Can Privacy Survive in the Digital Age?

Universiteit Leiden

Thesis Presented for the Master of Philosophical Perspectives on Politics and the Economy

Nathan van der Heyden

January 2019

Table of Contents

Introduction

This thesis will argue that our current conception of privacy is insufficient to properly survive the threats posed by technological innovation in modern society. Privacy is by all account a difficult concept to clarify and define. There are two things that most agree on: first, privacy is important; second, privacy is at best under threat or at worst a thing of the past. “We have come to the end of privacy; our private lives, as our grandparents would have recognised them, have been winnowed away to the realm of the shameful and secret”, wrote Alex Preston in The Guardian (2014), and this sentiment seems to be shared amongst many.

According to Shoshana Zuboff, this phenomenon is a logical evolution of capitalism. The economic logic of capitalism, rendered possible by the advent of new technology and, in particular, Big Data analytics, has lead to the increasing commodification of things that were not part of the economic sphere previously. With the advent of surveillance capitalism, it is human experience itself that is commodified. Through this process, companies try to better predict human behaviours to anticipate market needs, and as Zuboff argues, this approach culminates in actually controlling human behaviour, compromising any form of agency (2019).

This thesis sets out to diagnose privacy, identify the threats surrounding it, demonstrate the ethical, technical and economical issues with our current conception and our preferred tools for its protection and demonstrate its incompatibility with our modern economic system. Finally, this thesis will propose potential solutions and avenues of reflexion that allow us to hopefully adapt our conception of privacy and potentially protect this vital right in our society.

Privacy is widely understood and defined, like here in the Merriam-Webster dictionary, as "the quality or state of being apart from company or observation". Surveying other definitions, the ideas of seclusion and secrecy, control over our own information and anonymity often surface. While it seems there is a certain agreement in civil society that privacy needs to be protected, it is unclear exactly what privacy means and why it is worth defending. US Supreme Court Justice Louis Brandeis defended it in 1928 already as "the most comprehensive of rights and the right most valued by civilized men"(Olmstead v. United States, 1928).

The 12th article of the United Nations Declaration of Human Rights reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

The legal scholar Daniel Solove admits that after extensive study he was not able to bring a satisfactory answer as to what exactly privacy is. According to him, privacy is a plurality of different things and efforts to define it into a single concept is a losing battle. He argues that it is necessary to understand privacy as an evolutionary process (Solove, 2008).

The reason why privacy is so complicated to define can be partially explained by the natural evolution of the values it protects and its interdisciplinary nature. The widely shared conception of privacy as a form of secrecy does not do justice to the fact that any conception of privacy is based on evolving ethical concerns. Helen Nissenbaum defends a theory of privacy in "Privacy In Context: Technology, Policy, and the Integrity of Social Life" which argues that privacy is control over the flow of information about oneself. To do so, this flow of information has to abide by contextual information norms, which evolve based on the means of communication, the type of information and the identity of the sender and the recipient of this information (2010).

The difficulty in proposing a single definition of privacy becomes clearer in view of Nissenbaum's understanding of the concept. Not only do people change but the means of communication and the type of information communicated influence how we must consider privacy. Both flexibilities in the ethical framework and respect of core ethical values are needed to ensure that privacy, and all that it protects, are safeguarded (Nissenbaum, 2010). The contextual information norms she refers to could be understood, for example, as democracy. New informational norms brought about by technology might threaten democracy through a loss of privacy, and as such our understanding of privacy has to change and adapt to these new systems, such as social media for example.

This is the definition and theory of privacy that will be used in this thesis. In her view, while we have a right to privacy, it is neither a right to control our information or restrict access to it. For her, contextual integrity refers to the idea that our right is to live in a world where our expectations about the flow of personal information are met. These expectations are shaped by convention and by the confidence in the mutual support between information norms and key political and moral organising principles of social life. It's the evolution of these principles that allow for her conception of privacy to adapt to technological evolution (2010).

As Solove argues: "people in nearly all societies have debated issues of privacy, ranging from gossip to eavesdropping to surveillance" (Solove, p.4, 2008). However, the radical change brought about by information technology in the last fifty years clearly marks at least a need to reconsider our informational norms but more likely a complete redefinition of privacy. Some scholars such as Shoshana Zuboff in her new book "The Age of Surveillance Capitalism" propose that the challenge is even larger than we thought. According to her, surveillance capitalism which refers to the collection of behavioural data with the goal of accurately predicting human behaviour is simply incompatible with privacy. She compares the defence of privacy to closing the doors of a house on fire in order to preserve the rooms from smoke damage.

The idea shared by all scholars is that information technology represents a new challenge to privacy. In particular, Big Data analytics have managed to allow the harvesting, processing and analysis of immense quantities of data which are now worth a fortune. They've certainly changed the informational norms and, as will be shown in more detail below, rendered privacy almost impossible. Privacy understood as control over the flow of one's own information implies that the data subject knows that this flow of information is happening in the first place. In the case of Big Data analyses, this is often not the case. Our actions will be monitored without us knowing and the conclusions inferred from this data will be used to influence our behaviour.

Regulations such as the GDPR in Europe are certainly showing that politicians care about the protection of privacy and are ready to reinforce data security. However, data security is not always the solution, and the focus on greater technological protection of privacy and the provision of tools for users to control the flow of their data can also miss the mark. One of the greatest privacy scandals of the decade was the harvesting, processing and analysis of millions of users data in the Cambridge Analytica scandal in which none of the victims were "hacked" in the traditional sense

of the word. There were no hooded criminals trying to hack into the accounts of millions but rather a survey app that was massively and voluntarily downloaded by Facebook users. The academic researcher who developed this app sold it to Cambridge Analytica and therefore allowed them access to mountains of personal information from the people who downloaded the app but also their Facebook friends (Menand, 2018).

This problem becomes even more prevalent in the modern world for groups. While certain groups have a legal identity and can hold anyone invading their privacy accountable, Big Data analytics has the unique characteristic of creating groups without human input and do so without anyone realising it. When those technology-formed uninformed of their own existence are being discriminated against, it becomes impossible to limit our understanding of privacy simply as control over our information.

As of now, the understanding of privacy as protection of one's own information is insufficient to survive in the troubled waters of modern society. This thesis will first argue that all the values traditionally associated with privacy such as freedom of speech, democracy and self-determination are threatened by our insufficient understanding of what it means to protect our privacy. It is because of the reasons developed in the following chapters that privacy is not faring well in today's world.

The first chapter will focus on the main issues and criticisms against privacy. First, certain scholars argue that privacy, the sense of obscurity and secrecy, is not desirable for society. Second, the two main tools of privacy in the digital realm are not capable by themselves to truly protect it. Third, most privacy legislation focuses on the individual. Part of this chapter will advocate for the need to change this scope to the group.

The second chapter will clarify the position of privacy in the modern economic logic. Privacy has a bad reputation for market advocates, as greater information improves market efficiency. As behavioural prediction becomes one of the most profitable businesses in modern capitalism, privacy is under threat by some of the biggest companies in the world. What place can there be for privacy in modern economy?

The third chapter will develop a new conception of privacy that allows not only the clarification of the reasons why privacy is so important but also the avenues of reflexion over how it can be best respected. It will also offer a debate on whether it is already too late for privacy and much more pressing matters require public attention in the protection of autonomy.

Chapter 1: Assessing Privacy

The objective of this chapter is to show that the way we think about privacy today is problematic and spurs criticisms from different angles. First, this chapter will assess the argument that while privacy can benefit individuals, it is detrimental to society as a whole. Second, it will question whether the two main tools used to protect privacy are still capable of doing the job. Finally, it will propose a criticism to the individualistic approach often used when considering matters of privacy.

1. Privacy, Obscurity or Secrecy?

Our modern understanding of privacy can lead us to certain conclusions which show that privacy can be detrimental to the greater public good. While it provides a certain protection and breathing room, it can also allow for undesirable or uncivil behaviour. In "The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public", Heidi Anderson argues that society overestimates the benefits of privacy and underestimate exposure benefits. According to her, the fear for the loss of privacy in the event of technological innovation often appears between fears of the negative uses of this innovation and the following appreciation of the benefits. However, in the case of privacy, or rather loss of privacy, there are many benefits to look forward to.

First, exposure allows for better governmental accountability. Exposure here references the amount of publicity that a public action receives. From her point of view as an American citizen where police brutality is a very hot issue, we can see how total exposure can help counteract these types of actions. According to Anderson, the potential loss of privacy to the people is heavily offset by the gains that the exposure of the modern world offers. She gives the example of homophobic comments said by a politician at a private rally that were shared on social media, in this case certainly the public good is benefited by the truth being shared on social media even at the cost of the loss of the politician's privacy (Anderson, 2010).

Second, Anderson notes the potential individual behavioural improvements that a "no privacy in public" rule would generate. Just as police surveillance discourages crimes, it also discourages bad behaviour in the public space. People are less likely to jaywalk or drop cigarette butts on the ground if they know they are being monitored. This holds true as well in the digital world. At the price of personal privacy, great social improvements can be earned and might leave society better off than it was, she argues. For example, holding drivers responsible for their misconducts might even encourage better driving habits and potentially save lives. She also argues that surveillance can be the best deterrent to crime as well as facilitating apprehension and prosecution of criminals (Anderson, 2010).

Third, Anderson argues that there might be emotional benefits in exposing parts of our lives, even if it might be painful in the short term. These emotional benefits can also be shared by people watching the video. For example, the public can relate to certain emotions felt by the exposed or it can help normalise behaviour and allow other people who engage in similar conducts to feel less alone (Anderson, 2010). It seems however here that she's confusing privacy with secrecy, her point here refers to hiding emotions while privacy refers to deciding with whom we'd like to share private information about our emotions.

Finally, Anderson argues that more exposure allows for better prevention of deception by malicious people. According to her, this might be a net benefit for society even though it would hurt people who are trying to gain from this obscurity around themselves (Anderson, p.596). Jeffrey Wasserstrom also argues that the duality of private and public life can be a strain on individuals. He notes that maintenance of a private side leads to an unintegrated life which lacks a clear sense of self and leaves humans vulnerable and shameful (1984).

To summarize these points, the value of privacy in the sense of obscurity around a person should not be, in her view, overestimated. Exposure, while individually heavier to bear for citizens, might contribute to a better society as a whole. As David Brin said eloquently: "When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else" (Brin, p.13, 1998).

Obscurity as a legal and philosophical concept refers to the idea that some actions done in the public realm should still be legally protected to conserve the privacy of the individuals concerned. Exposure refers to instances where an individual gathers and shares to the public truthful information about someone else without the expressed consent of this other person. It could be a blog post, a video, a story recounted to another person, etc... Exposure reduces the obscurity of the person concerned by the story, the exposed (Anderson, 2010).

The Obscurity Problem, as Anderson calls it, arises when a citizen lawfully collects and exposes to the public certain information that another citizen has shared in public in the first place, in doing so increasing the exposure and reducing the obscurity around the other citizen's actions. The particular action that is exposed has to be shared with the public in the first place (Anderson, 2010). For example, if a citizen films a police officer abusing his powers in the street, whether he deliberately wanted to share that behaviour in public or not is not the issue. As he did so in the street, the information was public in the first place. While the police officer might want to reduce the overall visibility, or exposure, of that action; the action happened in public in the first place.

A debate ensues between the supporters of the "no privacy in public" rule and those who defend obscurity because it allows individuals a certain amount of shelter from social conventions. While there are certainly advantages to a society where public actions that legitimately deserve outcry are publicized and shared widely, there are also potential problems for the person's well-being.

What is important to note about Anderson's understanding of obscurity is that it only concerns pieces of information that are already, in a way, public. It is different from privacy in that privacy refers to the protection of private matters, while obscurity refers to limiting the amount of exposure a person's public actions might have.

While this debate started well into the 20th century, no one could have predicted the technological developments that have radically changed the way information can be collected, distributed and the growing threat to obscurity. Filming police brutality and live-streaming it to Facebook clearly creates another kind of problem to potential obscurity than the ones possible without this sort of technology. Whereas a small part of society mostly constituted of journalists were able to dramatically improve the exposure of events, technology has brought the necessary tools to a majority of the population to threaten the privacy and obscurity of fellow citizens.

We are all constantly one mistake away from becoming a viral video and losing our obscurity forever. One might one to share emotional thoughts on a blog to a small number of readers but strongly oppose these thoughts being shared worldwide. In this case, the difference between privacy and obscurity becomes clear; while the thoughts were never private, they were not destined for that level of exposure. In this sense, a person might want protection both of his privacy and of his obscurity as two different values, leading us to think of privacy as protection of both private information and public information about oneself.

While this shows that privacy still has a certain amount of importance, Anderson argues that it is still debatable whether privacy truly benefits society as a whole, both as the control over private information and the amount of exposure of our public actions.

2. Providing the Tools for Reliable Privacy Protection

While the previous point offered a criticism of the very concept of privacy and its desirability in modern society, this previous problem might not even matter. Privacy protection in the digital age relies on its two trusty tools without which it seems to have no chance to survive: anonymity and informed consent. However, as this chapter will show, both of these are threatened by Big Data analytics and might have been rendered useless when it comes to protecting the values insured by privacy.

Anonymity refers to the state of a person whose name is unknown. Anonymity has been seen by many to be the panacea in the context of privacy and Big Data. In a way, anonymity does not really protect privacy as much as it bypasses it entirely. By detaching identity of data subjects from the data, extensive studies are allowed on a group level which has done tremendous good to several

domains such as education and public health without threatening anyone's privacy (Barocas and Nissenbaum, 2014).

However, anonymity has some flaws as well. Anonymised data can often easily be traced back to the data subject. In the year 2000 already, researchers proved that 87 per cent of Americans could be uniquely identified on the basis of 3 small bits of information about themselves: sex, zip code and birthdate (Barocas and Nissenbaum, 2014). If that was already possible twenty years ago, the prospect of privacy through anonymity is even bleaker now. In the legal domain, this is referred to as "mosaic theory". It suggests that while some bits of information may appear harmless by themselves, in a large database linked with others they have the potential to be traced back to one single identifiable individual (Powers and Jablonski, 2017).

One of the most notorious events in mosaic theory happened in 2006 with the AOL Data Release. America Online, an American Internet Service Provider, decided to release the anonymised data of its search engine, one of the most widely used at the time in the US: 20 million search queries from 650 thousand users. The objective was to encourage internet behaviour research. It anonymised the data by removing identifying information such as AOL username and IP addresses but identified all queries of a particular user to a certain random identifying number to allow researchers to correlate different searches to a single user (Ohm, 2010). Within days, not only researchers but also bloggers and normal citizens had a lot of fun assembling bizarre search histories together and mocking certain numbers for their search queries. Until there, no harm to privacy though considering the names of actual people were not linked to the queries. However, New York Times journalists very quickly managed to piece together search queries to identify unique individuals. Using searches in certain localities. In particular, a certain Thelma Arnold from Lilburn, Georgia had looked for landscapers in her small village, several people whose last name matched hers and other searches that, while harmless and untraceable by themselves, quickly pointed to her when put together. Associated with her number were also searches such as "60 single men", "numb fingers" and "dog that urinates on everything" (Ohm, 2010). Needless to say, the resulting fallout and loss of trust in AOL led to the resignation of many employees and certainly played a role in the sharp decline of the company.

Computer scientists have been working hard this last decade to rethink anonymisation through measures such as k-anonymity and differential privacy, both techniques that make identifying single individuals much more difficult. However, in the arms race of privacy between computer scientists making data harder to link to individuals and Big Data analytics' increasing capacity to find correlations and identifying information in seemingly random data, no actual real-world application has been so far implemented to completely guarantees the anonymity of data subjects (Barocas and Nissenbaum, 2014).

it is important to note that anonymity is only a useful solution when researchers do not need nor want to know the identities associated with the data. For example, if researchers want to know how much smoking relates to lung cancer, they might look into medical data and find a correlation.

However, if doctors want to find out which patients in a database are more likely to have lung cancer then an anonymised database is of no use to them.

Barocas and Nissenbaum go further in their critique of anonymity and ask whether, in a world where anonymity is infallible and we have the necessary technology to protect the identity of data subjects, anonymity is still capable of addressing the problems and risks that Big Data analytics poses to privacy.

Anonymity is the protection of identity by completely getting rid of it. We could describe anonymity as namelessness. It allows individuals to interact with each other without any sort of control or punishment possible to their real identity. This protection allows individuals to express opinions, ask questions or reach out for help without fear of repercussions and consequences to their reputation. Nissenbaum argued in earlier work than anonymity supported "socially viable institutions like peer review, whistle-blowing and voting."(Nissenbaum, 1999). However, according to the authors, anonymity's value, does not lie in namelessness but rather in the unreachability that it affords (Barocas, Nissenbaum, 2014). By that, the authors mean that protecting his name is not the main worry of the individual using anonymity but rather it is what this namelessness affords - the lack of consequences to his real identity - that is of interest.

This is a very important distinction to make, one that commercial actors often abuse. If a company claims to maintain anonymous records, it means that they rely on persistent identifiers that differ from more regular personally identifiable information (or PII). In such instances, while a company might have no way of matching my purchase history to my name, they can certainly recognize me as a unique individual that has previously used their services and match my different historical purchases together to recommend future buys. While they would not use my name to do so, I am still in this case anonymous but identifiable (Barocas and Nissenbaum, 2014).

For example, this is exactly how Google uses its AdID to recommend certain advertisements to users that are more likely to act on them. While AdID is anonymous because it does not use names or PII, this anonymous identifier will be used to track each individual users behaviour online (Barocas and Nissenbaum, 2014). In this particular case, even though Google can claim to protect the anonymity of its users behind an AdID that is unique and untraceable to a real-world identity while still compromising what anonymity affords.

Another tech giant also shows the issue that anonymous identifiers can create. As Facebook privacy policy does not allow it to share email addresses of its users to potential advertisers, the website uses a formula to transform these addresses into a unique string of characters. Then, when the advertisers use the same formula on their customer email lists, they can check for matches between those email lists and Facebook users. They can then target ads on Facebook to customers already on their email lists and no actual email addresses were exchanged in the process (Barocas and Nissenbaum, p.2014).

Does the question then become what is anonymity actually protecting? The protection of anonymity is important because of the unreachability that it affords, not because citizens do not want companies to know their names. If a company can still amass data, facts and a profile around me without actually having to know my name and use this profile for their own purposes, can I still consider myself and my privacy protected?

The other way we can control our privacy and decide which pieces of information we'd like to share and with whom is by providing informed consent. Privacy does not refer to a state of secrecy but rather to the control over one's data. One of the most obvious effects of the GDPR regulations to European internet users has been to compel websites to ask for consent to use all sorts of trackers and cookies to retain pieces of information about their users. However, can privacy really be considered as protected by these consent forms?

Privacy, above all, is a choice about the flow of information. I can choose to disclose certain pieces of information about myself or I can choose to keep them private. In privacy theory, informed consent is often an answer proposed because it ensures that I get to choose which informations I want to disclose to the world. If I am informed as to which data is collected, by whom, for what and with whom it could be shared and I still agree to share this information then my privacy should be respected (Barocas and Nissenbaum, 2014).

it is not so simple though and Big Data analytics threatens the statute of informed consent as a competent protector of privacy. At the core of the issue is the transparency paradox which necessitates two seemingly opposed characteristics from classic terms of service contracts. On the one hand, research has shown that very few people read terms of services while using online tools and the ones who do read them do not understand them (Barocas and Nissenbaum, 2014). On the other, for informed consent to be worthwhile, it needs to be exhaustive and inform the users on all of the ways in which he will be monitored, his data will be used etc...

This transparency paradox necessitates at the same time information to be completely transparent and exhaustive but also clear and succinct as to encourage the user to actually read it. As clarity results in less fidelity, it seems hard to defend informed consent as the sole guardian of privacy online (Barocas and Nissenbaum, 2014). Big data analytics only adds to this issue when one considers that one of its defining characteristics is its ability to find correlations that researchers did not account or plan for. Often the researchers do not know in advance what they will get out of the data and so could not possibly be capable of truthfully informing the subjects about what they are consenting to.

The issue of informed consent as a protector of privacy with Big Data analytics also stems from a phenomenon called tyranny of the minority. If a representative minority of a target group consents to its data being analysed and disclose personal information, the conclusions that Big Data analytics can draw might apply to the rest of the target group (Barocas and Nissenbaum, 2014). For example, smokers might want to hide from health insurers that their smoking may lead to lung

cancer. If a minority of smokers accept to undergo tests that show that they are more likely to develop lung cancer than the rest of the population, the health insurance prices of smokers that did not consent to these tests will still go up.

This can also be used to discover information about a person that they did not consent to share. For example, recent studies have shown that through social network analysis we can infer great amounts of data about certain users on the basis of their friends. Facts such as university majors, sexual orientation, age or graduation year can be accurately guessed because of other person's consent to share them. The company we keep can then threaten our online privacy (Mislove, 2010). The same study revealed that multiple attributes can be inferred globally if only 20% of the users reveal that information. If this verifies, then the consent of the other 80% is unnecessary.

We can conclude that both of these tools are insufficient to ensure the protection of privacy in the digital age. On the one hand, while anonymity can still protect our personally identifiable information, advertisers, governments and social media giants have already found ways around them that, while not threatening our anonymity, threaten the unreachability of users. Anonymity for its own sake has very little value, it is the unreachability that it used to afford that mattered to individuals. On the other hand, the transparency paradox implies that informed consent is nowadays insufficient to guarantee a certain value to our mindless clicks on myriads of consent forms.

3. From the Individual to the Group

The previous subchapter highlighted some of the reasons our current conception of privacy is unable to protect us from the threats that Big Data analytics poses. In this one, we will also interrogate whether an individual approach to the analysis and potential protection of privacy is sufficient. In the digital age, more often than not, the individual is incidental to data analysts. Data is gathered from large and undefined groups of individuals and draws conclusions that we were previously unable to reach. Big Data analytics, as the name indicates, strives for a broader view.

The group, in this case, has to be understood as more than a collective of individuals. Protecting the privacy of the group is only useful if it does more than protecting all the individual privacies of the members of this group. it is only because Big Data analytics threatens something different than simply individual privacy that a debate on group privacy is necessary. While most legislation focuses on the individual and the protection of his potential identification, which has been shown in the previous chapter to be already an incomplete approach to privacy protection, this subchapter will argue further that there is a necessity for a collective approach to privacy.

On the one hand, the expectations that a group can have when their privacy is protected are quite similar to those of an individual. They can expect to act anonymously, to be unreachable from

advertisers, to try different things without the pressure of social norms, to act autonomously and to be treated with dignity. On the other, while the previous expectations are often linked to normative values, the calculation that happens on an individual level when considering the value of their privacy do not function in the same way for groups (Taylor et al., 2017).

Consider a situation where a patient is being asked for his medical record because another patient has a similar disease and more information could be crucial in helping the second patient. The individual calculation for the value of the privacy of the first patient will result in a very different outcome than when taking into account the added value for the second patient. What this means is that the value of the privacy of someone depends on the benefits to others, highlighting here the need for thinking about privacy for groups and not for individuals.

Earlier, Barocas and Nissenbaum argued that informed consent is problematic as a defence for privacy because of the transparency paradox. The clearer these pieces of information are, the more likely people are to read it and meaningfully consent but at the same time this makes the information incomplete and the consent meaningless. This paradox leads the defenders of group privacy to argue that we can not expect all individuals to be aware of every data processing activity and have the necessary knowledge to meaningfully consent to everything they are being asked to. It seems more realistic that a group would be able to carefully weigh the importance of these pieces of information and give informed consent in the name of its members (Taylor et al., 2017).

The philosophical issue that comes up however in the study of group privacy is that method would require to first identify a group then analyse its properties. This would mean that we can not discuss the privacy of groups before we clearly identify which groups we are discussing. However, this is impossible to do in this context as the technology which allows for the creation of those groups also creates the composition of the groups themselves. Sometimes, these fabricated groups overlap with how we view the world as well, for example, teenagers, Christians, football aficionados could all be considered as groups by Big Data analytics but also by any other observant. Most of the time, however, these groups are dynamic and fluid, so not only fixing them in place seems impossible but also useless (Taylor et al., 2017).

While this can be discouraging for anyone building a working understanding of group privacy, it does not have to be. Sure, the group of people who use a certain product each day, or is currently standing on a bus or even the group of people who need new vacuum cleaners is constantly changing, but that does not mean that this group does not deserve to have its privacy protected. In such cases, it is not the composition of the group that defines it but it is the particular property that is being analysed. it is the properties that have to come first in this study in order to meaningfully be able to interact philosophically with that group (Taylor et al., 2017).

As the authors point out: " it is misleading to think of a group privacy infringement as something that happens to a group that exists before and independently of the technology that created it as a group."(Taylor et al., 2017). Technologies such as algorithms or Big Data analytics design the

groups according to the feature of interest they are focusing on, a feature that might not have been chosen by the human analyst. This is called data mining, the study of a pre-existing large database in search of new information.

In a recent conversation with an employee of a data-mining company, he explained that they had analysed a car insurers' database in search of new information. Often, very fast sports cars are quite expensive to insure because of their high price and the added potential for an accident caused by speed. They realised though that a certain type of persons, in this case, male above 50 with stable employment and no prior accidents with the cars were largely overpaying their car insurance. Data mining managed to single out certain customers that were likely collectors and that probably cared for their car extremely preciously. Using that new information, this specific insurer managed to poach members of that specific group from competitors by offering much better prices while still knowing that they were still likely to profit from them. This harmless example shows why these groups are dynamic and that depending on the purpose of the researcher, the composition can drastically change.

According to this and considering the grouping occurs before the group, the methodic requirement that one should first describe a group to then analyse its properties does not apply in this case. This activity of grouping can also be referred to as profiling which can be done by advertisers or governments to target a specific subset of the population. If the profiling is done in a way that violates the privacy of a not-yet composed group or that the goal of this profiling is something that will violate the privacy of the group once-composed, then there is good reason to investigate these practices and denounce them when they are unethical (Taylor et al., 2017). In short, to argue for the protection of group privacy is not to argue for the protection of already determined groups as much as for the protection against unethical techniques used to target these not-yet formed groups.

Technology is blurring the distinction between groups and individuals. Individuals are part of groups that are dynamically created and destroyed constantly by modern technology and, subsequently, it is difficult to discern group rights that are completely separate from individual rights. A group is understood normally as a number of person or things, but in Big Data analytics it is more complicated than that as the study of one person's habits or behaviour can be used to draw conclusions or even predict the behaviour of the rest of the group.

The defining change of Big Data analytics in the study of groups however is in the composition of these groups, as noted above. Groups are traditionally composed of individuals who have explicit ties between one another, whether it be political affiliation, age, sex, employment or religion. Big Data analytics allows aggregation of individuals' data on a scale previously unthinkable. Once the data has been collected, an infinite amount of subsets can be created dynamically from that data. Those subsets do not respond to our traditional categories and are often much more complex and unpredictable than a human researcher could have devised.

The change in policy in regards to group privacy is linked to the two main characteristics of traditional groups that have been lost in the wake of this technological shift in paradigm. First, the traditional groups exist in the members' consciousness. The group is self-aware of its existence and the members know they are part of it, or at least that the rest of society perceives them to be a part of that group. Second, the group is self-proclaimed in the case of an active social group. A passive social group is also possible where the members are treated as a group by society even though they do not identify with it (Kammourieh et al., 2017). In this case, they would still be self-aware but not self-proclaimed.

These groups are often deliberate and possess legal personality, such as the population of a county for example. These groups are the source of legislation, for example, that disallows discrimination on the basis of membership to certain groups. Refugee law, for example, protects individuals persecuted on the basis of their perceived membership to a certain group (Taylor, 2017).

While the focus of our legal system has been centred around individuals, with at its core the Declaration of Human Rights, there is a certain history of group rights. In modern times, the Convention on the Prevention and Punishment of the Crime of Genocide that started after the Holocaust and refers to crimes against specific groups on the basis of their ethnicity, religion or nationality can be considered as a turning point in the history of group rights. In International UN Law, it is declared that the right to reparations may be held by groups who have been targeted collectively (UN Charter, 2017).

Groups have always been created on the basis of commonalities. In the digital age however, these commonalities are not perceived by humans anymore but by computer algorithms in the context of Big Data analytics. At the basis of these new commonalities that can be found between individuals is the exponential increase of data points about human beings. The World Economic Forum estimates that by 2020 we'll have reach 44 zettabytes of data, which is 40 times more bytes than there are stars in the observable universe, or written plainly 44,000,000,000,000,000,000,000 bytes. Every day, 294 billion emails are sent, 65 billion WhatsApp messages are sent, 5 billion internet searches are made, 4 petabytes of data created on Facebook (WEF, 2019). The 2018 documentary "Can you trust your computer?" affirmed that everyday 500Mb of information was collected on each American citizen. As noted in the first chapter, the business models of some of the world's most valuable companies rely on data.

Considering the data points about us multiply, the potential commonalities between ourselves and others do so as well. Big Data analytics refers to two things: this newfound plethora of available data points and the tools that allow for the processing of this data. Without algorithms and artificial intelligence, it is unthinkable to expect human researchers to go through so much data and find these potentially useful commonalities. Through pattern recognition and machine learning however, we can spot correlations that would've been unspottable to the naked eye of the researcher (Kammourieh et al., 2017). These commonalities create these new passive groups (groups that might not know they are groups, lack the self-awareness of traditional active groups).

As these new groups or commonalities between individuals are constantly identified, created and dismissed, the notion of the group becomes blurry and by extension, the notion of the individual within these groups (Kammourieh et al., 2017). In these cases, the anonymity of the individuals does not matter to the analytics and they will still be classified and targeted all the same (assuming their identity has been replaced by a pseudonym or an anonymous identifier).

Then what? What can scientists, researchers, governments, advertisers do with these new groups? How do we define those groups? On the basis of what? Purpose, as noted Taylor earlier, is the main actor in play. Depending on the purpose of the research, groups change.

There are four main ways to identify groups using Big Data analytics. First, data analytics can be used to find out more about pre-existing active groups. In this case, it is not identifying but it allows the researcher to find out more about such group? Second, using certain parameters, we can identify groups that were non-apparent. For example, one could use internet search patterns to identify a new group on the basis of certain behaviour. One such group might be individuals who check Facebook before going to sleep. These unconnected users can then be grouped together to, for example, target them with ads for apps that help better sleep hygiene. Third, we can identify groups but this time without asking for specific parameters. Simply by asking the algorithm to find an interesting or unexpected connection amongst a database. This would be the example of the data-mining firm who found out that a certain subset of people buying sports cars are a lot less likely to get into accidents (Kammourieh et al., 2017).

Finally, the last way of identifying groups might be even unknown to the analyst himself. In the analytics process, algorithms identify groups as a step to further research which is then proposed to the eyes of the data analyst. In such cases, no parameters were dictated by researchers, no mention of a created group has been made to the researcher but the latent group has still been created by the algorithm. This can be particularly problematic as the methods used by the algorithm to create these groups might have been unethical and the end result could be tainted by this process. This can also happen if the dataset was problematic as well (Kammourieh et al., 2017).

In short, the commonalities by which groups have been identified throughout history are increasingly imperceptible details only perceivable to the algorithms that create them and these details are a result of the general paradigm shift in technology of which Big Data analytics is part of. Even shorter, technological innovation is creating groups on the basis of commonalities that are impossible without it and can only be observed by it. The process of group identification becomes difficult to observe for the human eye. This then leads to an epistemic dependence on processes we do not understand (Kammourieh et al., 2017).

However, as privacy refers to personal control over private information, how can that, in practice, apply to groups in a way that is not simply a collection of individual rights to have this control over their information? Is there a justification that allows us to argue that there is a need for group

privacy? There are several situations that allow us to theorize group privacy that is more than the sum of its individual privacies.

First, we've described earlier the phenomenon of the tyranny of the minority that can happen in certain cases. This references instances in which certain individuals can give information about themselves which can be used to infer information about a majority that chooses to safeguard their privacy. In these cases, certain individuals relinquishing their privacy leads to the group's privacy to be threatened.

Second, in Big Data analytics individual privacy is not always enough to protect the interests of all the actors. There are situations in which even though individually the privacy of individuals is protected but possible harm could still be done to them because the privacy of their group is not. The reason for this is twofold. One the one hand, the exponential increase of data created makes it harder for individuals to care for all of it. The data they create is also collected and stored by the data collector, not by the individual himself. On the other, the "raw" data is not that useful by itself, it is only useful when processed by Big Data analytics (Kammourieh et al., 2017). This means that first, the control of the individual over his information is loosening and second, this information is somewhat cryptic and hardly useful if not processed and compared with other users.

These two problems show the necessity for protection of privacy on a group level as well as on an individual one. If we return to the previous definition of privacy as a buffer allowing individuals to control the flow of information about themselves and to differentiate themselves from society, Big Data analytics threatens these core values of democracy even if individual privacy is ensured (which is already hard to guarantee, cf. the earlier chapters on consent and anonymity).

As groups are formed and studied for themselves and not their members, it becomes a necessity to address the issue of protecting these groups' privacy. Earlier, the difference between active groups and passive groups was described, and the task of protecting the privacy of passive groups whose members lack self-awareness of their membership is particularly problematic when these groups are created by algorithms. The ethicacy of the processes by which the data was extracted from these groups and the methods that dictated their compositions need to be regulated on a collective basis and are a different set of interests from individual rights. A good example of such situation is given in "Group Privacy in the Age of Big Data": " Since the outbreak of the conflict in 2011, millions of Syrians have been displaced, either internally or internationally, fleeing their homes in search of safety. Consider the possibility of a town under assault, with groups of residents beginning to flee. The population can be broken down by religious beliefs, known political leanings, law enforcement history, and neighbourhood of residence. The government may have ready access to such information, as well as the surveillance capability to monitor population movements in real-time. Such data might reveal that 5% of the town population left on week one of the assault, that nearly all members of the group belonged to the same religious community, that a significant percentage of them had previously been noted for anti-regime leanings, and that two neighbourhoods of the town are overrepresented in the group. The following week, as conditions

worsen, they are followed by a further 10% of town residents sharing similar characteristics. Such data could easily be used to project population movements on week three, and change the parameters of military action accordingly. It is the analysis of the group as a group that could then allow the analyst to predict the behaviour of the third wave of displacement. It might not be possible to say exactly which individual members will decide to leave next. But the inferences drawn can still conceivably put the group, as a group, at risk, in a way that cannot be covered by ensuring each member's control over his or her individual data. It is in this sense that we can talk of a group privacy interest" (Kammourieh et al., 2017, p.68).

The issue demonstrated here is that Big Data analysts are able to perceive groups that were impossible to perceive previously. it is because of the immense amount of information that the government would have on these citizens that they are able to target these citizens as a group even though they might not do so themselves. This means that on the one hand, they have no legal or political representation that would allow them to hold this government accountable but also that other unknowing members of that group will suffer from this data that is not theirs but might still be detrimental to them.

The authors of "Group Privacy in the Age of Big Data" propose to base the legal framework around group privacy on two key concepts: self-determination and sovereignty. Self-determination refers to the legal right at the core of international law that allows people to decide their own destiny. The definition of people is a bit blurry though as it can refer both to minorities inside a country and protect them from discrimination but it also refers as the people of a country as a whole when they decide to change governments, potentially overthrowing the previous one. it is relevance to group privacy comes from the fact that this right is exclusively for groups and considers groups as a legal entity united around a specific interest (Kammourieh et al., 2017).

Sovereignty refers to the fact that states are only accountable to the rules they have accepted and that no superior authority can force them to accept what they do not want to. When states accept rules, they are then bound to them and they wield some part of their authority. The term is also used to refer to the sovereignty right of people over their own natural wealth and resources (Kammourieh et al., 2017).

Using these two concepts, we can imagine a legal framework centred around these values which would dictate that groups have sovereignty over their own data and that this data can only be used if they've agreed to it. There seem to be two large flaws to this argument.

First, self-determination implies self-awareness. It seems impossible to imagine any kind of self-determination for a group that does not know it is a group. It can not use a right it does not know it has. As we've seen, most groups in Big Data analytics are passive groups, not self-aware. Any kind of legal right has to be wielded by a legal entity, which these groups often are not.

Second, even if there only existed active groups with legal identity, data does not behave like other natural resources. While it is certainly precious, control solely over the ownership of data is not enough to protect privacy. There needs to be a strict control around the analysis of such data to avoid the problems described earlier in group composition and in treatment of these groups.

As the authors note, these rights might protect the privacy of self-aware active groups, but certainly not of the numerous passive groups constantly dynamically created by Big Data analytics. They then advocate in those cases to focus on a different point of the data collection process, namely the analysis and targeting stage. If a group can not control the collection process, regulation has to be put in place to protect the interests of that group at these two stages by regulating the use of their data with a focus on the safety of the data subjects (Kammourieh et al., 2017).

4. Conclusion

This chapter has proposed three main lines of criticism around our modern understanding of privacy. While the first criticised privacy outright and questioned its very desirability, the second and third start from the assumption that privacy is a good thing that needs to be protected. However, both criticize how we think today about privacy and show that the tools and the scope of our privacy protection initiatives are not capable of protecting our private lives in the digital age.

The next chapter will attempt to show that simply updating our tools and changing the scope of our conception of privacy will not be enough however to meaningfully protect privacy. While privacy is compatible with capitalism, the particular form of surveillance capitalism promoted by the tech giants is not. In short, even if we were to decide that privacy is desirable, significantly improve technologies ensuring anonymity, managed to bridge the transparency paradox and adapted our conception of privacy to include groups, even ones lacking self-awareness, surveillance capitalism and the modern logic of our economy are simply incompatible.

Chapter 2. Privacy and Capitalism

1. The Economical Value of Privacy

In our modern economies, privacy is chastised for slowing down the free market. In what is often called the information economy, an economy with an emphasis on informational activities, privacy hides some of that information and hurts overall productivity and the capacity for prediction. Prediction is particularly financially profitable because it increases efficiency in the economy. As US Senator Marsha Blackburn noted in a 2010 Congressional hearing: “What happens when you

follow the European privacy model and take information out of the information economy? Revenues fall, innovation stalls and you lose out to innovators who choose to work elsewhere" (Sadowski, 2013).

These problematic facets provide a negative view of privacy. Under this view, privacy is a tool we use to protect our personal information from prying eyes but, when this personal information can help the public good, we should disregard privacy and share this information. In this instrumental view, privacy is a very costly luxury that slows down innovation and potentially detrimental to the public good. While this is not the view that this thesis will defend, it is very useful to describe the arguments that back it.

There's no simple answer to the question of the economic impact of sharing personal information. Privacy as a bad reputation in economics. At an aggregate scale, it is the accumulation of data about individual preferences that allows for the production to be optimized in a way that best answers the needs of consumers. This greater efficiency results in the market generating the most value at the lowest cost. This benefits society as a whole, so some of that value necessarily has to return to the individuals sharing their data. This has led researchers such as George Stigler to argue already in the 1970s that excessive protection of privacy may result in inefficiencies in the market (1971).

This can also apply at the individual scale: concealing personal information could result in a transfer of costs to the other party, using the example of recruitment where the employer, lacking enough information about the candidate, would bear the cost of inefficient hiring (Posner, 1981).

More often, at the individual scale, when a consumer shares personal information, he puts himself at a disadvantage in terms of bargaining power: he discloses data that may allow the supplier to infer his needs, his financial means and, ultimately, the maximum price he's willing to pay for the goods or service he's interested in. So this data imbalance may result in the value mostly remaining in the hands of the party with the information advantage: the supplier.

This is the "redistributive effect", the fact that accumulating more information beyond what's needed for market efficiency will result in an advantage for the one gathering the data (Hirshleifer, 1971). In other words, sharing data creates value but sharing too much data transfers too much power to the firms collecting it. To economists, this typically sounds like something that should balance itself out in a free market, consumers naturally tending to share "just the right amount" of data to maximise social benefit. In a fair market without uncertainties or transaction costs, such an equilibrium would be reached, thus making privacy regulation unnecessary (Noam, 1996). Even in a less than perfect market, research from Acquisti and Varian (2005) showed that consumers would expect for their behaviour to be "tracked" and adopt behaviours that made this tracking inefficient unless they found that the firm was using this data in a way that brought them a personal benefit.

In other words, consumers understand (more or less explicitly) that they give away value when sharing personal data but they may choose to still do it if results in a benefit to which they attribute an equal value. A typical example is online services such as social networks, on which large amounts of personal data are disclosed and shared with the service provider, in exchange for the free access to that service.

Numerous research has attempted to put a monetary value on consumer's private data, and the results demonstrate a high variation linked to the context and the type of data that's being shared. Furthermore, even consumers that report themselves as privacy-conscious turned out to be as willing as others to trade privacy for convenience and discounts (Spiekermann et al.,2001).

This "privacy paradox" is partly explained by a number of factors. First of all the lack of transparency: the customer may not know how much of his information is being captured (for example when his activity on a website is being tracked) nor when it is being used (for example when an ad is displayed based on an item he's viewed previously). He also may not know the value of that information that's been collected about him. A second factor is the lack of influence: the customer is not always in a bargaining position. Often, it is more a choice between sharing information or not using the service at all. While the option to opt-out might be given, the costs to do so are often too heavy for the consumer. Finally, consumers are subject to biases, for example, consumers may overestimate the immediate benefit while discounting the potential risk (for example the risk of being subject to identity theft) (Rabin and O'Donoghue, 2000).

All this further reinforces the above-stated imbalance: there is an incentive for "suppliers" to collect more data and a lack of "resistance" from consumers, who tend to insufficiently value the personal data they are sharing. Beyond the amount of data that will ensure market efficiency, consumers tend to disclose "too much" in exchange form insufficient benefits.

So the question becomes: is there a right amount of sharing or, even better, a right way of sharing, that optimizes the market benefits without disadvantaging the individuals sharing their data? And, if the market will not self-discipline towards this "right way", should regulation intervene?

In terms of "right amount", economists disagree on where the benefit of consumers ends. Lenard and Rubin for example, argue that any legal constraint on the amount of personal data that can be used by businesses would ultimately hurt the consumers themselves (2009).

In terms of a "right way", progress in analytics and Big Data technology have introduced multiple new privacy-enhancing techniques that may lead to ensuring most of the benefits of data usage while still protecting the privacy of individual consumers. There seems to be matter to discuss with this affirmation though.

As to the question of whether the market will self-discipline towards those new privacy-enhancing techniques, the answer lies in the value consumer estimate for their personal data as well as their

ability to influence the companies using this data. The more aware consumers are of both the value of their data and the risks associated with sharing it, the more they will be willing to use their power to influence the market. And the more this power exists in the hands of consumers, the more the market will evolve in a direction that is more respectful of their interests. The minimal role of regulation should be to ensure that consumers can influence the market with their choice, ideally, in a more granular way than the current "take it or leave it" proposition they face today with some online services acting in a dominant position (Acquisti, 2014).

2. Privacy and Surveillance Capitalism

In her new book “In The Age of Surveillance Capitalism”, Shoshana Zuboff argues that, further than the aforementioned privacy paradox, the rise of surveillance capitalism is making privacy a luxury that our modern economies not only can not afford but most importantly must destroy in order to pursue its goals. She defines surveillance capitalism as an advanced form of market capitalism. According to her, capitalism constantly evolves and claims things outside of the market dynamic and bringing them inside. This process of commodification allows these things to be sold and purchased. Surveillance capitalism emulates this pattern with private human experience and repurposes it as a source of raw material for production, sale and prediction. To do so, human experience is translated into behavioural data which is used to improve products and services. She describes the behavioural data that is not useful to this as behavioural surplus, valued for its predictive signals. This behavioural surplus is traded in a new kind of market, the behavioural futures market, that focuses on the prediction of human behaviour (2018).

Zuboff’s example of the first of these prediction products was invented by Google and named “click-through rate”. This predictive tool allows Google to see how many users clicked on ads. Coupled with Google’s targeted advertising business model that linked search queries from their users to ads, these tools allowed Google to build one of the world’s most valuable company.

Zuboff argues however that prediction is not bad in itself. In the year 2000, data scientists invented the Aware Home. The Aware Home would be an automated house capable of being commanded but also reacting by itself to certain situations on the basis of human commands or information picked up by context-aware sensors. This Aware Home would function in a closed-loop, a direct line between the user and the devices in his house producing the data. This personal data would be used to facilitate his life, for example by raising the temperature when the sensors determined it was necessary based on the previous behaviour of the user. Previous instances where the temperature dropped below twenty degrees and the user had asked for more heating would be studied and the home would automatically do so in the future while respecting the privacy of the user (2018).

This sort of project has now been piloted by Google with its Nest project. Nest allows users to control security, heating, music, lights, household appliances and all the rest of the connected

Internet of Things machines in the user's home. Zuboff reports that users agree to around a thousand privacy contracts when they install a Nest in their home. All sorts of data in their house is then sent to Google which sells this data to third parties, with the consent of the user. She argues that this consent is misinformed due to the complexity of the privacy agreement (the transparency paradox described in chapter 1) but also because Google limits the functionality of their products to users that do not agree to their data being shared.

While the functionality of both projects is the same to the user, the main difference is in the relations at play in surveillance capitalism. While for market capitalism the Aware Home is enough to fit a classic business model, for surveillance capitalism it's the collection of the behavioural data surplus that is the most profitable enterprise. Surveillance capitalism turns the line between user and product into a triangle where data about the interaction of the other two is stored, analysed, sold and used by the company (Zuboff, 2018).

This behavioural surplus data does not have to be relevant to the product that collects it either. Often, Zuboff argues, the product sold is incidental to the business model. Google's operating system for phones Android is free to install because its business model relies on capturing as much behavioural data as possible. As internet use became mobile, Google had to rethink its main supply chain of raw behavioural data and smartphones were the perfect support to enter the pockets of billions of new users. Through Google's free services such as Android and Google Maps, they managed to create new plentiful sources of behavioural data including the particularly lucrative geolocation data (2018). Mapping users allows for better-targeted advertising and movement also ensures that the users targeted are real humans and not bots.

Even more impressively, Google made its operating system Android open-source, which allowed any developer to create apps for Android users. Once a good number of these apps were developed, Google bundled them into the Google Play store. For phone manufacturers to have access to the Google Play Store, they have to agree to install by default on all their phones the rest of Google's services: the predictive data machines that are Gmail, Youtube, Google Maps etc...

The last step in this process, Zuboff argues, is to directly intervene in people's decision making processes. While predictions always have the potential to be wrong, intervention in the life of users is the most secure way to guarantee outcomes. These predictions are designed to incentivise users, nudge them into modifying their behaviours without them realising it, whether it be by inserting a certain phrase in a Facebook feed or, she proposes, "by shutting down your car engine when insurance payment is late" (p.326, 2018).

One might ask if this is truly a break from the complete realisation of advertising. Advertisement marks the shift from fulfilling needs to creating wants, so is surveillance capitalism truly doing something different than what advertisers have tried to do for decades? To understand the difference between an advertisement and incentivising, a critical assessment of what incentives actually are is necessary.

Ruth Grant asks in "Rethinking the Ethics of Incentives" how to make an ethical distinction between legitimate and illegitimate forms of incentives. Traditionally, incentives are viewed as a form of trade. Indeed, he argues, some incentives are benign. Placing vegetables at the start of the line in school cafeterias or saving a lane for carpoolers for example. Other incentives can be purely evil though, as in for example rewarding violent competitive football players who injure the other team. Some of them are grey areas though: to stay in the domain of Big Data we could imagine Google monetarily rewarding users who share all of their personal data, the Chinese government attributing points to their citizens to reward social behaviour or humanitarian organisations offering aid to vulnerable populations but demanding information.

Grant argues that the most prevalent way to think about incentives is as a form of trade. In that case, the only thing that should matter to ensure that the incentive and by extension the economic exchange is ethical is whether both parties voluntarily participated. If they did so, it must mean that both parties are subjectively better off from the exchange and the trade is ethical. Voluntariness is the only ethical standard in that case (2015).

Grant's argument, however, is that incentives are forms of power more than forms of economic exchanges and in such, the ethical concerns are more complex than simply voluntariness. Bribery for example is a voluntary exchange where money is offered as an incentive but it is certainly not ethical. According to him, incentivising someone is more than gently nudging them towards a more profitable decision, it is abusing an asymmetry of power. While it is not illegitimate per se, it is necessary to study the legitimacy of all kinds of power relationships to differentiate when benign encouragements from abuse of power. This allows a shift in responsibilization in incentive situations. Considered as trade, the responsibility to accept or reject an incentive is on the shoulders of the individual. Considered as power, the responsibility lies in the legitimacy of the power and the motivations of the powerful incentiviser.

Grant proposes three ethical questions that should be answered by each relationship of incentives. Does the incentive serve a legitimate purpose? Does it allow for a voluntary response? Does it affect character positively or not at all (p.367, 2015)?

If we take the example of Google's Nest project, we can see in action how Grant's view of incentives allows us to pinpoint what is unethical about Google keeping part of the functionality of this product unavailable to users who do not wish to share their personal data with third parties. If thought about as a relation of trade, the voluntariness of the user to use this product is enough to argue that this incentive is legitimate and the trade is ethical. If we think about it from the point of view of power relation, then the abuse of Google's power is identifiable with Grant's three questions.

First, the purpose of the incentive is to make sure clients agree to Google's abusive privacy policy. Zuboff reports that researchers have shown that refusing to share personal data with third parties

by refusing to agree to Google's privacy policy can lead to "frozen pipes to failed smoke alarms to an easily hacked home system" (p.18, 2018).

Second, it is hard to argue that users' agreement to Nest's privacy policy is voluntary. While their agreement to bringing Nest into their homes might be voluntary, it's the agreement to the privacy policies which share personal data that is not voluntary. Any definition of voluntary necessitates that at least two options are available and that none of them be unreasonably difficult to choose. It seems in this case, choosing not to sign these agreements is particularly problematic.

Third, the effect on character can not be described as positive as it threatens the privacy of the user. While the comfort afforded by such technologies might be beneficial, the resulting loss of privacy has negative effects on the autonomy and agency of the user.

3. Consequences of Surveillance Capitalism

In the above chapter, we've shown one of the ways in which surveillance capitalism departs from advertisement. Incentives, instead of informing us about certain products in an effort to sell them in a trade relation, supply extrinsic reasons to make a certain choice sometimes unethically by abusing a power asymmetry between the incentiviser and the incentivised. However, Zuboff argues that there is another argument that shows that surveillance capitalism departs from the traditional tools of market capitalism.

As noted earlier, surveillance capitalism shapes and modifies human behaviour in a direction that increases its predictability. While the marketing industry also tries to modify behaviours to push individuals towards certain decisions and indeed, persuasion is nothing new, Zuboff argues that the change lies in the fact that it has become impossible to avoid interacting with surveillance capitalism. All everyday activities have been commodified in a way that behaviour data is gathered. At the same time, an increasing amount of time is spent by children and adults alike online as it has become an indispensable tool for social participation. This ties into her previous argument that surveillance capitalism strives to commodify as much of human experience as possible and turn it into behavioural data. And, the time we voluntarily spend on the internet is interacting socially in these modern supply chains of data that are being designed by some of the most valuable companies in the world. These companies spend billions ensuring that individuals do not realize they're providing this almost infinite supply of the most valuable resource of the information age.

Most individuals are unaware that they are participating in this process which is why Zuboff considers this to be an attack on our autonomy and sense of agency. She argues that Google disregards the boundaries of private human experience, essentially bypassing entirely privacy and "the moral integrity of autonomous individuals" (p.36, 2018). This usurpation of individual decision rights leave the question of privacy far behind as the distinction between private human

experience, social interactions and self-authorized surveillance and commodification of behavioural data becomes inexistent. Privacy, while not a direct target, is a casualty of the lack of decision rights that result from this interaction. How can one agree to something they do not know about? How can anyone make a conscious decision about the flow of private information about oneself when autonomy and the awareness of that decision itself is bypassed.

The work of french technical philosopher Bernard Stiegler revolves around his conception of technology as *pharmakon*. *Pharmakon* is an ancient greek word that means both poison and remedy depending on the context of its use. His understanding of technology as *pharmakon* underlines the category error Zuboff also warns against. Confusing digital technology and surveillance capitalism is not useful because it can lead to a fear of technology that is counter-productive for humanity.

Zuboff argues that the problems that threaten humanity, from the climate crisis to poverty, desperately need technology such as Big Data analytics to find solutions. However, according to her, those technologies have been diverted by surveillance capitalism's economic logic. In her words, we should focus on the puppet master, but not the puppet. Surveillance capitalism is dependent on certain technologies but equating those two is wrong. Surveillance capitalism is an economic logic that takes possession of these technologies and uses them to its ends.

When Google claims that its search engine conserves informations on their users, they play into the common misunderstanding of conflating the technology with its economic logic. The search engine does not need to conserve this information to function but other Google projects can use it to build more predictive models and accumulate data on users. Google is very happy to claim that this is a technological inevitability, a logical continuation of capitalism but Zuboff argues that technologies are economical means that can be oriented in whatever direction society decides it to be which amounts to the previous definition of technology as *pharmakon*.

To Zuboff, the direction that is taken now by these technologies is clear. As most of the world's data scientists work in Silicon Valley for Google, Facebook or Amazon, as millions of predictions of user behaviour are produced by these companies, as the computational capabilities necessary for Big Data analytics belong to these companies and as the data we create using these websites is not protected by any law and is the proprietary data of these companies, there is no doubt, according to Zuboff, as to whom decides of the direction of this technology and benefits from it (2018).

While commercial abuses are certainly problematic, the massive harvesting of behavioural data also threatens democracy as was shown with the scandal around Cambridge Analytica. The model is similar, accumulation of behavioural data and information points about individuals, around four to five thousand (p.451) per individuals they claimed, allowed the British consulting firm to engage in micro-behavioural targeting and intervention in individual decision making. Just as commercially, the paroxysm of efficiency in prediction was to actually intervene in individuals decision making, the consequences of adapting this business model to politics are simply

incompatible with democracy. The capabilities developed by surveillance capitalism in what Zuboff describes as a lawless space over the two decades since the start of Google's targeted ad project were deployed in full force associated with behavioural psychology to serve political outcomes to arguably devastating effects in the Brexit vote and the 2016 US presidential election (2018).

The following quote from Chris Wiley, the Cambridge Analytica whistleblower is particularly telling as to the risks to society that such capabilities afford: "I think it's worse than bullying, because people do not necessarily know it's being done to them. At least bullying respects the agency of people because they know... if you do not respect the agency of people, anything that you're doing after that point is not conducive to a democracy. And fundamentally, information warfare is not conducive to democracy."(Cadwalladr, 2018). Agency is impossible without awareness and without awareness, there can be no privacy.

Following this diagnosis, Zuboff argues there are two ways of fighting surveillance capitalism. First, it should be illegal for private companies to gather data unilaterally and in such secrecy on their users. Certain domains of human experience should be off-limit for capitalism. Sectors such as public health, childcare or social interactions should not be used to create predictive models. This, she argues, is not a debate about data ownership, it is an affirmation that data on such human experiences should never exist in the first place. Certain classes of human experience must be protected from all commercial interferences. Second, markets that trade in human futures should be banned. Whether it is for commercial purposes or political ones, playing with human autonomy should never be allowed. Threats to the autonomy of individuals are threats to democratic society as a whole.

One might still ask Zuboff how to repurpose technology in a way that is beneficial for society and while this transition is happening how society can still harvest the formidable power of Big Data analytics. She argues that truly informed consent can be a solution and that prudence when it comes to the use and analysis of our data is to be recommended (2018).

Finally, Zuboff recommends that regulation over forms of surveillance capitalism should come swiftly. As time passes, the so-called tech giants grow larger and more powerful by the day and breaking these monopolies is becoming extremely urgent as this task will be more complicated the longer legislators wait. She argues that the tech sector is incapable of self-regulation due to its business model being reliant both on growth and on the increasing commodification of more and more human experiences (2018).

4. Conclusion

In summary, it seems very hard to reconcile privacy with the logic of the free market. As shown in the first subchapter, the informational asymmetry naturally created by the privacy paradox ensures that, as long as consumers continue to negatively evaluate the benefits of their privacy, there will be very little reaction from the markets to self-regulate when it comes to privacy matters. This idea has been shown in action scandal after scandal and is demonstrated by the underwhelming reaction of Facebook in the aftermath of the Cambridge Analytica scandal. While they were heavily criticized for their lacklustre privacy policies, their growth was not meaningfully impacted by a public underestimating the value of their privacy ((Cadwalladr, 2018).

The second and third subchapter insisted on the logic of the market and its tendency to commodify as much as possible coupled with the invasiveness of behaviour analytics which results in a threat to human agency itself. While the previous chapters argued over threats to privacy, a common theme can be found between the ethics of Big Data analytics on groups lacking self-awareness and the consumers in surveillance capitalism. In both cases, the debate over privacy seems to take a backseat.

If we understand privacy to be control over the flow of one's own information, it logically implies and even necessitates that the person or the group knows that the flow of information is happening in the first place and the extent of this flow. After the Cambridge Analytica scandal, the Time's leading technology writer wrote an article titled " I Downloaded the Information That Facebook Has on Me. Yikes". In the article, he explains he had no idea how much data Facebook had on him and was shocked by the number of companies this data had been sold to. If even the leading technology writer of the *Time's* was dumbfounded by the amount of personal information being sold and shared without his explicit permission on the internet, one can only imagine that on a collective level, we severely underestimate the ubiquitousness of Big Data analytics and surveillance capitalism. It is clear that one of the challenges of this decade is improving data literacy.

Chapter 3: The Future of Privacy

In the two previous chapters, this thesis has demonstrated that our approach to privacy is clearly problematic. Not only scholars question the desirability of privacy, the effectiveness of its tools and the validity of its focus on individuals before groups but the logic of our modern economy, defined by Zuboff as surveillance capitalism, seems to be downright incompatible with privacy.

This chapter will offer answers to previous criticisms, avenues of reflexion and potential solutions to these issues and provide guidelines as to how privacy should be protected and more importantly why it is so important.

1. A New Theory of Privacy

As seen in the very first chapter of this thesis, certain scholars such as Heidi Anderson criticize privacy and more precisely obscurity as something that is not desirable in society. While it certainly has upsides such as the guarantee of truly free speech, she argues that the cons outweigh the pros and the transparency and accountability resulting from loss of privacy is likely to benefit all in the long run. This argument rests on a conception of privacy that is mistaken. This understanding of privacy, in this case, is as a protection, as nothing more than secrecy around one's actions. A better comprehension of privacy is given by Julie Cohen in "What is Privacy For?".

Privacy shelters individuals from the forces of governmental and commercial actors that are actively trying to predict, monitor and standardise the population. Without privacy, she argues, there is no self-determination (Cohen, p.1905, 2012). She argues that there is no liberal free self that is sheltering himself in privacy. To have any kind of freedom, there needs to be subjectivity which is exactly what is at risk if we disregard privacy.

In liberal political theory, the idea that the self is autonomous and privacy acts as a sort of protection around it is predominant. In this view, privacy can only be seen as a defence mechanism, it is reactive only. However, Cohen argues that in the real world, however, privacy choices are heterogeneous and unruly and cannot be easily schematized (Cohen, 2012). She notes that we might share certain information with a stranger sitting next to us on a flight that we might not share with close friends. Her criticism of liberal political theory understanding the self as naturally autonomous and gifted with some pre-cultural core is based on the idea that we are constantly situated in culture and in social contexts from the moment we are born. There is no autonomy that transcends these, just as there is no privacy that is a fixed condition as we are always subjective beings being thrown into new situations and forced to relate to them dynamically (Cohen, p.1908).

Cohen draws from social psychology to illustrate how individuals, as they construct their subjective relationship with the world around them slowly build their own personal differentiation and their own unique subjectivity (Cohen, p.1909). This Heideggerian view of the self as a *Dasein*, a unique subject always embedded into a social context is central to developing a proper conceptualisation of what privacy is and why it is so important. The subjective Dasein is always part of a social moment in which he builds his subjectivity by differentiating himself from the rest. This is the process that is at risk when privacy is threatened.

Cohen uses Foucault's postmodern concepts to propose what she refers to as a postliberal theory of selfhood. Her position is between postmodernism and classical liberal theory of selfhood. In this understanding, our identities are more or less fixed which means that there is a self irreducible to social shaping but this self is also malleable, emergent and constantly differentiating himself (Cohen, p.1909). In this view, all individuals are emergent subjectivities that are influenced by

social and cultural norms but not suffocated by them. They can also decide on new original ways of positioning themselves against or in the margin of these social codes in a process of differentiation that allows for personal autonomy and agency (Cohen, 1910). Cohen's approach is interesting because it argues that this irreducible self can conduct his own personal appraisal of the liberal model with all its flaws and virtues without outright rejecting or embracing it.

A truly independent and free liberal self is unrealistic in any society, but a *Dasein* thrown into situations and having to use its reasoning to decide what he wants to associate or dissociate, with the caveat that he will never have complete information about any choice he can make, is a more realistic formulation of the self. These qualities of judgement are necessary to allow individuals to pursue self-fulfilment and the creation of their own unique personality (Cohen, 2012). The importance of this with regards to privacy is that, according to Cohen, this critical subjectivity can only exist if privacy can protect the interplay between social shaping and the emergent self. Without privacy, there is no breathing room for this emergent self to reflect and judge of its surrounding norms. In a previous article, she argued that "Privacy's goal is to ensure that the development of subjectivity and the development of communal values do not proceed in lockstep" (Cohen, 2012).

Part of the reason why privacy has been tossed aside for better efficiency in the last few years has to do with our poor understanding of the benefits privacy affords. Technological innovation and in particular Big Data analytics has changed the way in which we share, collect, store and analyse information. These changes have created a necessity for an updated theory of privacy from two angles.

We must redefine the values that privacy protects in order to justify its importance. Very often, privacy is described as the enemy of information which, in an information economy, gives it a bad reputation. This liberal vision of privacy limits it to secrecy but a postmodern vision of privacy shows that extends beyond secrecy. In a world where we are constantly assailed by commercial actors, cultural and social norms or government surveillance; privacy is what allows us to constitute and differentiate our emerging subjectivity.

This postmodern understanding of privacy allows us to answer different version of the classic argument "privacy does not matter if you've got nothing to hide" often used by governments to justify their surveillance programs. This argument common in the public sector, as US Majority Leader Trent Lott said in 2006 "What are people worried about? What is the problem? Are you doing something you are not supposed to?" (CNN, 2006). But we can find this argument as well in the private sector with, for example, Eric Schmidt who was CEO of Google at the time and declared "If you have something that you do not want anyone to know, maybe you should not be doing it in the first place" (Esguerra, 2009).

The right to privacy is one of the cornerstones that guarantees the right to self-determination and autonomy. Under constant control and constant pressure, emerging subjectivities are unable to

differentiate themselves and to constitute themselves as a unique person. Accepting the "nothing to hide" argument would suggest that human evolution is over, that no one can be or try something different that might be socially frowned upon today. Understanding privacy through this view explains the reason why privacy is so highly regarded as a right, not for the secrecy it provides but for the freedom of speech, thought and democracy that it ensures. Without privacy, there is no agency, without agency there is no free will and without free will, there is no democracy. Privacy is the right to be let alone, the right to be unreachable and in that breathing room allowed, develop yourself under your own terms.

This view of privacy is compatible with Nissenbaum's theory of privacy as contextual integrity which has been used throughout this thesis. While Nissenbaum's view argues that privacy refers to the control of the flow of information about oneself and this postmodern theory sees it as the necessary breathing room that allows for self-development, these two claims can coexist. Both are opposed to a theory of privacy as secrecy, and while the first focuses on how exactly privacy operates and what our right to privacy actually is while the second focuses on why privacy is necessary.

Nissenbaum argues that while the contextual informational norms underlying her theory of privacy are never fixed, they are undergoing a disruptive discontinuity caused by the rapid infiltration of digital information technologies "into virtually all aspects of life" (p.231, 2010).

2. The Privacy Paradox

As described in the second chapter, the privacy paradox refers to the fact that while users claim to care about privacy, they behave as if they did not. In literature, for example, the loss of privacy is a staple in dystopian science fiction novels such as George Orwell's "1984" or Aldous Huxley's "Brave New World".

Several experiments have shown the existence of this paradox and demonstrated the irrationality of individuals when it comes to the gap between their perceived evaluation of privacy and their actual behaviour. In a recent experiment during which subjects were asked to download certain apps, researchers discovered that users value the cost, the ratings, the reviews, the graphics, the functionality and the design of an app higher than the requested permissions when deciding whether to download it (Barth et al., 2019).

As demonstrated earlier, users tend to economically underestimate the value of their data. While trading privacy for functionality could be understood as laziness, the theory of ethics of incentives developed in chapter 2 shows that these trades are not done voluntarily. If the incentive fails to satisfy Grant's three requirements - Does the incentive serve a legitimate purpose? Does it allow for a voluntary response? Does it affect character positively or not at all (p.367, 2015)? - then the

privacy paradox really is not one. In reality, we do care about privacy but scholars have also underestimated the power of incentives. We live in a time where much of social life is spent online, can we truly consider a young adolescent creating a Facebook profile as acting irrationally?

As argued by Zuboff, the ubiquitousness of surveillance capitalism can explain its dominance on the market and in our increasingly commodified lives and experiences. While individuals might want to do more for their privacy, they also realise that they want to take advantage of free services on which social life as a whole has become increasingly reliant. This does not detract from the fact that data literacy has to be improved as well in order to guarantee that users truly understand what is at risk.

3. Beyond Privacy

One of Zuboff's metaphors for privacy was used in the introduction. When her house burned down, she remembers running upstairs and closed the doors to protect the rooms from smoke damage. Sadly, her house burned down completely. She explains in her book the lesson she drew from that traumatic event: "The danger of closing doors to rooms that will no longer exist is very real. The unprecedented nature of surveillance capitalism has enabled it to elude systematic contest because it cannot be adequately grasped with our existing concepts. We rely on categories such as "monopoly" or "privacy" to contest surveillance capitalist practices. And although these issues are vital, and even when surveillance capitalist operations are also monopolistic and a threat to privacy, the existing categories nevertheless fall short in identifying and contesting the most crucial and unprecedented facts of this new regime."(p.29-30, 2018).

For Zuboff, our privacy can not coexist with surveillance capitalism. Trying to protect privacy now would be closing a door while society is on fire. In her view, surveillance capitalism is leading society to a totalitarian future as the economic inequality resulting from surveillance capitalism following a canvass she compares to the domination of nature starting in the industrial revolution.

Ever since industrialisation, humans have increased their control over nature for the sake of development, growth and human betterment. We only now realise the consequences of industrialisation and the negative effect it has had affecting the delicate balance of our planet. According to Zuboff, the aim of this generation is to now dominate human nature. Machines and software try to modify human behaviour in the service of market objectives (p.828, 2019).

She argues that "We are expected to cede our authority, relax our concerns, quiet our voices, go with the flow, and submit to the technological visionaries whose wealth and power stand as assurance of their superior judgment."(p.829, 2019). While clearly the main issue she demonstrates is the loss of autonomy, it does not seem that privacy is simply a door in the house on fire.

Her rejection of privacy is not a rejection per se. She never argues in her book that privacy is useless, but she does imply that it is a secondary concern compares to what she believes to be the loss of our autonomy and the end of civilisation as we know it. This hinges on a conception of privacy that is insufficient and does not recognize that privacy is effectively the only way to regain some of that autonomy.

It is because, as seen in a postmodern view, privacy allows us detachment from the constant aggression of advertisement, intrusion of government and ubiquitousness of surveillance capitalism that we can regain some kind of authorship of our own lives. Privacy is not a room in a house on fire, it is the lightning rod that protects the house.

The first step of regaining ground against surveillance capitalism according to her is informing public opinion. An important part of informing public opinion is increasing data literacy and spreading information on how best to protect privacy. Fighting for privacy and against surveillance capitalism go hand in hand as in, after all, it is only because companies are allowed to gather so much behavioural surplus information of their unaware customers that Big Data analytics systems can thrive. Only by protecting privacy can we starve the beast that is surveillance capitalism.

Conclusion

As pointed out in the introduction, privacy is a messy concept. As put by legal scholar Arthur Miller: “privacy is difficult to define because it is exasperatingly vague and evanescent.” (Solove, 2008). Defining privacy also requires an interdisciplinary approach. Any philosophical conceptualisation of privacy will have great influence over the legal framework put in place around it. The task of protecting privacy and building a legal framework around it is particularly sensitive to the philosophical issues that have been raised in this thesis. Additionally, privacy is now also understood in the logic of market objectives. Without understanding the economic impact of privacy, it is hard to meaningfully offer recommendations and a diagnosis of where privacy stands in society. Finally, a philosophical inquiry is necessary to determine the cause we serve when we protect privacy. As noted in the introduction, much of civil society seems to agree that privacy is important. Nevertheless, as demonstrated by the privacy paradox, these opinions do not seem to translate to actual consumer behaviour. Amongst the culprits for this irrationality is our misunderstanding of what we are actually protecting when we protect privacy. As explained by Robert Post: “Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.”(2001). It is only by keeping all of these dimensions in mind that we can arrive to a worthwhile discussion on privacy in the digital age.

Defending privacy does not mean banning Big Data analytics outright. An interesting avenue of reflexion which could complement this thesis is the devising of a model which helps differentiate cases where Big Data analytics is destructive and where it is helpful. Obviously, the distinction is not as easy and the fear of misuse of technology can lead to missed uses in which it could've been beneficial. The task of such a model would be to predict in which cases Big Data analytics can be beneficial.

I chose to base this thesis on Helen Nissenbaum's theory of privacy as contextual integrity. Volatility is an intrinsic component of privacy and explains the headache it has caused to philosophers and legal scholars in the past. In the theory of contextual integrity, privacy is based on informational norms themselves based on ethical values and key organising processes of social life. As these processes and our values change, it becomes inevitable that we find our conceptions of privacy poorly adapted to the digital age. This can be explained by the sheer speed of these changes and the rate at which information technology is changing all aspects of information flows.

This thesis set out to clarify and articulate the threats to our privacy and propose a better understanding of the stakes of privacy. The value in this exercise is the clarification of these stakes which in turn can influence policy. As noted by Daniel Solove: "The difficulty in articulating what privacy is and why it is important has often made privacy law ineffective and blind to the larger purposes it must serve." (p.12, 2008). For example, while the GDPR is certainly a step in the right direction, the discussion around informed consent in the first chapter shows that multiplying requests of permissions to users when they access websites can never be sufficient protection of privacy.

The tools that privacy has at its disposal are ineffective at fighting the behaviour prediction machine that surveillance capitalism has built itself. Without a second thought, most citizens agree to entrust all of their private information to Google and Facebook. We tend to consider this transaction as voluntary trade. Trades are ethical simply on the basis of voluntariness. If both parties wanted to proceed, then it is ethical. However, in the second chapter, it was demonstrated that incentives should be understood as a relation of power when a sufficient asymmetry of power was at play. Facebook and Google are abusing their position of power in the market to force users to accept their terms and conditions blindly.

Zuboff describes this phenomenon as a break from the rest of capitalist theory in that they both require freedom and knowledge. The bedrock of capitalist theory is that on the one hand markets are intrinsically unknowable and on the other that the ignorance produced by the lack of knowledge requires complete freedom of action for market actors. In turn, this ensures that "The individual actions that produce efficient markets add up to a staggeringly complex pattern, a mystery that no one person or entity could hope to know or understand" (p.798, 2019).

However, Zuboff argues that this is not true anymore when it comes to surveillance capitalism. According to her, markets are no longer invisible to the tech giants and the invasion of our privacy

which extends so far as the prediction and influence on our behaviours has led to the breaking point of the capitalist model. It is because privacy has been breached that society is tending towards this totalitarian model described by Zuboff. Markets are not intrinsically unknowable anymore, as described in Adam Smith's Wealth of Nations, and total information has allowed total prediction through Big Data analytics and at its peak, total prediction results in control and the loss of human agency (2019).

There is no way around governmental regulation. There can not be in our economic model an actor that is both omniscient and completely free. The topic of regulation of internet giants is also marked by the clear conflict of interest created by the ubiquitousness of these systems that have made the digital world the theatre of these important societal debates. Facebook has become hugely influential in the democratic process and shows no sign of slowing down. While using a knowledge advantage in a competitive marketplace is nothing new, the one wielded by surveillance capitalists is unprecedented.

To answer the original question of this thesis, privacy can survive in the digital age but with major conditions. First, privacy has to be understood as an evolving concept based on the changing informational norms which themselves are based on changing ethical values. Understanding it as a fixed concept can only lead to a privacy policy that is blind to the larger values it is supposed to protect. Second, reliance on informed consent and anonymity can not be the only defence of privacy as both of these can be easily fooled and even when they ensure anonymity, fail to protect the unreachability of individuals. Third, the focus of privacy policy has to shift from the individual to the group, as the individual is often incidental to Big Data analytics with a special focus on preventing computer programs to create groups without any human input and potentially discriminating against these groups, unaware of their own existence. Fourth, as explained in longer detail throughout this thesis, the informational asymmetry created by phenomenons such as the privacy paradox and the tyranny of the minority have to be offset both by regulation and greater data literacy. Finally, for privacy to regain its important central place in a democracy, it must be understood widely as more than secrecy. Conflating the realms of the private and the secret have led to the attacks on privacy and the famous "nothing to hide, nothing to fear" arguments. Promoting a postmodern conception of privacy as the necessary space around the *Dasein* to differentiate itself and invent itself as a unique person is of the utmost importance in the fight for privacy's survival in the digital age.

Bibliography

Acquisti, Alessandro, Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum. "The Economics and behavioural Economics of Privacy." *Privacy, Big Data, and the Public Good*, 2014, 76-95. doi:10.1017/cbo9781107590205.005.

Anderson, Heidi R. "The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public." *SSRN Electronic Journal*, 2010. doi:10.2139/ssrn.1577831.

Barocas, Solon, Helen Nissenbaum, Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum. "Big Data's End Run around Anonymity and Consent." *Privacy, Big Data, and the Public Good*, 2014, 44-75. doi:10.1017/cbo9781107590205.004.

Barth, Susanne, Menno D. De Jong, Marianne Junger, Pieter H. Hartel, and Janina C. Roppelt. "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 (2019), 55-69. doi:10.1016/j.tele.2019.03.003.

"BellSouth Denies Giving Records to NSA." CNN International - Breaking News, US News, World News and Video. Last modified May 16, 2006. http://edition.cnn.com/2006/POLITICS/05/15/bellsouth.nsa/.

"Big Tech Faces Competition and Privacy Concerns in Brussels." The Economist. Last modified March 23, 2019. https://www.economist.com/briefing/2019/03/23/big-tech-faces-competition-and-privacy-concerns-in-brussels.

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*. New York: Perseus Books, 1998.

"Bushfire Research." Commonwealth Scientific and Industrial Research Organisation, Australian Government - CSIRO. Last modified June 11, 2019. https://www.csiro.au/en/Research/Environment/Extreme-Events/Bushfire/Bushfire-research.

Cadwalladr, Carole. "'I Made Steve Bannon's Psychological Warfare Tool?: Meet the Data War Whistleblower." The Guardian. Last modified July 24, 2019. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

Cohen, Julie E. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven: Yale University Press, 2012.

Cohen, Julie E. "What Privacy is For." *Harvard Law Review* 126, no. 7 (May 2013), 1904-1933.

Desjardins, Jeff. "How Much Data is Generated Each Day?" World Economic Forum. Last modified April 17, 2019. https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

"The Economics of Data Privacy | Peter G. Klein." Mises Institute. Last modified July 19, 2019. https://mises.org/library/economics-data-privacy-0.

Esguerra, Richard. "Google CEO Eric Schmidt Dismisses the Importance of Privacy." Electronic Frontier Foundation. Last modified October 6, 2011. https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy.

Kammourieh, Lanna, Thomas Baar, Jos Berens, Emmanuel Letouzé, Julia Manske, John Palmer, David Sangokoya, and Patrick Vinck. "Group Privacy in the Age of Big Data." In *Group Privacy: new challenges of data technologies*, 37-66. Dordrecht: Springer, 2017.

Lazer, D., R. Kennedy, G. King, and A. Vespignani. "The Parable of Google Flu: Traps in Big Data Analysis." *Science* 343, no. 6176 (2014), 1203-1205. doi:10.1126/science.1248506.

Menand, Louis. "Why Do We Care So Much About Privacy?" The New Yorker. Last modified June 18, 2018. https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy.

Mislove, Alan. "You Are Who You Know: Infering User Profiles in Online Social Networks." *NY ACM Press*, 2010, 251-260.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Redwood City: Stanford University Press, 2010.

Nissenbaum, Helen. "The Meaning of Anonymity in an Information Age." *The Information Society* 15, no. 2 (1999), 141-144. doi:10.1080/019722499128592.

Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLE Law Review* 57 (2010), 1763-1815.

"Olmstead V. United States." LII / Legal Information Institute. Accessed December 21, 2020. https://www.law.cornell.edu/supremecourt/text/277/438.

Post, Robert C. *Three Concepts of Privacy*. Yale Law School, 2001.

Powers, Shawn M., and Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. Champaign: University of Illinois Press, 2015.

Sadowski, Jathan. "Why Does Privacy Matter? One Scholar's Answer." The Atlantic. Last modified February 26, 2013. https://www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/.

Solove, Daniel J. *Understanding Privacy*. 2008.

Solove, Daniel J. "Conceptualizing Privacy." *California Law Review* 90, no. 4 (2002), 1087. doi:10.2307/3481326.

Strandburg, Katherine J., Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum. "Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context." *Privacy, Big Data, and the Public Good*, 2014, 5-43. doi:10.1017/cbo9781107590205.003.

Taylor, Linnet, Luciano Floridi, and Bart V. Sloot. "Introduction: A New Perspective on Privacy." In *Group Privacy: New Challenges of Data Technologies*, 1-17. Basingstoke: Springer, 2016.

Taylor, Linnet, Luciano Floridi, and Bart V. Sloot. "Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World." In *Group Privacy: New Challenges of Data Technologies*, 18-40. Basingstoke: Springer, 2016.

"UN Charter (full Text)." Welcome to the United Nations. Last modified October 25, 2017. https://www.un.org/en/sections/un-charter/un-charter-full-text/.

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890), 193. doi:10.2307/1321160.

Wasserstrom, Jeffrey. "Resistance to the One-Child Family." *Modern China* 10, no. 3 (1984), 345-374. doi:10.1177/009770048401000305.

"Who Will Be the Main Loser from Europe's New Data-privacy Law?" The Economist. Last modified May 26, 2018. https://www.economist.com/business/2018/05/26/who-will-be-the-main-loser-from-europes-new-data-privacy-law.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books, 2019.