and benefits in deciding whether to provide information. Furthermore, it assumes that the value of privacy lies in the fact that it protects autonomy. This is what I will call the liberal paradigm of privacy.

While criticism on the GDPR is available in abundance, useful suggestions are scarcer. This might be because the question why privacy is important often stays unanswered, according to Cohen (2012), this is even the case with privacy activists. Jeffrey Reiman (2017) argues that if we want to make legislation about privacy, we first need to find a grounded answer to the question why privacy is important. However, I want to argue that the GDPR *is* based on a particular view on privacy: a liberal view. This liberal paradigm is most evident in the notice and consent rules that are dominant in the GDPR and constitute a kind of privacy self-management. They come with a view of what privacy is, how people respond to it and why it is important. The goal of this paper is to show that current privacy law is indeed based on this liberal perspective, and to seek alternative views. The research question that needs to be answered is: what are the alternative views on privacy, and what would be the consequence for law when these views would be employed? The societal relevance lies in the fact that with an answer to this question, new privacy laws could be suggested. These laws would be better able to protect consumer privacy.

Due to the very diffused academic field of privacy the answer is not that easy to find. Drawing from Deleuze and Foucault (1977), I will not try to find one theory that fits my argument and defend that theory. I will use bits and pieces from different theories to show that there are more conceptions of the meaning and value of privacy than the liberal paradigm. The scientific relevance of this paper is threefold. First, it creates order in the diffused debate about privacy, by categorizing the different theories. Second, it takes a different perspective, looking at the intrusion of privacy by companies instead of the government. Posner (1979) contends that those who argue in favour of restricting measures for business who use personal information of individuals are often confusing the issues of privacy with regard to the state with issues of privacy when it comes to private companies. This paper will show why it is important to protect consumer's privacy against invasions by private companies. Third, the paper will be interdisciplinary, bringing together political theory, sociology and psychology. Combining these three points, this study will fill a gap of knowledge in the field of privacy research:

previous studies have mainly focused on intrusions of privacy by the government and have not considered what the other disciplines can add to our understanding of privacy. Furthermore, this paper uses the theories of some of the great names of political theory; Aristotle, Hannah Arendt and Michel Foucault in a field where they, unfortunately, have not been used as much as they should have.

The overall structure of this paper takes the form of three chapters. The first chapter will discuss the different conceptions of privacy. The meaning of privacy varies across academic disciplines, in everyday live and in law (Margulis 1977). It will show that the basic "control over information" conception is the one that is currently dominant in law and fits the liberal paradigm. To show other possibilities, more extended versions of this conception of privacy will be discussed, as well as the reductionist approach and the conception of privacy as the right to be let alone. The second chapter will discuss the so called "privacy paradox". With the implementation of the GDPR, private companies had to change their privacy policies. Our mailboxes were flooded with emails about those changed policies, sometimes from sites we did not even remember we were a member of. But one could wonder how many people read those emails. This is part of the "privacy paradox". Where one claims to care about their privacy, but when an effort is needed to protect it, they tend to look the other way (Hull 2015; Bandara and Levine 2019). What we can see when discussing the different possible explanations of the privacy paradox is that the liberal paradigm fully relies on the calculus model, while behavioural economics and social theories suggest that this model does not sufficiently explain the privacy paradox. In concluding this chapter, some novel theories will also be discussed because this is a field of research that is still developing.

In the third and final chapter the different conceptions of the value of privacy will be discussed. Starting with the liberal conception, the one present in current privacy law, which argues that privacy is important for autonomy. Republican theory refutes the liberal view of privacy as an individual value and argues that privacy is a common value that is necessary for democracy. Borrowed from the field of sociology, we will then turn to a relationship theory about privacy, which argues that privacy is important for friendship, love, and trust. The final conception of the value of privacy comes from critical theory and contemplates that with the changes in privacy we are living in a society that is characterised by surveillance capitalism, where inequalities are becoming larger at a fast pace. The conclusion will look back at the previous chapters and suggests the effects that these different accounts of the meaning, inner working, and value of privacy will have on future privacy law.

Chapter 1: A conception of privacy

Alan Westin (1967) observed that it is remarkable that a concept as important as privacy has been so poorly theorized. In this chapter, different conceptions of privacy will be discussed and evaluated on the criteria as specified below. We need to delve into the different conceptions of privacy to answer our question what it means to have privacy. As will become clear, the second conception of privacy that is discussed in this chapter, privacy as control over information, is currently dominant in privacy law and belongs to the liberal paradigm. Before looking at the different conceptions of privacy I will first quickly discuss some of its history and define the criteria that this conception must meet.

Richard Posner (1979), drawing on information from the Oxford English Dictionary, describes the original meaning of the word "private" as the actions that were outside of the scope of government. Privacy was therefore not seen as something good: the people who had privacy in their village were often the pariahs of society. The concept slowly lost its negative connotation and in the 17th century evolved to be understood as excluding oneself from public life, in other words; seclusion. With his emphasis on history, Posner (1979) notes that the individual has also gained a lot of privacy over the last centuries. Rising urbanization has given us the opportunity to escape from village live, which was known for its gossip. While acknowledging this increase of privacy due to urbanization, we must also acknowledge the loss of privacy due to technological advancement as described by Warren and Brandeis (1890). The concept of privacy is therefore context depended, changing over time, and imbedded in culture. A true conception of privacy does not exist, and this paper will surely not suggest one. It is interesting, however, to look at the currently dominant conception and see what else is out there. Furthermore, besides being interesting, this will provide us with great insights on how to improve privacy law.

In 1972, in United States v. Whites, the Supreme Court of the United States ruled that during a conversation with another person, be it physical or on the phone, one could expect their words to be recorded, and therefore, there is no reasonable expectation of privacy during conversations (Parker 1973). This ruling inspired Parker to ask the question what privacy is: a psychological condition, control over your information, a form of power, or some kind of freedom? According to Parker, a definition of privacy must meet three criteria. First, it must fit the data, not being too broad or to narrow. Or, as we will see below, with the definition of Warren and Brandeis (1890), both. The second condition that must be met is the condition of simplicity (Parker 1973). Parker suggests that a list would be the simplest explanation of privacy. I question this and propose that a compact definition would be simpler to use. The third condition is that it must be applicable in the courtroom (Parker 1973). This also means that it must be applicable for policy makers: if they have a clear definition of privacy, they will be better able to protect citizens' right to privacy. Massing this together, we need a

fitting, simple and useful definition of privacy. Ruth Gavison (1980) argues that the concept of privacy should be value neutral, because otherwise it would be too difficult to identify a loss of privacy. I agree that neutrality is important in the defining of a concept, but I also want to emphasize here that neutrality is impossible. The fourth condition that a conception of privacy should meet is therefore; to endeavour neutrality.

To bring some order into the chaos of definitions concerning privacy, I have divided them into three broad categories: (1) the reductionist approach, (2) controlling assess to personal information, and (3) the right to be let alone. The second approach that will be discussed is the one that fits within the liberal paradigm. The other two approaches will show that there are different ways of looking at the concept of privacy. Solove (2002) identifies two other conceptions of privacy: personhood and intimacy. The personhood approach stipulates that privacy protects us against assaults to personal dignity (Solove 2002). The intimacy approach argues that privacy is important for personal relationships. I will not include these conceptions in the argument made below, because they do not meet the conditions as ascribed above, especially the condition of neutrality. Furthermore, these conceptions do not adequately answer the question what privacy is, and are more focused on why privacy is important, which will be discussed in the third chapter.

Reductionist approach

This section of the paper will discuss the reductionist approach to privacy. The work of Daniel Solove, Judith Thompson and Richard Posner will be discussed, before moving to the most important points of critique. What is central to the reductionist approach, is that the authors argue that we do not need new laws to protect privacy because it is already sufficiently protected in the common law. They all argue this, however, in their own distinct ways.

Daniel Solove (2002), a significantly original and influential author in the field of privacy, argues that we should not try to find an overarching concept of privacy. He defends a pragmatist point of view, where he tries to understand privacy by focussing on the context, instead of looking for a definition. He uses Wittgenstein's argument of "family resemblances" to explain that we do not need the classical approach of necessary and sufficient conditions (Solove 2002). The concept of privacy does not have to be bound together by one distinguishing feature but can be defined by a couple of overlapping elements. Consequently, a definition does not need fixed boundaries; these can be fluid. Even though Solove may be the odd duck in the current literature about privacy, previous authors have used similar arguments. Judith Thompson (1975) and Richard Posner (1979), have, both in their own way, argued

that we do not need new laws to protect our privacy, because it is already protected in the common law.

Thompson is an important critic of the conception of privacy as the right to be let alone, which will be further discussed below (1975). She asks the question "where is this to end? Is every violation of a right a violation of the right to privacy?" (Thompson 1975, 295). She argues that when a right to privacy seems to have been violated, some other rights have been violated as well. For example, when security agencies spy on a married couple having a quiet fight inside their home, their right to privacy has not been violated, but their "right not to be listened to, which is one of the rights included in the right over the person" (Thompson 1975, 305), has been violated. Thompson argues that the right to privacy is not a distinct right, but a cluster of all different kinds of rights. This cluster is not distinct enough to be its own right because it intersects with other clusters of rights. According to Thompson, the right to privacy can only be violated when another right is also violated. Just asking a person for information is not a violation of their right to privacy, torturing them to get this information, however, is. But only because the right not to be harmed is also violated (Thompson 1975). Because you have the right not to be harmed and not to be looked at, you have a right to privacy. The right to privacy never exists in itself, and is therefore derivative: "it is possible to explain in the case of each right in the cluster how come we have it without ever once mentioning the right to privacy." (Thompson 1975, 313).

According to his economic analysis of privacy, Richard Posner contends, just like Thompson, that the common law is sufficient to protect the amount of privacy society needs (1979). When we take his economic point of view, we can see that there is on the one side a demand for privacy, and on the other side a demand for prying or surveillance, and that one can only grow at the expense of the other. To some extent, privacy can be useful for innovation. But according to Posner, further protection will not be fruitful: "at some point, reached long ago, further increases in the amount of personal privacy no longer increased significantly the incentive to innovate but did, of course, continue to increase the ability of people to conceal their activities for manipulative purposes." (Posner 1979, 27).

According to Posner (1979), there are four types of privacy: concealment, seclusion, innovation, and conversation. These types of privacy are all interrelated. Concealment is an important economic tool to protect the creative ideas of individuals (Posner 1979). Being able to have concealment often requires seclusion, to be alone. In this way, seclusion and concealment are necessary in a society that wants to stimulate innovation. Information asymmetry is known as an important flaw of the free market and more privacy would only increase this flaw and thereby lower profit (Posner 1979). For a business to innovate, it is also important that certain conversations are private. Having a good reputation as a person or a business is especially important for economic transactions, because one will be able to get better deals and thereby contribute to society. Additionally, it reduces information costs, because it is

no longer necessary to gather a lot of information about the other person (Posner 1979). Privacy will only be used for malicious practices; to hide some facts about yourself that might damage your good reputation: "[w]hat people want more of today when they decry lack of privacy is mainly something quite different: they want more concealment of information about themselves that others might use to their disadvantage." (Posner 1979, 5).

According to Posner we could therefore see privacy as manipulation. However, he does make some important notes to this interpretation. Sometimes, the concealment of information is needed for the distribution of accurate information. For example, my personal, ill informed, thoughts about the COVID-19 virus will only confuse people and should therefore stay concealed. A second note Posner makes to the conception of privacy as manipulation is that sometimes concealment is necessary to protect yourself, he uses the example of a rich man that conceals his income to avoid kidnapping (Posner 1979). As a third point he notes that people may sometimes conceal facts about themselves for unknown reasons, these facts would not hurt their transactions and economic status and are therefore irrational (Posner 1979). He does not elaborate on this point, and I think this reveals a weak spot in his theory: people attach a value to privacy that cannot be rationally explained with purely economic arguments. His final remark is that sometimes, there can be too much information in a sense that it is no longer efficient and that therefore, concealment can be a good thing (Posner 1979). But these points aside, Posner argues that privacy facilitates manipulation, and in the way that it is important, is already protected in common law and therefore does not require any additional protection. He thereby resists the movement where individuals gain privacy and business and government lose privacy, because according to him, the privacy of an individual has no social purpose whereas the concealment of information of businesses has (Posner 1979).

Ruth Gavison (1980) criticizes this reductionist approach to privacy. As we have seen above, privacy is often dismissed because whenever there is a loss of privacy, there is also a loss of another fundamental right, like freedom. According to Gavison, however, this does not mean that a loss of privacy is not important in itself, and this importance should be recognised. The plead made by the reductionist theorists leaves the doors wide open to dismiss any claim of a right to privacy. It also seems to miss the point of neutrality, because as Fried (1978) notes, this work is inspired by scholars like Friedrich Hayek and Robert Nozick who maintain a hierarchy of rights where privacy is less important than other rights. Furthermore, I think that Posner's third argument, that there are some economically unexplainable reasons why people care about their privacy, is an important point of criticism on his own theory. Not everything can be explained by rational economic reasoning, especially not something as emotional as the concept of privacy (Laufer and Wolfe 1977). This will be further discussed in the chapter about the privacy paradox.

The reductionist approach to privacy has provided us with the contention that privacy is already sufficiently protected in common law and therefore does not need to be protected in itself. This conception of privacy is difficult to assess with the criteria that a conception must be: (1) fitting, (2) simple, (3), applicable, and (4) endeavour neutrality. It is, furthermore, impossible to apply these criteria to the reductionist conception of privacy, because it argues that we do not need one. The most important flaw of this approach is that it is not value neutral and adopts a clear hierarchy of rights.

Control over information

Where the reductionist approach argued that we do not need a conception of privacy because privacy is already protected in common law, in this section we will come across authors like Alan Westin (1967), who sees privacy as having control over information and argues that, especially in times where technological development is making it easier to collect information about people, the law should protect our privacy. Besides Alan Westin; Helen Nissenbaum, Robert Parker and Stephen Margulis also provide various arguments in favour of this conception of privacy. As announced in the introduction, this is the dominant view in current privacy law, which fits the liberal paradigm. After the approaches of the above mentioned authors are clarified, I will turn to Gavison and Solove for points of criticism to this approach.

Westin (1967) observed a decrease in privacy because the costs of surveillance become lower due to technological advancements, and people are getting increasingly more curious about others. Westin describes privacy as "the claim of an individual to determine what information about himself or herself should be known to others" (2003, 3). He later adds that this claim also applies to organizations and institutions. Just like "being let alone", "having control over one's information", is a conception that is widely shared by citizens according to the research of Laufer and Wolfe (1977). This definition does not only include things like wiretapping, but also, for example, personality tests, and thereby protects the privacy of inner thoughts (Westin 1967). The notice and consent paradigm is based on this very basic idea of having control over your information. In every step, the consumer gets the option to agree with the privacy policies or not, and is therefore able to exercise control.

Nissenbaum's (2004) explanation of privacy as contextual integrity relates to this view of privacy as controlling information. When Nissenbaum talks about contexts, she means structures and social settings that can change over time, like school, friends and hospitals. Some of these contexts have strictly defined roles, actions, norms and values; a voting booth for example. But there are also situations where this is not the case; like at a public market (Nissenbaum 2010). Her theory is inspired by Walzer and his spheres of justice. While it might be just to provide your doctor with your medical

history, when this information is taken outside of the medical sphere and provided to your boss in the sphere of labour this is no longer just. Nissenbaum emphasizes the importance of two kinds of norms: norms of appropriateness and norms of flow. Norms of appropriateness guide us in the question which information is appropriate to share in each given situation. For example, we would deem it as wildly inappropriate to share details about your personal life with a stranger on the streets, while this is very appropriate to share this with the people you see as your friends. The norms of flow, in turn, show us how this shared information should be treated. It would be inappropriate if a friend whom I told about my personal life would share this with their friends whom I do not know. A worry that immediately comes to mind with this theory is that it only considers established norms, which makes it a defence of the status quo. Nissenbaum is also concerned with this point but argues that it does not have to be such a big problem.

Another author who argues in favour of the control of information conception of privacy is Robert Parker. He defines privacy as: control over when and by whom the various parts of us can be sensed by others. By "sensed" Parker means: "seen, heard, touched, smelled, or tasted" (Parker 1973, 281). This definition does not, however, account for the disclosure of personal information, one's thoughts, and psychological state of mind. With this definition, Facebook using your "likes" to make psychological assessments is not a loss of privacy. While it could be argued that this is not a violation of a privacy right, it is a loss of privacy, because in this example Facebook gets to know new information about you. I would argue, therefore, that with the technologies of today, this definition is too narrow, and does not fit the data. The final author who will be discussed here is Stephen Margulis, who defines privacy as follows: "[p]rivacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (Margulis 1977, 10). In later work he adds that privacy is regulating who gets access to the self (Margulis 2003). He thereby includes the psychological state of mind, which was missing in the definition of Parker. Although all these author's definitions are different in the details, the focus is on having control over your personal information.

Ruth Gavison (1980) is a fierce critic of the overall perception of privacy as control. This line of argumentation, she contends, would suggest that if you voluntarily hand over information to someone, you do not experience a loss of privacy, because there is no loss of control. According to Gavison (1980), this is not the case: one does lose privacy even when having full control in giving it away, but this loss does not need to be considered as a violation of a right to privacy. When the proponents of privacy as control use a strong definition of control, however, they could argue that there is still a loss of control when you voluntarily give information away, because you do not know what the other person will do with it: they could sell it to third parties or accidentally lose it. Gavison (1980) refutes this argument by saying that in this case of a strong conception of control, what is considered a loss of privacy could just be a suspicion of this loss. Solove (2002) provides another point of criticism; he

questions whether control over information is possible when this information is relational. This problem does not only occur in personal face to face contact but is also an issue when using the internet. Because you are making use of a website, and there is some type of relationship there (Solove 2002).

The authors of the control over information approach has shown us that, in adverse to the reductionist approach, a definition of privacy is possible. While not trying to downplay the differences, all the proponents of this approach identify a loss of privacy as a loss of control, which is the basis of current privacy law. This is also where the main point of criticism comes in: one also loses privacy when voluntarily sharing information (Gavison 1980). When looking at our four criteria that a definition of privacy should have ((1) fitting, (2) simple, (3), applicable, and (4) endeavour neutrality), it seems that the main problem with this approach is that it does not fit the data.

The right to be let alone

The third and final conception of privacy that will be discussed here is privacy as "the right to be let alone". The right to be let alone has its foundations in legal definitions of privacy in the United States (Joinson and Paine 2007). It is also one of the answers most people give when asked what privacy means to them (Laufer and Wolfe 1977). This part will start out with two of the most important authors in the field of privacy: Samuel Warren and Louis Brandeis. After delving into their theory and looking at points of criticism, the conception of privacy by Gavison will be discussed. We have seen Gavison in different parts of this chapter, providing comments to the other approaches and now it is time to perceive the alternative that she proposes.

Warren and Brandeis (1890) were one of the first authors to define privacy as the right to be let alone. Their work is now described as "the foundation of privacy law in the United States" (Solove 2002, 1100) and was also highly influential in the academic world. In their article, Warren and Brandeis (1890) explain how the right to privacy is already present in a lot of existing rights in American law; like the right not to be a victim of bodily harm. But contrary to the authors of the reductionist approach, they do not agree that the protection of privacy in the common law is enough. They show that due to technological developments, we need a more comprehensive right to privacy, to protect citizens against, for example, emotional harm.

The conceptualization of privacy as "the right to be let alone" has stumbled upon a lot of criticism, ranging from it being too narrow to being too broad. Thompson (1975) argues that it is not broad enough because it does not recognize for example people spying on you, or recording your conversations, as those things are possible without someone being aware of it, and therefore the person

is not being bothered. Anita Allen (1988) takes the other side and claims that the definition is too broad, because it includes almost everything. Stepping on someone's toe would be an invasion of the person's privacy as well as secretly taking pictures of their toe. This feels counter intuitive, because we recognize stepping on someone's toe as bodily harm, not as an invasion of privacy. A final important critic is Gavison (1980), who rightfully noticed that the right to be let alone is often seen as a negative right, where the state is not allowed to spy on their citizens. But the right to privacy should also be a positive right, a duty for the state to protect its citizens from intrusion by other citizens or companies.

Gavison (1980) suggests a conception of privacy as limited access. She argues that a concept of privacy must tell us when there is a situation of a loss of privacy. Therefore, the concept must be neutral. Only after this neutral conception of privacy is established, will we be able to understand what the value of privacy is. Once you know what a loss of privacy means, you can start grasping which losses of privacy are important. Gavison (1980) argues that there are three elements which we need to consider when we talk about a loss of privacy: secrecy, anonymity, and access. Secrecy refers to the information that is known about a person, whether this information is false or true, it constitutes a loss of privacy. Another way to lose privacy is when you are no longer anonymous, in other words, when someone pays attention to you. It is not required that the person paying attention to you gets information from observing you, it is the mere practice of giving attention that constitutes the loss of privacy. When one loses privacy because a person has access to you, this means physical proximity, like a stranger sitting next to you on a bench in the park while there are more than enough empty benches (Gavison 1980). These three elements can of course be combined: when someone sits next to you on the bench, he might discover that you like to eat a tuna salad sandwich. But they can also work separate.

> *Our interest in privacy, I argue, is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. This concept of privacy as a concern for limited accessibility enables us to identify when losses of privacy occur.* (Gavison 1980, 423).

Solove (2002) criticizes this definition of privacy because it lacks a distinction between which information is private and which is not. I, however, disagree with this point, and would argue in line with Gavison (1980) that every kind of information, when shared, constitutes a loss of privacy. Whether or not this is undesirable does depend on the type of information that is shared.

The conception of privacy as the right to be let alone takes many forms. Where the most basic one as offered by Warren and Brandeis might be both too broad and too narrow, Gavison gives the conception of privacy as being let alone more body. Her definition could be criticized for being too

broad, but I think it is rightfully so, because losses of privacy are everywhere. The real question is which ones are harmful and which are not. Gavison's conception is simple and useful and seems to withhold from giving a normative evaluation.

The different conceptions of privacy

What we can learn from this chapter is that privacy is a contested concept, and that the perfect conception of privacy does not exist. The first approach contends that we do not need a distinct conception of privacy, the second approach argued that privacy is having control over your information, and the third approach holds that privacy is being let alone. All three approaches highlight vastly different aspects of privacy. We cannot ignore Thompson's (1975) argument that when privacy is violated, there are often other rights also being violated. Neither do I want to dispute Westin's (1967) claim that having control plays an important role in the right to privacy. But by only using the conception of privacy as having control over information in the GDPR, a lot of different aspects of privacy are being ignored. The limited accessibility conception of privacy by Gavison (1980) conquers the most important points of criticism of the other two conceptions of privacy. Unlike the conception of privacy as control over information, Gavison's theory clearly shows when privacy is lost, and in contrast with the reductionist approach to privacy it does not create a hierarchy of rights and in that way attempts to be as neutral as possible.

Using Gavison's theory to improve privacy law, however, requires us to first answer the question when a loss of privacy is a problem and when it is not. This normative value of privacy will be discussed in the third chapter. This paper will now turn to an analysis of privacy behaviour; by seeking explanations for the "privacy paradox".

Chapter 2. The Privacy Paradox

In the previous chapter we have seen that there is no easy answer to the question what it means to have privacy. Before we can deal with the question why privacy is important, we need to discuss the allegation that privacy is not important because people would sell it for a BigMac (Carrascal et al. 2013). This chapter will elaborate on the "privacy paradox", which is, in short: the difference between privacy attitudes and actual privacy behaviour (Acquisi and Gross 2006). It is important to find ways in which the privacy paradox can be solved, because, as Spyros Kokolakis (2017) argues, government policy to protect privacy is often justified on the grounds that citizens find this important, but when citizens do not behave like this, this weakens the justification. Furthermore, it is not only important to solve it, it is also essential to understand the mechanism behind it: according to Patricia Norberg and Daniel Horne (2007), we need to understand the nature and cause of the privacy paradox in order to develop appropriate privacy policies.

This chapter will start by explaining what the privacy paradox is and will show some of the studies that proofs its existence. It will, however, also cover some of the limitations of this research to provide a complete picture. We will then turn to the possible explanations of the privacy paradox: (1) the calculus approach, (2) behavioural economics, (3) social theories, and (4) novel theories. These theories explain how people deal with their privacy, and therefore, how this must be legislated. The current notice and consent paradigm holds onto the calculus approach, but as will become apparent, this approach has some important limitations. While the previous chapter has shown that there are limitations to the conception of privacy as having control over information, this chapter will use this conception of privacy. Simply because this conception is not only dominant in law, but also in academics, and is used in most of the privacy paradox literature.

What is the Privacy Paradox

This section will discuss the privacy paradox in depth. It will start with the definition of the privacy paradox, where it is important to acknowledge the difference between the theories from Allesandro Acquisti (2004) and Susan Barnes (2006). It will then turn to look at some of the evidence in favour of the privacy paradox and discuss a couple of them providing an overview of the different context of these studies. I will then turn to some studies that suggest that the privacy paradox does not exist and will look at some points of criticism to privacy paradox literature.

Even though Acquisti (2004) did not use the term "privacy paradox" he was one of the first authors to note the importance of the dichotomy between privacy attitudes and behaviour. Barnes (2006) was the

first author to use the term “privacy paradox”, however, the way Barnes described it is different from how it is used now: “[h]erein lies the privacy paradox. Adults are concerned about invasion of privacy, while teens freely give up personal information. This occurs because often teens are not aware of the public nature of the internet” (Barnes 2006, 4). Adults are concerned about invasion of privacy, while teens freely give up personal information. It could therefore be confusing to, as some authors do, refer to Barnes as the person who invented the privacy paradox, while using the operationalization of Acquisti (Dienlin and Trepte 2015; Taddicken 2014). In this paper the definition of Kokolakis will be used, he describes the “privacy paradox” as a: “dichotomy of information privacy attitude and actual behaviour” (2017, 122). Most of the other definitions are alike, and studies that explain the privacy paradox use these definitions as well.

There has been a lot of research that shows the existence of the privacy paradox (Acquisti and Grossklags 2005; Barnes 2006; Barth et al. 2019; Beresford, Kübler and Preibusch 2012; Carrascal et al. 2013; Egelman, Felt and Wagner 2013; Hann, Hui and Lee 2007; Huberman, Adar and Fine 2005; Lee, Park and Kim 2013; Norberg, Horne and Horne 2007; Spiekermann, Grossklags and Berendt 2001; Taddicken 2014; Tufekci 2008; Zafeiropoulo et al. 2013). These studies all use different operationalizations, methods, and conduct their research on different platforms. They research the privacy paradox in online shopping (Spiekermann, Grossklags and Berendt 2001), on social media websites (Acquisiti and Gross 2006), with location data (Zafeiropoulo et al. 2013), and for mobile phones (Barth et al. 2019).

While the evidence in favour of the privacy paradox seems overwhelming, Kokolakis (2017) also provides us with an overview of research that shows that the paradox does not exist. However, when looking at these studies in more detail, they are often more nuanced about the issue. For example, the research by Grant Blank, Gillian Bolsover and Elizabeth Dubois (2014), does not show that the privacy paradox as described by Kokolakis (2017) does not exist, but uses the definition by Barnes (2006), where young people are less concerned about their privacy than old people are. They, therefore, do not provide proof that the privacy paradox, as defined above, does not exist. Furthermore, while in their research about the privacy paradox in Switzerland, Christoph Lutz and Pepe Strathoff (2014) do not find the classical paradox, they do find it when only looking at location data, a highly privacy sensitive sort of data (Lutz and Strathoff 2014). While the evidence is not unambiguous, most studies show that the dichotomy between privacy intentions and privacy behaviour exists within varying contexts. In the next sections of this chapter, some of the possible explanations of this paradox will be elucidated, starting with the privacy calculus approach.

Privacy Calculus

We will now turn to one of the ways in which the privacy paradox can be explained: the calculus approach. As will become apparent once this theory is explained, the calculus approach is dominant in current privacy law and is most visible within the notice and consent rules. I will start by introducing the calculus approach in is most basic form, as described by Robert Laufer and Maxine Wolfe (1977), and by Mary Culnan and Pamela Armstrong (1999). When their argument is clear, we will then turn to some more extended versions of the privacy calculus approach and discuss some examples of how the value of privacy is calculated. I will conclude this section by discussing some points of criticism to this approach.

Laufer and Wolfe use their "calculus of behaviour" theory to explain the choices made in revealing personal information: "[s]imply stated, in many instances the individual has to ask himself/herself: If I am seen engaging in this behavior or that behavior or am seen with this person or that person, what are the consequences for me in the future, in new situations, and so on?" (Laufer and Wolfe 1977, 36). Culnan and Armstrong explicate what this calculus approach would look like in the case of privacy: "individuals are willing to disclose personal information in exchange for some economic or social benefit" (Culnan and Armstrong 1999, 106). They argue that organizations must see the collection of personal information as a social contract, where there is not only an exchange of money and goods, but also an exchange of personal information and customer service. When the customers see the costs of this social contract exceed the benefits, they will end the social contract (Culnan and Armstrong 1999). This is the perspective on privacy behaviour that is reflected in the liberal paradigm.

With their mixed-method study about disclosing personal information on social networking sites, Haein Lee, Hyejin Park, and Jinwoo Kim concluded that: "the intention to share context information is influenced by expected benefit and expected risk simultaneously. Especially the effect of expected benefit is larger than that of expected risk" (Lee, Park and Kim 2013, 873). The most frequently stated benefit of sharing personal information on social networking sites is that of relationship development (Lee, Park and Kim 2013). Other benefits are: social control, social validation, self-presentation and self-identification (Lee, Park and Kim 2013). But there are also potential risks. Lee, Park and Kim (2013) identified the security risk as most critical, but we must also consider the relational risk. In their extended privacy calculus model, Tamara Dinev and Paul Hart (2006) argue that there might be contrary believes, that are all equally valid, but of which one might be stronger than the other. They found evidence for this hypothesis when studying the factors that influence the willingness to provide personal information over the internet (Dinev and Hart 2006).

The different privacy calculus theories have multiple things in common, the most important one is that they believe that you can calculate the worth of privacy, or certain pieces of information. In their

experimental research about the willingness to pay for privacy, Alastair Beresford, Dorothea Kübler and Sören Preibusch (2012) provided respondents with the choice to either buy something in a store that explicitly asked for their day of birth and income, or to buy in a store that only asked for year of birth and favourite colour. They found that in the situation that the price was equal, the division of respondents over the two stores was close to equal. And when the store who requested the more sensitive personal information about income, had a one-euro discount, 39 out of 42 respondents selected that store. This could indicate that the respondents do not care about their privacy, however, in a questionnaire that was answered after the experiment, 95% of them indicated an interest into protecting their personal information (Beresford, Kübler and Preibusch 2012). The calculation approach would thus argue that the monetary benefits were valued higher than the loss of privacy.

The calculus approach has, however, not gone without their share of criticism. Acquisti and Grossklags (2007), provide us with some difficulties where the classical rational choice theory can't account for: (1) information asymmetry, (2) the inability to calculate the effects, and (3) behavioural anomalies and biases. The first point, information asymmetry, has a double roll in the privacy issue. On the one hand, the consumer has some information that the company does not have but wants to have. On the other hand, the consumer does not know what the company might do with this information once provided to them (Acquisti and Grossklags 2007). When it comes to the second point, the inability to calculate effects, we have on the one hand the argument that it is impossible to calculate the risk of disclosing information (Lutz and Strathoff 2014). On the other hand, we have the argument by Acquisti and Grossklags (2007), that we should not even speak of "risk" when talking about privacy, because risk implies that we know what is at stake. However, when we give away personal information, we do not know what will happen with it, the control is out of your hands once you have provided it. Furthermore, technological development makes it even harder to assess what will happen with this information in the future (Acquisti and Grossklags 2007). The third point, behavioural anomalies and biases will be discussed in the next section of this chapter.

The privacy calculus approach is currently the dominant mode in privacy paradox literature. Therefore, their share of criticism is also bigger than with the other approaches that will be discussed. As we have seen, this approach argues that the privacy paradox can be explained by considering that people make a calculation. In this calculation, not only their privacy attitude plays a role, but other costs and benefits are also considered. The calculus approach is part of the currently dominant liberal paradigm within privacy law. Privacy self-management with its notice and consent rules relies on the assumption that individuals can make a calculation where they consider both the benefits and the costs of sharing personal information. In the next part of this chapter we will see how behavioural economics argues that this calculation is impossible.

Behavioural Economics

The calculus approach as described above is part of the currently dominant liberal view on privacy. As we have seen in the previous part, one of the points of criticism to the calculus approach comes from theories that highlight the existence of behavioural anomalies and biases. While it is often suggested by policy makers that consumers should have more information so they can make a rational decision about their privacy, this might not actually help them (Acquisti and Grossklags 2007). Even in the case of complete information, psychological processes will influence behaviour. We will start out with the research by Norberg and Horne (2007) about the way attitudes develop. Taking it one step further into the decision-making process, we will look at how biases influence this decision (Kokolakis 2017; Acquisti and Grossklags 2007). This section will be concluded by, with the help of attribution theory, looking at how the perceived outcome of a decision influences future behaviour (Norberg and Horne 2007).

In their research about exchanges of personal information for commercial benefits, Norberg and Horne (2007) explicate the way in which attitudes develop: "attitudes range from non-attitudes through weakly held attitudes to those that are strongly held" (Norberg and Horne 2007, 832). The strongly held attitudes have higher predictive power of behaviour than the others do. The creation of these attitudes is affected in multiple ways. First, they depend on the way information is provided: personal experiences are of more influence than information that is provided by others. Additionally, negative information affects attitude creation more than neutral or positive information. A side note, however, is that while negative experiences may have a larger impact on attitudes, people could be more focused on the positive because they are nudged this way by marketing strategies and because the negative outcomes are in the future and the positive outcomes are directly visible. Finally, we need to see how relevant the attitude is to the specific context of a loss of privacy, a person needs to consider the attitude as generalizable for the specific situation (Norberg and Horne 2007).

The development of attitudes is not as straightforward as the calculus theory might make it seem. When looking at the next step in the decision-making process, there are even more psychological processes to consider. Cognitive bias theory has shown that there are multiple biases that affect decision making (Kokolakis 2017; Acquisti and Grossklags 2007). Taking the ones highlighted by Acquisti and Grossklags (2007) and Kokolakis (2017) together, there are nine. Firstly, the optimism bias; thinking the risk of online privacy are not that big. Secondly, the overconfidence bias, where people are too optimistic about their own skills and knowledge. Thirdly, the affect bias, which shows us that people use shortcuts to make fast decisions, and in doing this they overestimate the benefits and underestimate the risks. Fourthly, hyperbolic discounting, makes people value present benefits higher than future benefits (Kokolakis 2017). Fifthly, the valence affect makes us believe that it is more likely

that favourable events will happen. Sixthly, rational ignorance is in place when the costs of learning new information are higher than the benefits of using this information in our decision making. In their calculations of the costs of reading privacy policies, Aleecia McDonald and Lorrie Faith Cranor (2008) found that it would take a US citizen 201 hours a year, and the total loss for the US economy would be 781 billion dollar. Seventhly, the status quo bias makes us prefer things to stay the way they are. Eighthly, our tendency to fairness makes us do things if we believe these are fair. Ninthly, inquiry aversion makes us turn down a good offer because someone is getting a better offer (Acquisti and Grossklags 2007).

As we have seen above, both the creation of attitudes and the process of decision-making are influenced by psychological processes. Taking it one step further, the attribution theory looks at how the outcome influences future decision-making (Norberg and Horne 2007). Attribution is a process in which a person determines the causes of a specific outcome and assesses the impact on future behaviour. There are three factors that influence the way someone looks at an outcome: (1) locus; who is responsible for the outcome, (2) control; is control possible or not, and (3) stability; will this situation recur (Norberg and Horne, 2007). So in a situation where the person is responsible for the outcome, is able to have control, the context of the next situation is similar and the experience was negative, it is likely that the person will change their behaviour (Norberg and Horne 2007). But this seemingly simple process might be disturbed by certain attribution biases. One of those biases is that when value is uncertain, people are likely to engage in goal-based behaviour, where the gains are perceived as larger than the losses (Norberg and Horne 2007). Adding to this process is that people are not always the best judges and may make mistakes in their assessments.

As behavioural economics showed, the weighing of costs and benefits, as proposed in the privacy calculus theory and integrated in the GDPR, is not as unequivocal as it seemed. There are multiple psychological mechanisms that influence this process, making it seem highly unlikely that a person could make the rational calculus in the case of privacy. These mechanisms also explain the privacy paradox, since the connection between privacy attitudes and privacy behaviour is not as straight forward as previous research has made it seem in their models. However, there is still a lot of research that needs to be done to see if, when including the biases in the model, the privacy paradox can be solved. In the next part we will look at yet another possible explanations of the privacy paradox: social theory.

Social Theory

While, as we have seen above, there has been a lot of research about the privacy paradox, what is missing in the literature is the social context of the usage of social media (Taddicken 2014). Distributing personal information, or in other words, self-disclosure, is a social activity and even a precondition for building a social relationship (Taddicken 2014). Social theory does not refute the privacy calculus approach or the biases approach, but adds to it, that we need to look at the social dimension of exchanging information.

Showing the importance of the social context, Lutz and Strathoff (2014) distinguish between social privacy concerns and institutional privacy concerns. Social privacy concerns are about other individuals, like the concern about your parents looking at your browser history. Institutional concerns are the concerns people have about companies or government using their data. This last concern is not as present in the daily lives of people, furthermore, it is very abstract (Lutz and Stratthoff 2014). Alyson Young and Anabel Quan-Haase (2013) show that most college students are concerned about their social privacy and do adjust their privacy settings to protect this. They are, however, not as concerned with institutional privacy, which could be explained by a lack of understanding of what companies like Facebook do with their data (Young and Quan-Haase 2013). Zhenhui Jiang, Cheng Suang Heng and Ben CF Choi (2013) studied why people disclose personal information on online social interaction sites, like chatrooms, while they do not get any directly visible rewards in return. Their results show that: “in the absence of monetary or tangible rewards, social rewards are just as attractive in balancing privacy concerns and governing individuals’ behavior” (Jiang, Heng and Choi 2013, 590).

Lutz and Strathoff (2014) identify trust as a possible explanation of the privacy paradox. They use the conventional definition of trust where trust is conceived as a psychological state wherein a person accepts a certain amount of vulnerability because they expect that the other will behave in a positive way (Lutz and Strathoff 2014). In their empirical test, it turned out that trust in companies or government is not significantly associated with privacy protective behaviour. This might indicate that the institutional privacy concern is, indeed, quite weak. They explain this different behaviour when it comes to social privacy and institutional privacy by referring to the differentiation between Gemeinschaft and Gesellschaft (Lutz and Strathoff 2014). People connect on social media in their search for belonging, one of the implicit parts of this Gemeinschaft-like community is that people share personal information with one another (Lutz and Strathoff 2014). However, the risks that are apparent with sharing information about yourself do not get adequately processed, as they would be in a Gesellschaft, which is more about a rational consideration of costs and benefits. Lutz and Strathoff

summarize it as follow: “the urge of being member of a community seems to trump the abstract recognition of data security issues” (2014, 98).

In the context of this strong urge to be a member of a community (Lutz and Strathoff 2014), combined with the social necessity of being active in the online community (Taddicken 2014), we can question whether it is really a choice not to be active on, for example, Facebook. Social theory explains the privacy paradox by showing that, while privacy attitudes might be strong, social pressure and need make someone disclose personal information. In this light, the notice and consent paradigm might not be giving you a fair option, the decline button might be harder to reach than thought.

Novel Theories

The research about the privacy paradox is, as became apparent above, quite extensive. However, the studies are not conclusive, and some studies show contradicting results. There is, therefore, still room for new theories about the privacy paradox to develop. Three of these new studies will be discussed here, to give an idea of what is still to come.

In a recent study about the privacy paradox, Wenjing Xie, Amy Fowler-Dawson, and Anita Tvauri (2019) used the theory of rational fatalism to explain the dichotomy between attitudes and behaviour in disclosing private information online. The theory of rational fatalism holds that when people assess a risk as being unavoidable, they will give up on avoiding this risk (Xie, Fowler-Dawson and Tvauri 2019). The results of rational fatalism theory are not conclusive. However, this could be due to some measurement errors in the design, and future research is necessary to enable us to say more about this theory.

In another novel study, Christian Pieter Hoffman, Christoph Lutz and Giulia Ranzini (2016) suggest that the privacy paradox could be solved by looking at privacy cynicism. They define privacy cynicism as an: “attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile” (Hoffman, Lutz and Ranzini 2016, 2). They see this privacy cynicism as a cognitive coping mechanism that allows people to ignore privacy concerns and assign the responsibility for the risk they are taking to forces outside of their control (Hoffmann, Lutz and Ranzini 2016).

A third novel approach comes from Adil Bilal, Stephen Wingreen and Ravishankar Sharma (2020) who argue in favour of a virtue ethics approach. Additionally, they argue that the previous research has been mainly based on Kantianism or Utilitarianism. Advocates of virtue ethics argue that, based on prior decisions and experiences, “our decision-making process is the outcome of our character dispositions and habits” (Bilal, Wingreen and Sharma 2020, 225). According to virtue ethics, a good

decision made by a virtuous person, is a decision that is based on its character dispositions. Bilal, Wingreen and Sharma (2020) state in their research proposal that the current day technology user lacks the dispositions and habits to make a good decision, and that this is an ethical issue that could be addressed by virtue ethics.

While these three new approaches are still underdeveloped, they show that besides the theories discussed above, there are still alternative explanations to be discovered.

The Privacy Paradox and the GDPR

In this chapter we discussed the privacy paradox, which is the dichotomy between privacy attitudes and privacy behaviour. A lot of research confirms this paradox; however, there is also research that contradicts it. This can at least partly be explained by the different theories that are used. The privacy calculus theory proposes that this paradox can be explained by considering that people weigh the benefits of disclosing information against the costs of disclosing. And apart from privacy attitudes, there are other costs and benefits to consider. This is the view that is reflected in the current liberal paradigm, where you must choose to accept or decline privacy policies. Behavioural economics argues that this process is not so simple, and that there are biases in the decision-making process that need to be considered. Social theory enlightens us about the role of social pressure and the urge people experience to belong to a group, making the disclosure of information not a real choice.

Kokolakis (2017) concludes his paper by saying that: “the dichotomy between privacy attitude and behaviour should not be considered a paradox anymore, since recent literature provides several logical explanations” (2017, 130). I do, however, not fully agree with this statement. As the contradicting results show, there is still room for improvement within the literature about the privacy paradox. The novel theories discussed above give us an insight of what can still be done within this field, and the results of new research will still be able to lead to new insights about this complex phenomenon. Furthermore, all studies apply the control over information conception of privacy, whereas as became apparent in the first chapter, there are more conceptions of privacy possible. Applying these conceptions to privacy paradox studies might lead to new results.

Even though this chapter did not provide us with an unambiguous conclusion about the privacy paradox and how to understand it, it still gives us some guidance in how policies could protect the online privacy of individuals. One of the most important aspects of the GDPR is that it gives the individual the ability to collect information about what happens with their data. Both through the ability to request a company to delete the data and through notice and consent systems on websites. This fits within the definition of what Solove called “privacy self-management”:

> *Under the current approach, the law provides people with a set of rights to enable them to make decisions about how to manage their data. These rights consist primarily of rights to notice, access, and consent regarding the collection, use, and disclosure of personal data. The goal of this bundle of rights is to provide people with control over their personal data, and through this control people can decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information.* (Solove 2013, 1880).

This model of privacy self-management fits the privacy calculus theory since it trusts on the individuals' ability to weight the costs of disclosure against the benefits. However, as the theories from behavioural economics has shown us, even with complete information, psychological biases in the decision-making processes may interrupt this rational calculus behaviour. Furthermore, social pressure might make it impossible not to disclose information. Different authors who studied the privacy paradox already expressed their concerns about this privacy-self management model.

Patricia Norberg, Daniel Horne and David Horne (2007) question the effectivity of policies that put the responsibility of the protection of privacy in the hands of individuals, since these individuals have shown to be willing to disclose personal information. This creates the difficult dilemma whether consumers should be protected against their own behaviour. They advise that more research should be done to really make effective policy to protect consumers privacy (Norberg, Horne and Horne 2007). According to Gordon Hull (2015), the system of "notice and consent" is a way of privacy self-management that does not work in protecting citizens' privacy. Inspired by Foucault, Hull calls this a successful failure because: "their failure to protect privacy tells only half the story. The other half of the story is their success in establishing a very specific model of ethical subjectivity" (Hull 2015, 90).

In conclusion, the literature about the privacy paradox suggests that the current privacy self-management model as used in the GDPR, might not fit the behaviour of people. This means that the GDPR does not provide a suiting protection to privacy violations. Policymakers in the field of privacy need to incorporate the research about the privacy paradox in their considerations of new policies, to make them fit with the behaviour of people.

Chapter 3: the value of privacy

The first chapter showed that while privacy law is mainly based on the conception of privacy as control over your information; there are other possible conceptions that would require a change in privacy law. In this chapter, I will discuss different conceptions on the normative value of privacy. The GDPR is based on a liberal perspective on the value of privacy that holds that it is crucial for personal autonomy. While I do not want to argue that the liberal perspective has nothing to offer, there are some points of criticism to discuss. I structured them into three main points: (1) privacy is not an individual value but a social value, (2) privacy is important for more than just autonomy, and (3) structures of power are not considered. In corresponding order, after discussing liberalism I will discuss republicanism, relationship theory, and critical theory. While there might be other theories that explain the value of privacy, these three theories represent the most important points of critique to the liberal paradigm and are therefore most suited in respect to the research question. The goal is not to refute the theory of liberalism, but to show that there are other possibilities, and these other possibilities require a change in privacy law.

Liberalism

In this section, a liberal perspective on the importance of privacy will be explicated; this is the currently dominant view in privacy law. While not all authors discussed here are devoted liberal thinkers, their perspectives on privacy fits the liberal scheme. Jeroen van den Hoven (1997) explains in four points why privacy is important for individuals. First, it is important to avoid information-based harm, like identity theft or extortion. Second, it is important to avoid informational inequality, for example, when you get discount coupons in exchange for your personal information. Third, it is important because it declines informational injustice, inspired by Walzer, van den Hoven argues that information should remain in one sphere and not transport into others. The final point is that privacy is important because it protects the moral autonomy of individuals. Van den Hoven (1997) argues that while communitarians might agree with the first three points, they will disagree with the point about moral autonomy, because this is based on the liberal self-image. Because this is the most distinctive part of liberal thought, I will discuss the final point of van den Hoven, that privacy is important for autonomy. This argument is made in two different ways, first, privacy is necessary for the creation of the "self", and this "self" is necessary for autonomy, and second, privacy is necessary for autonomy in a direct way.

Creation of the self

As articulated above by van den Hoven, what distinguishes liberal theory from other theories is the particular image of the self that they hold onto: “privacy is a necessary condition for something of basic value – the development of an autonomous self.” (Kupfer 1987, 81). To act autonomously, one needs to see itself as capable of shaping one’s own life. According to Kupfer, autonomy does not require just any self-concept, it requires an autonomous self-concept: seeing yourself as capable of having control over your life. Having privacy gives a child its very first experience of control, discovering how to use secrets, and how to strategically provide information. This enables the child to develop the autonomous self-concept (Kupfer 1987). Reiman (1976) sees privacy as a “social ritual” that is necessary for personhood, for creating the “self”. Reiman observes two distinct connections between privacy and personhood. Privacy is necessary for creating persons, in the sense that children learn that they have exclusive moral rights over their body: “I know this body is mine because unlike any other body present, I have in the past taken it outside of the range of anyone’s experience but my own, I can do so now, and I expect to do so in the future.” (Reiman 1976, 42). And in a second sense, privacy is needed for already developed persons to confirm this respect for their personhood. This importance of privacy for the development of children’s autonomous self-image also contains a difficulty in the liberal perspective on the importance of privacy for autonomy. Since children are less autonomous, one could question whether they should have any privacy, and at the same time, without privacy they may never become autonomous beings. This problem can be solved, however, by arguing that it is not a matter of absolutely no privacy and absolutely no autonomy. Children are somewhat autonomous and respectively deserve a certain amount of privacy. The same argument, of course, holds for the mentally or physically disabled. Where the individual in a wheelchair is not able to act autonomously in showering, the privacy of this act also decreases.

Autonomy

While Nissenbaum (2009) is not particularly convinced that the autonomy argument is the most convincing in the privacy debate, she does provide us with a useful categorization of the different connections between privacy and autonomy. Nissenbaum identifies three forms of relationships between privacy and autonomy. First, we can see privacy as a form of autonomy; where one can determine for themselves what happens with their personal information, in this way you control how others see you. Secondly, privacy enables us to have autonomy, a panoptic situation will make us behave like we think we ought to, and we might lose all autonomy. This reflects the ethical understanding of autonomy, as being able to determine for yourself what is your version of the good life (Cooke 1999). Maeve Cooke (1999) argues that to be able to develop this ethical autonomy, you

need to be able to exercise various attributes, like thinking critically and creatively and reflect on certain matters. And to exercise such things, one needs a private space. When making hard choices in life, we need privacy to critically consider the different options, without immediately getting punished for considering them (Kupfer 1987).

The final relationship between privacy and autonomy is that privacy protects us from being manipulated: "the more that is known about a person, the easier it is to control him" (Schwartz 1989, 676). A person is more autonomous when they are truer to themselves, and therefore, more authentic: "[f]reedom would consist in acting on the desires she would have if she were more rational and better informed." (Swift 2014, 84). It is often said that Facebook knows you better than you know yourself, so why then, is data collection a problem when it can give you what you really want? Online clothing stores know what you like, YouTube knows what you want to see during your lunch break, and Google Maps knows that on Thursday afternoons you like to visit the red-light districts. The final example shows the problem with this argument, not all information gathering is harmless. Furthermore, the value of autonomy is not that you immediately get what you want. It is the possibility of making decisions that fit your own moral standards. Mill argues that making difficult choices is important because: [t]he mental and moral, like the muscular powers, are improved only by being used." (Mill 1909, 61). And therefore, you should not just do anything because it is custom, you need to make choices. When all choices are made for us (by means of data collection) and not by us, we will lose the very skills that we need to make decisions.

When we want to apply this connection between privacy and autonomy to the topic of privacy law, however, we stumble upon a difficulty. Can laws protect autonomy? Cooke (1999) seems to find a way out of this by arguing in line with Habermas, Kant and Rousseau that there can be public autonomy when citizens can see themselves as joint authors of the law. To have public autonomy therefore, in a way, safeguards having private autonomy, and having private autonomy is only possible when privacy laws are in place. But this remains a difficult point. This might be why current privacy protection laws mainly place responsibility in the hands of the users by means of notice and consent rules. Notice and consent policies follow two logics. First, they see privacy as having control over information, but as we have seen in chapter one, there are more conceptions of privacy. Second, they use the logic of the free market, where to make a free and rational purchase, you need full information (Nissenbaum 2011). I would add a third, which is that it lays the responsibility of the protection of privacy with the individual. It articulates the idea that privacy is having control over your information and control is when you, as an autonomous being can decide whether you share your data or not.

Turning now to some points of criticism on the liberal notion of the value of privacy, Zuboff (2019) argues that the notice and consent paradigm might just be a way to give people the illusion of autonomy, while data-hungry companies like Facebook and Google find their ways to bypass the laws.

She also argues that the force of surveillance capitalism is too strong to fight as an individual, and that therefore the notice and consent laws will not protect the individual from privacy related harms. Additionally, one could argue that in the current situation where individuals have been made into subjects and have internalized the logic of self-surveillance, they are no longer able to act autonomously (Davies 1997). These points will be further explained in the section about critical theory.

A second category of criticism comes from the fact that the liberal notion of the value of privacy does not see privacy as something intrinsically valuable. The defence of privacy strictly in terms of liberty or autonomy leaves the door open to theories which argue that some invasions of privacy are better for autonomy than the protection of privacy (Fried 1984). In his criticism on the liberal perspective of privacy, Cohen argues that in the way as it is described by the liberals: "privacy is reactive and ultimately inessential." (2012, 1905). Furthermore, he questions the entire idea of having an autonomous self, because this self is always situated in a social context. He argues that we need to move the discussion into the field of sociology. This perspective will be further explained in the section about relationship theory. A final important point of criticism comes from Pricilla Regan, who argues that in the traditional liberal school of thought, privacy is seen as an individual good (Regan 2002). This view also prevails in current day laws and regulations, which aims to provide options for individuals regarding their own privacy. This is problematic because other values like security and prosperity are seen as social goods. Therefore, privacy will always end up as the loser when in conflict with these collective goods. Furthermore, privacy is constitutive for a well-functioning democracy, and should therefore be protected. This view will be further developed in the section about republican theory. While the proponents of liberalism undoubtedly have many great solutions for the proposed points of criticism, I will not discuss those here. The goal of this paper is not to defend the liberal notion of the value of privacy. It is to discover what other theories might be there and which ideas those theories could contribute to the discussion of privacy laws.

The liberal perspective on the value of privacy is currently dominant within privacy law. It holds that privacy is important for autonomy in both a direct and an indirect way. Privacy directly affects autonomy because without privacy, you do not have control over your information and therefore are not able to make autonomous decisions about what happens with your personal information. The indirect effect of privacy on autonomy lies in the argument that privacy is necessary for the creation of an image of the self, which is a necessity for autonomy. Current privacy laws also reflect this normative assessment of privacy as important for autonomy. The notice and consent rules enable individuals to choose whether or not they accept privacy policies and provide information; they therefore protect autonomy.

Republicanism

An alternative to the liberal account of the value of privacy can be found in republicanism. While liberal thinkers argue that privacy is important because it protects individual freedom and autonomy and therefore protects the individual from the state, republicans argue that citizens need privacy in order to participate in the state; to be active in politics. The respect for preferences is a very individual value, and in the liberal school, privacy is seen as an individual good (Regan 2002). This makes it possible to trade one basic human right for the other whenever this seems convenient. This view also prevails in current day laws and regulations, which provides individuals with options regarding their own privacy. In line with republican thought, Priscilla Regan, however, argues that privacy is not an individual good but a common good for at least three reasons: (1) most individuals value privacy and therefore it is a common value, (2) privacy is important for a democratic system and is therefore a public value, and (3) it is becoming more and more challenging for one person to have privacy when others have not. The first point is apparent as I already showed in the second chapter about the privacy paradox. The second and third argument by Regan will be elaborated upon below, by looking at the work of Hannah Arendt and Cass Sunstein.

Hannah Arendt

In multiple publications by Hannah Arendt, the distinction between the private and the public is reflected upon; while it might not take centre stage, it does form an important basis for her work. She sees it as it were day and night, where we need both because without one the other wont function (Borren 2010). While privacy is highly important for the natural man in the private sphere, in the public sphere it constitutes a form of inhumanity (Borren 2010). Arendt explains this by referring to inmates in concentration camps during the second world war, who were truly invisible. The other side of the same medal, natural visibility - when the private becomes public - is just as inhumane as public invisibility (Borren 2010). Natural visibility is an important aspect of totalitarian regimes, where there cannot be a private live: “political problems were distorted to the point of pure perversion when Jews tried to solve them by means of inner experience and private emotions; private life was poisoned to the point of inhumanity” (Arendt 1973, 67). What totalitarian regimes do, is abolish the separation between the private and the public, and thereby they destroy the private person: “After a few years of power and systematic co-ordination, the Nazis could rightly announce: "The only person who is still a private individual in Germany is somebody who is asleep.”” (Arendt 1973, 339).

Where the private life is that of the household and reproduction, the public life is about politics. But this does not mean that the natural man becomes entirely visible in the public sphere. To be able to

participate in politics, means to leave the private sphere behind and enter the public sphere while wearing a mask. The citizen that we see when involving in politics, is not the same as the natural man in his private life. In the political sphere we wear a mask to ensure that "our politically irrelevant qualities and inevitable natural inequalities" (Borren 2010, 171), do not constrain us. The mask, however, is not the same as the private sphere: "[t]he mask protects men against inappropriate visibility; the private sphere disallows visibility entirely. The mask still allows for disclosure; the private sphere does not." (Borren 2010, 172).

The distinction made by Arendt between the private and the public, however, leaves us wondering where consumer privacy belongs. To solve this, we need to look at a third sphere that Arendt distinguishes: the social sphere. This third sphere is a modern-age invention and makes it difficult to see the distinguishing line between private and public (Arendt 1958). This sphere was birthed when tasks of household and labour, previously belonging to the private sphere, became of collective concern. Apart from blurring the lines, the new sphere has changed the old spheres beyond recognition, and is constantly gaining ground:

> *[M]ass society not only destroys the public realm but the private as well, deprives men not only of their place in the world but of their private home, where they once felt sheltered against the world and where, at any rate, even those excluded from the world could find a substitute in the warmth of the hearth and the limited reality of family life.* (Arendt 1958, 59).

The social sphere is the sphere where the economy belongs, and therefore the appropriate sphere to place the problem of consumer privacy. In line with the argument made by Arendt, this sphere is gaining space. Corporations are hungry for ever more information and are intruding upon both the private life of individuals as well as the political life of citizens. Arendt's argument would therefore be that; to protect consumer privacy is to protect both the private life of individuals as well as the political life of citizens. When the social sphere keeps gaining space, and the private and public sphere dissolve, only one sphere is left, and this one sphere could very well be the sphere of totalitarianism.

Cass Sunstein

Focussing more on how the data is used once gathered, Sunstein (2017) shows us the existing tension between political sovereignty and consumer sovereignty. He argues that people are creating a "daily me" where they only read and see items that are in line with their own perspectives. Where free consumer choice leads people to create a daily me, this undermines their ability as citizens to make informed decisions about policies. Free choice is not the same thing as freedom. And the unlimited free choice we have in creating our own bubbles of information, might be decreasing our freedom.

Furthermore, the choice to limit yourself to read exclusively from CNN or watch only Fox-news does not only influences you own situation, but in your duties as a citizen also influences the lives of others.

In applying the republican perspective on privacy law, Sunstein makes a useful suggestion: "my basic claim is that we should evaluate communication technologies and social media by asking how they affect us as citizens, not only by asking how they affect us as consumers" (Sunstein 2017, 157). Even though he is not strictly speaking about privacy, I think this does not make the claim any less valid. While in the notice and consent regulations individuals are mainly treated in their role as consumer who needs to be able to choose, privacy law should treat them as citizens, who deserve protection. Sunstein (2017) teaches us that we must distinguish the role we have as citizens from the role we have as consumers. As a citizen, we might very well be in favour of strict laws to protect our privacy, but as a consumer, we might want to accept all Cookies to have the best online shopping experience.

The market is creating desires, which in turn, the market will satisfy. But is this making us happier? Sunstein, inspired by Jon Elster, shows that humans are adaptive: "[t]he fox does not want the grapes because he believes them to be sour, but the fox believes them to be sour because they are unavailable" (2017, 165). When deprived of certain things, people tend to not want them anymore, but them not wanting it is a direct result of the deprivation and should therefore not be seen as a justification of this deprivation. In his explanation of the consumption treadmill, Sunstein argues that our consumption of more, better, and faster delivered goods does not necessarily improve our lives. Because our standards are rising, the amount of happiness something brings us is declining. Furthermore, while the many different options we have might seem to give us a sort of freedom, this might not be the case:

> *[W]e do freedom a grave disservice by insisting on respect for preferences. When options are plentiful, things are much better. But from the standpoint of freedom, there is also a problem when people's past choices lead to the development of preferences that limit their own horizons and capacity for citizenship.* (Sunstein 2017, 174).

I will return now to the final point made by Regan and try to clarify why it is difficult for a person to have privacy when others have not. We must see the collection of data as a puzzle; the more pieces that are in the right spot, the easier it is to know where the other pieces need to go. Recently, companies like MyHeritageDNA, 23andMe and AncestryDNA are gaining in popularity. You might want to know who your ancestors are, and therefore send your DNA to one of those companies. But what lots of people do not realize is that this does not only compromise your own privacy, but also that of your family with whom you share DNA with (Erlich et al. 2018). Research even suggest that it will not take long until the puzzle is completed, and these companies can identify everyone. This argument does not only hold for DNA but could be applied on all sorts of data.

Concluding, we must say that the main point of the republican school of thought about privacy is that it is not an individual value but a community value. As showed above with the example of DNA, it is extremely difficult for one person to have privacy when others have not. But most importantly, according to republican theory; a democratic society is not possible without privacy. We need to distinguish the private from the public or social sphere to be really human, and when this is no longer possible, a totalitarian state might arise. While in the sphere of consumer privacy individuals might act as consumers, the state should protect them and their rights as citizens.

Relationship Theory

A completely different view on the importance of privacy is provided by Charles Fried and James Rachels, who argue that privacy is important for creating and maintaining intimate relationships. Fried (1984) sees privacy as a necessary precondition to have friendship, love, and trust. He does not take the importance of these intimate relationships lightly: "privacy is the necessary context for relationships which we would hardly be human if we had to do without – the relationships of love, friendship and trust." (Fried 1984, 211). After the relationship between privacy and friendship is established, we will turn to the importance of friendship by looking at the work of Aristotle.

Rachels and Fried

Rachels contemplates that a lot of theories that try to answer the question why privacy is important can only be applied in cases of harmful or embarrassing information. If we want to include cases where we just feel like some information is "none of your business", we need to look into the role that privacy has in the creation and maintenance of social relationships (Rachels 1975). In the divergent social relationships that we maintain, we behave in different manners: being polite to your parents in law, making jokes with your friends, and sharing intimate thought with your lover. This differentiation of behaviour is in part possible because of the privacy we have. The amount and sort of information that one shares with another defines the type of relationship and level of intimacy in this relationship. Providing information to build intimate relationships with other persons is in a way providing "moral capital". In choosing the amount of moral capital that you provide the other with, you control the extent of intimacy that you have with them: "where any intimate revelation may be heard by monitoring officials, it loses the quality of exclusive intimacy required of a gesture of love and friendship." (Fried 1984, 216). But beside this moral capital, respecting other's privacy means having respect for each other, which is necessary in relationships of love and friendship.

Trust works in a slightly different way from friendship and love. Being monitored means that you are not being trusted, and since trust is reciprocal, you will also not trust the one that is monitoring you: "the man who cannot be trusted cannot himself trust or learn to trust." (Fried 1984, 213). And since trust is important in all types of relationships, this is another important problem of declining privacy. Besides trust, a distinct aspect of social relationships is respect. Using a Kantian point of view, Fried argues that persons must always be seen and treated as ends in themselves, and that all persons are entitled to basic rights, like privacy. Fried thereby also argues against utilitarianism, because basic rights are not to be overridden in the search for the greatest happiness for all. Describing persons as being entitled to basic rights is to give them respect, and in turn, deeming yourself worthy of basic rights is a form of self-respect (Fried 1984).

Reiman does not hold back in his critique on the theory of Fried and Rachels: "I find this analysis both compelling and hauntingly distasteful" (1976, 32). What Reiman finds compelling is that it fits our everyday experiences, and is a great explanation of the feeling of jealousy: if I give you more information about myself than I give someone else, you must be more important to me. But it is also distasteful, because it provides a market conception of the value of privacy, where it is only important that I have more than others. Additionally, the other person might be my psychologist, with whom I share my deepest and darkest thoughts with. This does not mean that my relationship with the psychologist is more intimate than the relationship with my friend (Reiman 1976). Reiman argues that instead of sharing information, the basis of relationships is caring for each other. Reiman's second objection to the theories of Fried and Rachels is that when there is no ability to have social relationships, there is no right to privacy. Which would mean that people with a severe form of autism, or people in solitary confinement would not have a right to privacy. While these are very valid points, they do not contend that there is no connection between the development and maintenance of relationships and privacy.

Aristotle

Rachels and Fried argue that privacy is necessary for the development and maintenance of friendships. This leaves us with the question what it is that makes friendship so essential. One of the most decisive works on friendship is to be found in Aristotle's *Nicomachean ethics,* where friendship is seen as one of the most meaningful aspects of life (Pangle 2002).

The natural starting point for the study of friendship is Plato's *Lysis,* where Socrates portrays friendship as nothing more than neediness and trying to get things from it. In academics, however, the opinions are divided on whether this is indeed Socrates' honest opinion, or whether he is exaggerating to make a different point. Socrates argues that nothing is simply good in itself, but things are always

good for someone. He even goes as far as to suggest that we only value our own virtue for what is gives us. However, what makes it confusing, is that further in his conversation with the two young friends, Socrates contends that we can also love someone because of his kindred soul: “whose excellence and happiness we enjoy vicariously, as in some way akin to our own excellence and happiness.” (Pangle 2002, 31). The *Lysis* therefore seems to suggest that there are two different types of friendship: one based on utility and one based on kinship.

Aristotle identifies three types of friendships: the useful, the pleasant and the good (Pangle 2002). A friendship of the useful is like the friendship as described by Socrates, where you are friends with each other for the goal of getting something out of it. Friendships of pleasure are more satisfying forms of friendships that are based on having pleasurable experiences together: “[t]he presence of the friend is cherished as an end in itself, even if the friend’s complete good is not actively sought as an end in itself.” (Pangle 2002, 40). Friendships of the good resemble a perfect friendship where both partners love each other for their character and their virtue. Virtue, according to Aristotle, is what brings us true happiness. But that is not all that friendship brings us: “[f]riendship is an essential safeguard for the life, property, and political freedom or power that virtue requires as equipment for its full exercise, and it provides the worthiest objects of virtuous action.” (Pangle 2002, 16). In its relationship to the political community, friendship might even be more important than laws to hold the polis together, for without friendship community ties will be unable to exist.

According to Fried and Rachels, privacy is important for friendship, love, and trust. Hence, different types of relationships depend on the information you share with each other. We might argue that in the friendship of the good, as described by Aristotle, one must be able to share the most intimate information with one another to be able to really see the virtues of the friend. This requires trust that the other will not distribute this personal information in any way that might hurt you. While Kant would say that you can never fully trust a friend, Aristotle argues that in a good friendship you should open your hart without reserve and thus trust the other (Pangle 2002). According to Fried (1984), when information shared with a friend is also picked up by someone secretly listening, this lessens the value of the friendship. This makes one wonder whether in a society where companies are eager to gather ever more information about us, the good friendship of Aristotle is still possible.

Critical Theory

Critical theory focusses on power structures within society. While the other theories do consider power - the power of a citizen in the political sphere, or the power of an autonomous individual to do as he wants - critical theory looks at systems of power and provides us with an insight into their inner

mechanisms. This section will start out with the theory by Shoshana Zuboff, who describes the current age as surveillance capitalism: “[i]t revives Karl Marx’s old image of capitalism as a vampire that feeds on labor, but with an unexpected turn. Instead of labor, surveillance capitalism feeds on every aspect of every human’s experience” (Zuboff 2019, 9). This will be followed by work of Michel Foucault about disciplinary power and biopower: “The old simple schema of confinement and enclosure – thick walls, a heavy gate that prevents entering or leaving – began to be replaced by the calculation of openings, of filled and empty spaces, passages and transparencies.”(Foucault 1991, 172).

Surveillance capitalism

According to Zuboff (2019), we are living in the age of surveillance capitalism, which is characterized by a new economic order where power, wealth, and knowledge are more centralized than ever before and where human experience is seen as free raw material, up for grabs. While surveillance capitalism is profoundly anti-democratic, its power is not centred in the state, but in companies. The first economic imperative of surveillance capitalism is the extraction imperative, which holds that there needs to be a constant flow of data, of raw material: “[u]nder this new regime, the precise moment at which our needs are met is also the precise moment at which our lives are plundered for behavioral data, and all for the sake of others’ gain” (Zuboff 2019, 53). This raw material is behavioural surplus, which is data that is gathered while it is not necessary for the improvement of the product but is solely used as raw material. The second imperative of surveillance capitalism is the prediction imperative, which is the need to always be able to predict future behaviour of individuals.

Surveillance capitalism has at least three important points in common with market capitalism: (1) they claim the privilege of freedom and knowledge, (2) they change the relationships between humans, and (3) a collectivist society is no longer possible. But there are also differences between the two capitalisms, for a starter, while market capitalism was a combination of freedom and ignorance, where the workings were mysterious, surveillance capitalism is freedom and knowledge, where we are looking for the most certainty. Furthermore, where market capitalism was highly dependent on the work of people, this is no longer the case for surveillance capitalism, which only requires a small group of highly intelligent people.

Zuboff (2019) argues that we are currently living in the era of second modernity, which is characterized by the existential contradiction of the desire to exercise control over our lives, while that control is declining ever more. For members of this period, the division of learning is the new social order, just like the division of labour was the social order for their grandparents. In defining the division of learning, we need to ask three questions: “Who knows? Who decides? Who decides who

decides?" (Zuboff 2019, 327). This division of learning is a new form of social inequality that is increasingly dividing society. "Who knows" is about the inequality of knowledge and whether one can learn. "Who decides" is about which institutions or people have the power to determine who gets to learn or not. "Who decides who decides" is about who determines who has this power.

While the complaint about surveillance capitalism is often that privacy is eroded, Zuboff (2019) argues that this is not the case. Privacy is redistributed, and what is eroded is the decisional rights over privacy. However, this still means that a large part of society experiences less and less privacy; since the extraction of data is a privacy breach. But now comes the difficult question of why this is a problem. From reading Zuboff's book, multiple problems can be established, but in the end they all come down to the fact that it will cost us our humanity: "if industrial civilization flourished at the expense of nature and now threatens to cost us the Earth, an information civilization shaped by surveillance capitalism will thrive at the expense of human nature and threatens to cost us our humanity" (Zuboff 2019, 347). This happens because people are merely treated as behavioural surplus ready to be gathered, and as a consequence, this data is used to manipulate our behaviour and make us into predictable individuals: "it is no longer enough to automate information flows about us; the goal is to *automate us*" (Zuboff 2019, 8). Behavioural surplus is no longer only gathered to understand us, it is more often used to nudge us. Zuboff labels this modification of behaviour: instrumentarianism. In reaction to Hannah Arendt, Zuboff argues that surveillance capitalism will not lead to a totalitarian state, but to an instrumentarian state. Where totalitarianism reconstructed the human species by both genocide and engineering the soul, instrumentarian power engineers behaviour and creates predictable individuals.

At the start of surveillance capitalism, companies took advantage of the lack of laws about the unprecedented social territories they were exploring. Now that laws about the privacy of citizens are there, Facebook and Google will do anything within their power to "kill online privacy protection, limit regulations, weaken or block privacy-enhancing legislation, and thwart every attempt to circumscribe their practices because such laws are existential threats to the frictionless flow of behavioral surplus" (Zuboff 2019, 105). The neoliberal ideology that is still prevailing in much of the Western world, has contributed to these practises with their dominant vision of laws as coercive and authoritarian. Furthermore, they often do not follow the law; agreements are made with a handshake. Companies like Google use different tactics to shield themselves from interference by the law (Zuboff 2019). First, they are not shy in showing how they can influence electoral politics. Second, they deliberately try to blur the lines between public and private interests, by lobbying. Third, Google's influence over the academic world, where it impacts public opinion and policymakers. A transparency rapport shows that during the Obama administration, 197 government officials migrated to work for Google, and 31 Google employees started to work for the government, in fields directly related to the work of Google (Zuboff 2019). While this paper examines the role of the GDPR in protecting citizen's

privacy, according to Zuboff, this will not protect us from surveillance capitalism. She notes that as history showed us, individuals cannot fight such a strong power on their own, so the form of notice and consent will not work. Furthermore, while Facebook officially announced that they were supportive of the GDPR, right before it went into working, they changed the location of the headquarter, to assure it would not fall under the GDPR laws (Zuboff 2019). So while laws might not be able to secure privacy, Zuboff does not propose a concrete alternative. However, I would argue that this must entail declining the power of the market.

Disciplinary power

Inspired by the panopticon as described by Jeremy Bentham where, by putting a central tower inside a prison, the prisoner could always be seen and would therefore act as if watched, Foucault (1991) argues that this model is not only used in prison, but is embedded in the different institutions of society. And wherever it is institutionalized, it will increase the effect of the institution. So, in the case of commercial surveillance, it will increase their profit. It is intended to make institutions work more effectively. This exercise of power Foucault (1991) calls "disciplinary power", and for this to succeed, you need three things (1) hierarchical observation, (2) normalizing judgement, and (3) examination.

The hierarchical power takes the form of surveillance that is always present and sees everything. It is anonymous, because the network of relations that fosters it is unclear to the individual that is being watched. The power of normalizing judgement is that it tells people how to behave; the worker how to work, the doctor how to treat his patient, and the student how to excel. Even though this creates some sort of homogenous society, it still fosters individuality, because there are still ranks, hierarchies, and gaps in how well people do. The final element of disciplinary power, examination, is a combination of the former two. It tests how well the student studied, and in that way determines his rank. Through this disciplinary power, subjectification happens (Foucault 1991). Hull (2015) argues that we need to see the notice and consent regime as a particular form of subjectification, which is, as argued by Foucault, a technique of power that makes persons into subjects: "users are presented with a repeated choice: more privacy or less? Everything about the context of that choice encourages them to answer "less." This in turn habituates them into thinking that less privacy is what normal people want." (Hull 2015, 97).

The account of disciplinary power is useful for demonstrating why it is that individuals hand over personal information voluntarily. Consumers take part in self-surveillance, voluntarily handing over information to corporations. In part, because of the commodification of privacy, where it is seen as something you can exchange for financial benefits. By introducing a voluntary component - the choice to provide information or not - into the scheme of surveillance, a lot of public concern is neutralized

(Davies 1997). Davies gives two examples, the first one being requests of the police to "voluntary" provide DNA for an investigation, but if you decline you will automatically become a suspect. The second example is that of the "voluntary" ID card, which when you do not own one, will make life impossible.

While being useful in understanding certain aspects of the effects of decreasing privacy, the classical description by Foucault about surveillance does not completely fit our current day society because surveillance is not visible like the tower of Bentham's panopticon was (Ceyhan 2012). In his work on biopower, Foucault argues that in ancient times this power was used by threatening life, but this has transformed into the modern-day threat of regulating life (Ceyhan 2012). In this frame, bio-politicized surveillance observes the human body in all its aspects, with the goal to provide security in the sense of certainty (Ceyhan 2012). This is comparable with the view of Zuboff (2019) that surveillance capitalism creates predictability. Contrary to the technique of discipline, security, the goal of biopower, is exercised on society at large, while discipline focuses on individuals: "managing their life, health, psychology and behaviors" (Ceyhan 2012, 39). Security is not limited to one aspect of society, like crime, but is constantly broadening its scope into other domains, ensuring normalization where it comes. Biopower is part of the liberal ideology of aiming towards ever more efficiency, both by governments and corporations (Ceyhan 2012).

What the different perspectives within critical theory have in common is that they refuse the comparison that is often made between modern society and Big Brother from Orwell's dystopian novel *1984*: "[w]e may have feared the intrusion of Big Brother into our homes and private lives, but we open wide the door to his corporate cousins even as they reduce us to economic abstracts and marketing segments." (Campbell and Carlson 2002, 604). According to Zuboff (2019) it is not the dystopia from Orwell that is becoming reality, but the utopia as described by Skinner (1948) in *Walden Two*, where behavioural engineering is used to create predictable individuals. Not a Big Brother as in totalitarian states that changes souls, but a big other that uses behavioural modification. Not so much Big Brother, but Brave New World or Big Other, not tyranny but harmony (Davies 1997).

Recapitulating the above stated, what critical theory has shown us about privacy is that the declining of privacy accounts for greater social inequality. Humans are merely treated as sources of raw material, like if they were oil, to be used for large corporations to make money. At the same time, the data that is gathered is used against them in the form of biopower to make them into predictable beings. Concluding, privacy is important because without it, there is an accumulation of power in one place, and ordinary people will be made into subjects that are merely good for the extraction of data.

The value of privacy and the GDPR

As this chapter showed, there are different ways of looking at the value of privacy. While current privacy law is mainly derived from the liberal view on privacy and autonomy, it is important to look past this and see the different theories that are there. Liberal theory showed us that privacy is needed to create an image of the self as an autonomous being. Without this, the person will not be able to act autonomously. Acting autonomously also means having control over your own actions, which is in line with the conception of privacy as control over personal information. These conceptions of the meaning and value of privacy are constitutive for the currently dominant "notice and consent" laws. Republicanism refutes the liberal idea that privacy is an individual value. They argue that it is important for democracy to have privacy, and therefore laws should not just give the option to share personal information or not, but should sometimes protect individuals from these options and forbid certain data collection. As Sunstein (2017) argued, it is not always constructive for freedom to have a lot of options, sometimes you need to protect citizens against their own choices. Furthermore, while people might act like consumers, the state should treat and protect them as citizens. Fried and Rachels argue that without privacy we are unable to experience friendship, love, and trust, and therefore privacy should be a basic right worthy of protection. The good friendship as Aristotle described it might no longer be in reach without the privacy necessary to develop a friendship. Privacy laws should therefore be stricter. Critical theory focusses on power structures and shows us that the power of corporations is gaining space and that they are using us for our data. Consequently, inequality is rising, and people are made into subjects to be used by companies to make money off. If a law aims to prevent this, this will not happen through a notice and consent policy because individuals have internalized their role as subjects. The law should be limiting the power of companies and thereby strengthen the power of individuals. I will not suggest which of these perspectives is "right" or "wrong", because they have all made important contributions. What is the problem is that privacy law is only based on the liberal account on the value of privacy while this account has its limitations and other accounts have new insights to offer.

Conclusion

"We can achieve a sort of control under which the controlled, though they are following a code much more scrupulously than was ever the case under the old system, nevertheless feel free. They are doing what they want to do, not what they are forced to do. That's the source of the tremendous power of positive reinforcement – there's no restraint and no revolt. By a careful cultural design, we control not the final behavior, but the inclination to behave – the motives, the desires, the wishes."

(Skinner 1948, 246-247)

Just like many other authors in the field of privacy, I started this paper with a quote from Orwell's dystopian book *1984.* Even though I still think this book has many great insights to offer, after the information this paper provided us with, a quote from Skinner's (1948) utopian *Walden Two* seemed more appropriate. The obvious power present in *1984* by Big Brother that watches your every move is not our present reality. The power we are experiencing now is more subtle, the surveillance more latent and behavioural modification is the chosen tactic of domination. At least, that is what the critical theorists would argue. We might consider that Orwell's book is most in line with a liberal dystopia, where personal autonomy is brought back to a minimum, while Skinner describes how, while having a lot of freedom of choice, behaviour is modified to fit the goal of efficiency. Current privacy laws like the GDPR are based on the liberal notion of privacy. The aim of this paper was to find alternative meanings to the concept of privacy, privacy behaviour, and the value of privacy. By looking at both the liberal conception and its critics, alternative conceptions were found.

In the first chapter the different conceptions of the meaning of privacy were described, roughly distinguished into three categories: (1) the reductionist approach, (2) the control over information approach, and (3) privacy as the right to be let alone. The chapter started out with the reductionist approach because it argues that we do not need any more privacy laws because privacy is already sufficiently protected in common law. Thompson (1975) argues that when privacy is violated, there is always another right also being violated. Posner (1979) agrees and with his focus on the economic features of privacy argues that the important aspects of privacy – like protecting innovation – are already protected sufficiently in common law, and more privacy would only benefit the people who have something to hide. The control over information approach is the one currently dominant in privacy law. The notice and consent policy is based on giving people the option whether or not to accept privacy policies. While not trying to downplay the differences, all the proponents of this approach identify a loss of privacy as a loss of control. The main point of criticism is that one also loses privacy when voluntarily handing over information (Gavison 1980). The final approach that was discussed in this chapter was the approach by Warren and Brandeis (1890) who argue that privacy is the right to be let alone. Gavison (1980) gives the conception of privacy as being let alone more body

by arguing that there are three elements that we need to consider when we talk about a loss of privacy: secrecy, anonymity, and access. Her definition could be criticized for being too broad, but I think it is rightfully so, because losses of privacy are everywhere. The real question is which ones are harmful and which are not. Gavison's conception is simple and useful and seems to withhold from giving a normative evaluation. Privacy is not only lost when there is no control. When accepting cookies, one has a choice but still loses privacy. Policy makers must consider that only giving the option is not to protect citizen's privacy.

In the second chapter, research about the privacy paradox was discussed, which is the discrepancy between privacy attitudes and privacy behaviour. While the evidence on the privacy paradox is ambiguous, it does show that privacy attitudes and privacy behaviour are not always in line. There has been an abundance of studies that try to explain this paradox, I divided them into three broad categories: (1) privacy calculus, (2) behavioural economics, and (3) social theory. The privacy calculus model is the one that is currently dominant in privacy law, which assumes that people make a balanced choice between the costs and benefits of providing personal information. Behavioural economics argues that this does not work in the way that the calculus model describes because there are multiple psychological mechanisms that influence this process, making it seem highly unlikely that a person could make the rational calculus in the case of privacy. These mechanisms also explain the privacy paradox, since the connection between privacy attitudes and privacy behaviour is not as straight forward as previous research has made it seem in their models. Social theory adds to this that there is an important social aspect of providing information and refusing to do so might seriously harm your social life. People have a strong urge to belong to a community, and therefore, to decline certain privacy policies might be harder than it seems. As the ambiguous results and the novel theories show, however, this is still a field that requires more research. But what we can conclude is that the GDPR is only based on a limited perception of privacy behaviour, while the other perceptions would require stricter policies.

The third and final chapter covers four different theories about the normative value of privacy: (1) liberalism, (2) republicanism, (3) relationship theory, and (4) critical theory. The liberal perspective, also prominent in law, argues that privacy is important because it is constitutive for autonomy and freedom. Both in a direct way because without privacy you lose the option not to share certain information, and in an indirect way through the creation of an image of the self as an autonomous being. This is echoed in current privacy law where the notice and consent paradigm is mainly protecting freedom of choice instead of privacy. While liberalism holds a negative conception of freedom, republicanism holds a positive conception, where you do not need to be free from the state but free to participate in the state. In their theory about privacy, republicans make two important points. First, privacy is not only of value for the individual but for the entire community, for it is exceedingly difficult to have privacy when others have not. Second, we need to be able to distinguish

the private from the public sphere because, as Hannah Arendt argues, when the private becomes public it is no longer possible to be human. Furthermore, it is no longer possible for a democracy to really function and totalitarianism is a possible threat. Sunstein adds that freedom of choice is not the same as freedom. So, for privacy policy, giving citizens the choice whether to share personal information might not be constitutive for their freedom and their role as citizens. In the somewhat brief account of relationship theory, it became clear that privacy is important for friendship, love, and trust. An important point is that when privacy is breached, this also shows a lack of trust. Trust is reciprocal and therefore people who are constantly under surveillance will never learn to trust. Building intimate relationships with others also depends on privacy, because to have differentiating levels of intimacy means to share particular personal information with different people. Aristotle enlightened us on the importance of friendship, not only because it is something that we cannot happily live without, but also because the polis will fall apart without it. Finally, critical theory has shown us that declining privacy accounts for greater social inequality. Humans are merely treated as sources of raw material, like if they were oil, to be used for large corporations to make money off. At the same time, this data that is gathered is used against them in the form of biopower to make them into predictable beings, producing more certainty and efficiency.

There is no short answer to the research question feasible, but I will try to state it here as clearly as possible. The GDPR is designed on the back of three assumptions: (1) privacy is having control over information, (2) people can make a costs/benefit analysis about their privacy, and (3) privacy is important because it protects autonomy. I have put together these three assumptions under the name of the liberal paradigm. The aim of this paper was not to proof that this view is wrong, but to show that there are alternatives. Throughout the paper it became clear that the liberal view is a limited view on privacy and that this has massive implications for the current protection of privacy. Answering the second part of the research question; how these different views on privacy would influence privacy policy, I would like to suggest a couple of points that policy makers should keep in mind. First, privacy is more than just having control, the other aspects like the right to be left alone must also be considered. Second, people do not behave as a calculus when it comes to difficult privacy questions, so the assumption that they will, needs to disappear from the drawing board. Third, privacy is not only valuable for autonomy and freedom but has a much greater value. Fourth, do not treat privacy as an individual value but as a community value when weighting different rights. As critical theory suggested, however, the privacy problem will not only be solved with new privacy policy; there is an inherent problem with the power of the market. As long as big companies have the power they have now, they will do anything to keep harvesting our data. We need a privacy policy that firmly restricts the gathering of data by companies by default, not by option. The responsibility of privacy protection needs to shift from the realm of the individual into to realm of the government, who carries the task of protecting its citizens.

While I think that this paper has made a good contribution to the field of political theory, it obviously has its limitations. For a starter, because it covers so many different theories, details and nuances are sometimes missing. For example, there are big differences between liberal scholars that have not been discussed. All theories discussed can and should be a paper on their own. This did, however, not fit the goal of the paper, which was to show multiple alternatives to the liberal point of view. Another limitation is that this paper solely focusses on a part of the GDPR that is about notice and consent, while the GDPR does contain other rules for protecting privacy. However, the notice and consent part of the regulations is throughout the academic world seen as one of the most important within the GDPR (Politou, Alepis and Patsakis 2018). But this does indeed not take away the argument that there is more to the GDPR than just the notice and consent rules. A final limitation is that this paper only considers the Western view on privacy. And might therefore be missing important insights from scholars that work outside of the Western tradition.

The field of privacy research is still quite a dispersed field, where different disciplines come together to tackle this one difficult subject. From studies of technology and ICT, to studies of medicine and psychology, sociology, law, political science, and political theory, all these studies and more make separate contributions to this field but are not often combined together. This paper has brought some of this fields together to tackle three important questions. According to Nissenbaum (2010), part of the confusion in the academic debate about privacy comes from mixing descriptive conceptions of privacy with normative conceptions in privacy. The attribution of this paper to the field of knowledge is in part to make a clear distinction between the conception of privacy and the value of privacy. Furthermore, while the value of privacy for the development of children and adults have gotten quite some attention in psychology, there is a lack of literature in the field of political theory. Finally, this paper has used the theories of some of the great names within political theory in a field where they are not used often enough. While privacy is a vastly changing field, these authors have great insights to offer and their work should be further examined to see what else they can add to the privacy debate.

In a field so quickly changing as that of privacy, there is always more research to be done. While the literature on the conception of privacy was fairly organized and documented, this is not the case for the value of privacy. While I attempted to provide an overview of the different possible arguments, future research can discover new arguments, new perspectives and therefore reach new conclusions. In the research about the privacy paradox there is still a lot of work to do, and these new studies should not solely focus on the calculus approach but give extra attention to behavioural economics and social theory. A research that could combine all three approaches, since they all have valid points to make, would be a great addition to the current literature. This paper is written during the COVID-19 pandemic, a time where the development of tracking apps and the discussion about privacy is taking mainstage. As Foucault argued that “the plague gave rise to disciplinary projects” (Foucault 1977, 198), future research needs to look back on the developments made during this crisis and their effects

on privacy. In doing so, the arguments made in this paper need to be considered. Especially that when you measure privacy as an individual value against healthcare as a community value, privacy will always lose. But when considering the republican argument that privacy *is* a community value, this might lead to different conclusions.

By using an interdisciplinary approach, this paper showed that there is more to privacy than meets the eye. The liberal paradigm only tells part of the story of what privacy is, how it works, and why it is important. While *1984* is often used to warn us about the changing society, our focus on trying to avoid Big Brother might be giving us tunnel vision. This paper does not argue that the liberal paradigm is wrong or that Orwell's *1984* should be disregarded as outdated. Is does, however, argue that we need to broaden our perspective on privacy, and that we should take into account different theories and seek our comparison of the current society in alternative literature: Big Brother is Watching You, Welcome in Walden Two's Brave New World.

Literature

Acquisti, Alessandro. 2004. “Privacy in electronic commerce and the economics of immediate gratification.” *Proceedings of the 5th ACM conference on Electronic commerce*: 21-29.

Acquisti, Allesandro and Ralph Gross. 2006. “Imagined communities: Awareness, information sharing, and privacy on the Facebook.” *International workshop on privacy enhancing technologies*: 36-58.

Acquisti, Allesandro and Jens Grossklags. 2007. “What can behavioral economics teach us about privacy.” *Digital privacy: theory, technologies and practices* 18: 363-377.

Allen, Anita. 1988. *Uneasy access: Privacy for women in a free society*. New Jersey: Rowman & Littlefield.

Allen, Anita. 1998. “Coercing privacy.” *William & Mary Law Review* 40 (3): 1-56.

Arendt, Hannah. 1958. *The human condition.* Chicago: University of Chicago Press.

Arendt, Hannah. 1973. *The Origins of Totalitarianism.* New York: Harcourt Brace & Company.

Barnes, Susan. 2006. “A privacy paradox: Social networking in the United States.” *First Monday* 11 (9). https://doi.org/10.5210/fm.v11i9.1394.

Barth, Susanne, Menno D.T de Jong, Marianne Junger, Pieter H Hartel, and Janina C Roppelt. 2019. “Putting the Privacy Paradox to the Test: Online Privacy and Security Behaviors among Users with Technical Knowledge, Privacy Awareness, and Financial Resources.” *Telematics and Informatics* 41: 55–69.

Beresford, Alastair R, Kübler Dorothea, and Preibusch Sören. 2012. “Unwillingness to Pay for Privacy : A Field Experiment.” *Economics Letters* 117 (1): 25–28.

Bilal, Adil, Stephen Wingreen and Ravishankar Sharma. 2020. “Virtue Ethics as a Solution to the Privacy Paradox and Trust in Emerging Technologies.” *Proceedings of the 2020 The 3rd International Conference on Information Science and System:* 224-228.

Blank, Grant, Gillian Bolsover and Elizabeth Dubois. 2014. “A new privacy paradox: Young people and privacy on social network sites.” *Prepared for the Annual Meeting of the American Sociological Association* 17: 1-33.

Borren, Marieke. 2010. “*Amor Mundi : Hannah Arendt's Political Phenomenology of World*.” Dissertation, University of Amsterdam.

Hargittai, Eszter. 2010. “Facebook privacy settings: Who cares?.” *First Monday*, 15 (8). https://journals.uic.edu/ojs/index.php/fm/article/download/3086/2589.

Campbell, John Edward, and Matt Carlson. 2002. “Panopticon.com: Online Surveillance and the Commodification of Privacy.” *Journal of Broadcasting & Electronic Media* 46 (4): 586–606.

Carrascal, Juan Pablo, Christopher Riederer, Vijay Erramilli, Mauro Cherubini and Rodrigo de Oliveira. 2013. “Your browsing behavior for a big mac: Economics of personal information online.” *Proceedings of the 22nd international conference on World Wide Web*: 189-200.

Ceyhan, Ayse. 2012. “Surveillance as biopower”. In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, David Lyon and Kevin D. Haggerty, 38-45. New York: Routledge.

Cohen, Julie. 2012. “What privacy is for.” *Harvard Law Rev*iew 126: 1904-1933.

Cooke, Maeve. 1999. “A space of one’s own: autonomy, privacy, liberty.” *Philosophy & Social Criticism* 25 (1): 22-53.

Culnan, Mary J. and Pamela K. Armstrong. 1999. “Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation.” *Organization science* 10 (1): 104-115.

Daniel, Solove. 2013.” Privacy self-management and the consent dilemma.” *Harvard. Law Review* 126: 1880-1883.

Davies, Simon G. 1997. “Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity.” In *Technology and privacy: The new landscape*, edited by Philip Agre and Marc Rotenberg, 143-166. Cambridge: MIT Press.

Deleuze, Gilles and Michel Foucault. 1977. Intellectuals and power. *Language, counter-memory, practice*. https://theanarchistlibrary.org/library/gilles-deleuze-michel-foucault-intellectuals-and-power.pdf.

Dienlin, Tobias, and Sabine Trepte. 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): 285–297. https://doi-org.ru.idm.oclc.org/10.1002/ejsp.2049.

Dinev, Tamara, and Paul Hart. 2006. “An Extended Privacy Calculus Model for E-Commerce Transactions.” *Information Systems Research* 17 (1): 61–80. https://doi-org.ru.idm.oclc.org/10.1287/isre.1060.0080.

D'Souza, Giles, and Joseph E Phelps. 2009. “The Privacy Paradox: The Case of Secondary Disclosure.” *Review of Marketing Science* 7 (1). https://doi-org.ru.idm.oclc.org/10.2202/1546-5616.1072.

Egelman, Serge, Adrienne Porter Felt and David Wagner. 2013. Choice architecture and smartphone privacy: There's a price for that. In *The economics of information security and privacy,* edited by Rainer Böhme, 211-236. Belin: Springer.

Erlich Yaniv, Tal Shor, Itsik Pe'er and Shai Carmi. 2018. "Identity Inference of Genomic Data Using Long-Range Familial Searches." *Science* 362 (6415): 690–94. https://doi-org.ru.idm.oclc.org/10.1126/science.aau4832.

Foucault, Michel. 1977. *Discipline and punish: The birth of the prison.* London: Penguin Books.

Fried, Charles. 1977. Privacy: Economics and Ethics: A Comment on Posner. *Georgia Law Rev*iew 12.

Fried, C. (1984). Privacy [a moral analysis]. In *Philosophical Dimensions of Privacy*, edited by Ferdinand David Schoeman, 203-222. Cambridge: Cambridge University Press.

Gandy Jr, Oscar H. 1989. "The surveillance society: information technology and bureaucratic social control." *Journal of Communication* 39 (3): 61-76.

Gavison, Ruth. 1980. "Privacy and the Limits of Law." *The Yale Law Journal* 89 (3): 421-471.

GDPR. 2016. *GDPR*. Accessed February 3, 2020. https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679.

Groenendijk, Virgina. 2019. *Bedrijven klagen over privacywet: 'te complex en vaag'*. Accessed February 3, 2020. https://www.ad.nl/economie/bedrijven-klagen-over-privacywet-te-complex-en-vaag~a38af6e7/.

Hann, Il-Horn, Kai-Lung Hui, Sang-Yong Tom Lee, and Ivan P. L Png. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach." *Journal of Management Information Systems* 24 (2): 13–42.

Hoffmann C.P, Lutz C, and Ranzini G. 2016. "Privacy Cynicism: A New Approach to the Privacy Paradox." *Cyberpsychology* 10 (4). https://doi-org.ru.idm.oclc.org/10.5817/CP2016-4-7.

Huberman, B.A, E Adar, and L.R Fine. 2005. "Valuating Privacy." *Ieee Security and Privacy Magazine* 3 (5): 22–25. https://doi-org.ru.idm.oclc.org/10.1109/MSP.2005.137.

Hui, Kai-Lung, Hock Hai Teo, and Sang-Yong Tom Lee. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment." Mis Quarterly 31 (1): 19–33.

Hull, Gordon. 2015. "Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data." *Ethics and Information Technology* 17 (2): 89–101.

iang, Zhenhui (Jack), Cheng Suang Heng, and Ben C. F Choi. 2013. “Research Note-Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions.” *Information Systems Research* 24 (3): 579–95.

Joinson, Adam N and Carina B Paine. 2007. Self-disclosure, privacy and the Internet. In *The Oxford handbook of Internet psychology*, edited by Adam N. Joinson, Katelyn Y. A. McKenna, Tom Postmes, and Ulf-Dietrich Reips. 10.1093/oxfordhb/9780199561803.013.0016.

Joinson, Adam, Ulf-Dietrich Reips, Tom Buchanan, and Carina B. Paine Schofield. 2010. “Privacy, Trust, and Self-Disclosure Online.” *Human-Computer Interaction* 25 (1): 1–24. https://doi-org.ru.idm.oclc.org/10.1080/07370020903586662.

Kokolakis, Spyros. 2017. “Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon.” *Computers & Security* 64: 122–34. https://doi-org.ru.idm.oclc.org/10.1016/j.cose.2015.07.002.

Krasnova, Hanna, Oliver Günther, Sarah Spiekermann and Ksenia Koroleva. 2009. “Privacy concerns and identity in online social networks.” *Identity in the Information Society* 2 (1): 39-63.

Kupfer, Joseph. 1987. “Privacy, Autonomy, and Self-Concept.” *American Philosophical Quarterly* 24 (1): 81–89.

Laufer, Robert S, and Maxine Wolfe. 1977. “Privacy As a Concept and a Social Issue: A Multidimensional Developmental Theory.” *Journal of Social Issues* 33 (3): 22–42. https://doi-org.ru.idm.oclc.org/10.1111/j.1540-4560.1977.tb01880.x.

Lee, Haein, Hyejin Park, and Jinwoo Kim. 2013. “Why Do People Share Their Context Information on Social Network Services? A Qualitative Study and an Experimental Study on Users' Behavior of Balancing Perceived Benefit and Risk.” *International Journal of Human - Computer Studies* 71 (9): 862–77. https://doi-org.ru.idm.oclc.org/10.1016/j.ijhcs.2013.01.005.

Lutz, Christoph and Pepe Strathoff. 2014. *“Privacy concerns and online behavior–Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses.”* Accessed on April 15, 2020. https://www.alexandria.unisg.ch/228096/1/Lutz_Strathoff.pdf.

Margulis, Stephen T. 1977. “Conceptions of Privacy: Current Status and Next Steps.” *Journal of Social Issues* 33 (3): 5–21.

Margulis, Stephen T. 2003. “Privacy As a Social Issue and Behavioral Concept.” *Journal of Social Issues* 59 (2): 243–62.

McDonald, Aleecia M and Lorrie Faith Cranor. 2008. “The cost of reading privacy policies.” *Isjlp*, 4 (3): 543-568.

Mill, John Stuart. 1909. *On Liberty*. London: The Floating Press.

Nissenbaum, Helen. 2004. "Privacy As Contextual Integrity." *Washington Law Review* 79: 119–58.

Nissenbaum, Helen. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford: Stanford University Press.

Nissenbaum, Helen. 2011. "A Contextual Approach to Privacy Online." *Daedalus* 140 (4): 32–48.

Norberg, Patricia A and Daniel R Horne. 2007. "Privacy Attitudes and Privacy-Related Behavior." *Psychology and Marketing* 24 (10): 829–47.

Norberg, Patricia A, Daniel R Horne and David A Horne. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors." *Journal of Consumer Affairs* 41 (1): 100–126.

Orwell, George. 1949. *1984.* London: Penguin Group.

Pangle, Lorraine Smith. 2002. *Aristotle and the Philosophy of Friendship*. Cambridge: Cambridge University Press.

Parker, Richard B. 1973. "A definition of privacy." *Rutgers law review* 27: 275-290.

Pentina, Iryna, Lixuan Zhang, Hatem Bata, and Ying Chen. 2016. "Exploring Privacy Paradox in Information-Sensitive Mobile App Adoption: A Cross-Cultural Comparison." *Computers in Human Behavior* 65: 409–19. https://doi-org.ru.idm.oclc.org/10.1016/j.chb.2016.09.005.

Politou, Eugenia, Efthimios Alepis, and Constantinos Patsakis. 2018. "Forgetting Personal Data and Revoking Consent Under the Gdpr: Challenges and Proposed Solutions." *Journal of Cybersecurity* 4 (1). https://doi-org.ru.idm.oclc.org/10.1093/cybsec/tyy001.

Posner, Richard A. 1979. "Privacy, secrecy, and reputation." *Buffalo Law Review* 28: 1-55.

Rachels, James. 1975. "Why Privacy Is Important." *Philosophy & Public Affairs* 4 (4): 323–33.

Rajagopalan, Megha. 2019. *Period Tracker Apps Used By Millions Of Women Are Sharing Incredibly Sensitive Data With Facebook.* Accessed on January 6, 2020. https://www.buzzfeednews.com/article/meghara/period-tracker-apps-facebook-maya-mia-fem.

Regan, Priscilla M. 2002. "Privacy As a Common Good in the Digital World." *Information, Communication & Society* 5 (3): 382–405. https://doi-org.ru.idm.oclc.org/10.1080/13691180210159328.

Reiman, Jeffrey H. 1976. "Privacy, Intimacy, and Personhood." *Philosophy & Public Affairs* 6 (1): 26–44.

Reiman, Jeffrey H. 2017. “Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future.” *Santa Clara Computer & High Tech Law Journal* 11: 27-44.

Schwartz, Paul. 1989. “The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination.” The American Journal of Comparative Law 37 (4): 675–701.

Skinner, Burrhus F. (1948). *Walden Two.* Indianapolis: Hackett Publishing Company.

Solove, Daniel J. 2002. “Conceptualizing privacy.” *California Law Rev*iew 90: 1087-1156.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. 2001. “E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior.” *Proceedings of the 3rd ACM conference on Electronic Commerce:* 38-47.

Stuart, Avelie, Arosha K Bandara, and Mark Levine. 2019. “The Psychology of Privacy in the Digital Age.” *Social and Personality Psychology Compass* 13 (11). https://doi-org.ru.idm.oclc.org/10.1111/spc3.12507.

Sundar, Shyam S, Hyunjin Kang, Mu Wu, Eun Go and Bo Zhang. 2013. “Unlocking the privacy paradox: do cognitive heuristics hold the key?.” *CHI'13 extended abstracts on human factors in computing systems:* 811-816.

Sunstein, Cass R. 2018. *#Republic.* New Jersey: Princeton University Press.

Swant, Marty. 2019. *Edward Snowden Thinks Even The EU’s Sweeping Privacy Law Is Too Weak.* Accessed on January 12, 2020. https://www.forbes.com/sites/martyswant/2019/11/05/edward-snowden-thinks-even-the-eus-sweeping-privacy-law-is-too-weak/#7b9137567ffd.

Swift, Adam. 2019. *Political philosophy: a beginners' guide for students and politicians*. Cambridge: John Wiley & Taddicken, Monika. 2014. “The ‘Privacy Paradox’ in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure.” *Journal of Computer-Mediated Communication* 19 (2): 248–73. https://doi-org.ru.idm.oclc.org/10.1111/jcc4.12052.Sons.

Thomson, Judith Jarvis. 1975. The right to privacy. *Philosophy & Public Affairs* 102 (4): 295-314.

Tsai, Janice Y, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. “The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study.” *Information Systems Research* 22 (2): 254–68. https://doi-org.ru.idm.oclc.org/10.1287/isre.1090.0260.

Tufekci, Zeynep. 2008. “Can you see me now? Audience and disclosure regulation in online social network sites.” *Bulletin of Science, Technology & Society* 28 (1): 20-36.

van den Hoven, M. J. 1997. “Privacy and the Varieties of Moral Wrong-Doing in an Information Age.” *Acm Sigcas Computers and Society* 27 (3): 33–37. https://doi-org.ru.idm.oclc.org/10.1145/270858.270868.

Warren, Samuel D and Louis D Brandeis. 1890. “The right to privacy.” *Harvard law review* 102 (4): 193-220.

Westin, Alan F. 1967. *Privacy and freedom*. New York: Atheneum.

Westin, Alan F. 2003. “Social and Political Dimensions of Privacy.” *Journal of Social Issues* 59 (2): 431–53.

White, April. 2018. *A Brief History of Surveillance in America.* Accessed on January 12, 2020. https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/.

Xie, Wenjing, Amy Fowler-Dawson, and Anita Tvauri. 2019. “Revealing the Relationship between Rational Fatalism and the Online Privacy Paradox.” *Behaviour & Information Technology* 38 (7): 742–59. https://doi-org.ru.idm.oclc.org/10.1080/0144929X.2018.1552717.

Young, Alyson Leigh and Anabel Quan-Haase. 2013. “Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited.” *Information Communication and Society* 16 (4): 479–500. https://doi-org.ru.idm.oclc.org/10.1080/1369118X.2013.777757.

Zafeiropoulou, Aristea M, David E Millard, Craig Webber and Kieron O'Hara. 2013, May. “Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions?.” *Proceedings of the 5th Annual ACM Web Science Conference*: 463-472.

Zuboff, Shoshana. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* New York: PublicAffairs.