Master Thesis – Master Innovation Sciences

TechnoMoral Change in Data-collection technologies and Privacy.

Jelle Verweij – 3918971
j.verweij@students.uu.nl
Utrecht University
Supervisor: Koen Beumer

Table of contents

Summary

TechnoMoral Change refers to the process where technology influences morality and vice-versa. This research explores whether TechnoMoral Change has occurred between data-collection technologies and privacy. In the past years, technological developments have made it easier to access, collect, store and analyze large amount of data. As both governments and companies use these technologies to collect personal data of individuals, the privacy of those individual may be at stake. To test whether there has been a moral change, court cases of the last 20 years that concern possible privacy violations have been analyzed. Along with the court cases, technologies and relevant laws are being reviewed. The results show a spike in the amount of relevant court cases in 2018. 2018 was also the year where a new European-wide law, the General Data Protection Regulation was implemented. Due to this law, designed to protect individuals from new technological developments concerning data-collection, is became easier to sue governments, companies and individuals that possibly violated privacy. This law is expected to be one of the main reasons for the spike in privacy-related court cases. Other explanations are the extensive media coverage after well-known privacy violations, such as the widespread data-collection by the NSA. While there has been a change in the number and nature of court cases over the years, more research is needed to ensure that TechnoMoral Change has occurred. This paper sheds a first light on the matter and shows a possible change in thoughts and views on privacy but is not able to make a conclusive statement about the matter.

Introduction

The exponential growth of the internet increasingly poses challenges to privacy. By now, the five biggest corporation in the world (Amazon, Apple, Alphabet, Microsoft and Facebook) are all in some way data-driven, thus using their customer's personal information to gain a market advantage (Greenwald, 2014). Besides corporations, governments also use (meta-)data in their everyday work, for example in so called Smart Cities (Martijn & Blauw, 2019) and social score projects (Ma, 2018). As the use of data increases, several NGO's and other organizations try to bring the downside of these developments under public attention. Examples of these organizations are Bits of Freedom and human rights organizations like Amnesty International. As it can be unclear for individuals which data is collected, by whom and for what purpose, they are unable to make an informed decision about the matter. Due to this lack of transparency, their privacy can be at risk, as their data is used without their consent.

Large-scale data collection is being used by both companies and governments to make their products and projects work. Customers and citizens might be unaware of this and might even be forced to participate, for example in the case of governmental projects or through social pressure by their peers, as might be the case for several social media.

Most of the products, projects and services that use data are essentially 'black boxes' (Martijn & Tokmetzis, 2016). Blackboxing is "the way scientific and technical work is made invisible by its own success. When a machine runs efficiently, when a matter of fact is settled, one needs to focus only on its inputs and outputs and not on its internal complexity. Thus paradoxically, the more science and technology succeeds, the more opaque and obscure they become" (Latour, 1999). Blackboxing makes it impossible for individuals to know what happens with their data after it is collected. The individual's right to be in charge of their own personal information is thus increasingly jeopardized by the advent of digital data collection.

The right to remain in charge of your own personal data is mainly protected by the rules and regulations that are designed to protect our privacy. In general, rules and regulations are based on certain values we hold. Just like traffic regulations are based on the value of safety, regulations concerning data collection are based on the value of privacy. They protect privacy by prohibiting certain acts that are considered violations. As such, laws and regulations can be considered to be an operationalization of shared values. Values are generally shared by a large portion of people within a certain culture or country. The laws that follow from those values are thus a reflection of what the people within a certain country deem as good or bad (Brandt, 1954).

Opinions about what is good and what is bad are also reflected in morality. Morality is defined by Van de Poel and Royakkers (2011) as the totality of opinions, decisions and actions with which people express, individually or collectively, what they deem good or right. If people feel morally wronged, they can decide to file a court case. In this research it is argued that because of this, morality is visible in court cases, especially in the complaints of the accusers. Following the definition of morality, it is argued that a single complaint reflects the opinion on what is good or bad of a single accuser, while the totality of complaints concerning a certain subject reflects the morality of the whole group of accusers on that subject.

While laws are an operationalization of shared values, they can be subject to change. For certain laws, this is a necessity, for example because the subject of the law is changing. This could be the case for laws concerning technologies, as for example data-collection technologies develop over time and laws have to include newly developed technologies to ensure that they underlying values stay protected. This doesn’t necessarily reflect a change in values, technological developments merely change the interpretation or operationalization of established values. Speed limitations following the introduction of cars did not result from a change in values, safety was important before and after the introduction of cars. The introduction of cars resulted in a new possible violation of the value of safety, hence the introduction of speed limitations.

For long, values have been assumed to be stable over time. Cultural differences exist, but core values are not expected to change within a stable society, consisting of people that more or less share the same culture and historical background (Edwards, 1987). However, the stability of values is up for discussion. Recently, however, scholars have argued that values might not be as rigid as we thought. Swierstra (2013) for instance argues that morality co-evolves with changes in technology. This process, where changes in technology influences changes in moral value and vice-versa has been dubbed TechnoMoral Change (Swierstra, 2013).

As technology develops, it poses new challenges and offers new opportunities. Values can be subject to change, due to the new insights or possibilities provided by the new technological developments. For example, the introduction of the contraception pill revolutionized values associated with sexuality. The contraception pill separated sexuality and reproduction (Keulartz et al., 2004). This made it possible for individuals to freely experiment with sexuality without risking a pregnancy. The sexual revolution that took place along with the introduction of the pill shows the shift in values concerning sexuality. In time, values like not having sex before marriage were replaced with a looser interpretation of sexuality. Furthermore, the introduction of the contraception pill is also linked to a moral change concerning abortion (Ketting, 2000). Collected data showed no decrease in the number of abortions, while less women were getting pregnant. The pill and the changed views on family planning supposedly resulted in abortion coming up for discussion even if the pregnancy was simply unplanned, while this used to be only an option in the case of an unwanted pregnancy (ibid).

Despite the societal relevance of TechnoMoral Change, there is only a handful of studies that have looked into the phenomenon. For example De Beaufort (1998) has investigated the interplay between changes in technology and changes in morality for biotechnology and cloning (De Beaufort, 1998), and others have looked at self-driving cars and safety (Goodall, 2016; König & Neumayr, 2017) and artificial intelligence and safety (Bostrom & Yudkowsky, 2014).

What is more, Swierstra's work on TechnoMoral Change does not make it very clear how to study TechnoMoral Change. Swierstra (2013) presents the concept in a rather theoretical, almost philosophical way. While he does identify four different mechanisms of TechnoMoral Change that he illustrates with empirical examples from secondary literature, he does not provide a concise operationalization of TechnoMoral Change, nor provides an empirical analysis that can serve as an example. This research tries to improve the operationalization of TechnoMoral Change and tests this by applying the theory to the interplay between privacy and data-collection technologies.

Data-collection technologies are being used more and more often by both governments and companies. The rapid technological developments and the possibility of privacy violations has gained attention, for example in the media (De Volkskrant, 2019). This research applies the theory of TechnoMoral Change to test whether those technological developments changed our notion of privacy over the years. Therefore, this research is guided by the following research question:

How has our notion of privacy changed due to technological changes in the field of data-collection?

As mentioned before, this research argues that complaints of accusers in court cases reflect morality. This is one of the reasons that court cases are used to analyze a moral change concerning privacy. The initial goal was to analyze complaints filed to the *Autoriteit Persoonsgegevens*, the Dutch Authority for Personal Data. Unfortunately, in order to gain access to the privacy complaints filed to the Autoriteit Persoonsgegevens, a lengthy bureaucratic procedure had to be entered, which was not feasibly within the time-frame of this thesis. Furthermore, the spokesperson of the Autoriteit Persoonsgegevens did not think a request to access data for a master thesis would be likely to be successful. . Surveys were no option due to the longitudinal aspect of the research and the time-constraints. The court cases where deemed to be the best option as they are considered to reflect the most serious and pressing problems, as the accusers are willing to go to court. Furthermore, the records of court cases are more easily accessible compared to the complaints filed to the Autoriteit Persoonsgegevens, they are very rich and detailed and and are thus considered the next best option.

Due to different legal systems across countries and time-constraints, only one country of focus is chosen for the analysis. There are several conditions that must be met for this country. The technologies relevant for data-collection must be present, ideally from early on. The country must have accessible databases with court cases and the country must have a legal system with laws focused on privacy-protection. The Netherlands meets all three conditions. It has well developed relevant technologies, for example due to the large number of data-based governmental bodies (Martijn & Tokmetzis, 2016), a high availability of internet, with over 95% of the population having access to it (CBS, 2018), while 90% of the population owns a mobile phone or smartphone (CBS, 2018). It has extensive database with court cases, and it has well thought-out laws for privacy-protection, such as the *Algemene Verordening Gegevensbescherming* (AVG, European-wide known as the GDPR).

The court cases that are selected for the analysis also have to meet several conditions. The case must concern a privacy-related complaint. To meet this condition, the selected cases must involve the application of the earlier mentioned AVG, or its predecessor, the *Wet Bescherming Persoonsgegevens* (WBP). These are the most important privacy laws in the Netherlands and therefore offer a good view on TechnoMoral Change concerning privacy. Secondly, the case must involve a technology. For this research, this condition is met when privacy is violated using data-collection technologies. Technologies are able to create new ways of violation privacy or to make this easier. An example of the latter is the possibility for governmental bodies like the tax authority to ask commercial parties for their customer info, for example if they suspect tax fraud. Before digital databases existed, it was possible to ask for analog customer info, but technological developments have made it easier to perform this action. The last condition that has to be met concerns the timeframe of the analysis. As it takes time for change to happen, a 20-year time period is chosen. A longer period is not expected to give better results, due to the lack of relevant technologies before 1999 and the lack of relevant court cases in the used database before that time.

I will identify TechnoMoral Change by analyzing the court cases over time. I therefore draw upon a classification of four different types of privacy violations. Changes within and across these different types of privacy violations over time will indicate that moral change has occurred. These changes will subsequently be analyzed by look at the how, the who, and the what. As for the how, I will analyze what mechanism of TechnoMoral Change that Swierstra (2013) described can be observed. As for the who, I will identify different types of actors that have been accused of privacy violation. And for the what, finally, I will identify the different types of technologies that enabled these privacy violations to occur. This will allow me identify patterns in the types of privacy violations over time and help me to analyze whether these changes are for instance correlated to the emergence of different types of actors or technologies, and to see the mechanisms through which this TechnoMoral Change occurred.

The research is of an exploratory, qualitative nature. The theory of TechnoMoral Change has not been tested empirically before. This research tries to apply the principles that were thought out by Swierstra to the interplay between privacy and data-collection technologies, in the hopes that future scholars can draw upon it. The research is also designed to give insight into the tense relationship between privacy and data-collection, a subject that has become important during the last couple of years.

Theory

Within this section, the theoretical constructs that were mentioned in the introduction are elaborated on. The section starts with an explanation of morality, as this can be a difficult concept to understand. It is followed by a more thorough elaboration on TechnoMoral Change, the theory by Swierstra that describes the interplay between changing technologies and changes in morality. The third core concept that will be described and operationalized is privacy. An overview of the relevant laws and a selection of data-collection technologies is also provided.

Morality

To understand morality, it is first important to understand norms and values. Van de Poel and Royakkers (2011) provide definitions for these concepts. Values, first of all, are the ideas or matters that people feel should be strived for in general. This serves the goal of leading a good life within a just society (Van de Poel & Royakkers, 2011). Values are translated into rules that describe what is forbidden, required or permitted. These rules are called norms. Morality is defined as ‘the totality of opinions, decision, and actions with which people express, individually or collectively, what they think is good or right’ or as ‘the totality of norms and values that actually exist in a society’ (Van de Poel & Royakkers, 2011, p. 71). Using these definitions, moral change can be defined as a change in the opinions, decisions, and actions with which people express what they think is good or right.

As stated in the introduction, this research uses court cases to assess moral change. It is argued that the totality of the complaints of accusers in court cases reflect the morality of that group. It is important to differentiate between the complaint and the eventual judgement of the court. The judgement assesses whether the actions of the defendant conflict with the law. The complaint of the accuser is considered a direct reflection of the opinion of the accuser about what is right or wrong. For this research, it is argued that analyzing these complaints during a certain period reflects the morality in that certain period. The complaints thus serve as a sample of the totality of the opinions in the society.

To summarize, moral change is defined as a change in the opinions of people about what is good or right over a certain period. Complaints of accusers in court cases are a source for the identification of such opinions, as the accusers strongly believe that they are morally wronged and go to court to settle this. The court cases can thus be used to measure moral change. This can be used to measure TechnoMoral Change, which is discussed in the next section.

TechnoMoral Change

The term TechnoMoral Change was coined in 2013 by Swierstra, but others already worked on the idea that morality and technology influence each other prior to his work. Martin Heidegger noted that modern technology is a force that impacts not only our living environment, but also the people in it and the values we hold dear (Heidegger, 1954). This was however more a philosophical idea, not an empirically founded theory.

Scholars, mainly in the field of Science and Technology Studies, have established that morality influences the development of technology (Bijker et al., 1987; Bijker, 1992). Scholars in this field have demonstrated that technology does not develop autonomously but that its development is shaped by values. An example is the technological developments that followed the moral issues we have with climate change. Electric cars like those from Tesla are developed partly due to the moral issues concerning climate change of one of the owners, Elon Musk (Koppelaar & Middelkoop, 2017). These scholars thus demonstrated that morality influences technology.

More recently, in line with Heideggers work, Verbeek (2006) pointed out that technological developments are also able to give rise to new moral issues, as they influence our relationship with the world in several ways. Verbeek described how technology influences how we interpret the world. An example is the invention of the telescope, which made it possible for Galileo Galilei to observe that the Earth revolves around the sun. This challenged the existing catholic beliefs, thus questioning the catholic morals and values.

Verbeek also identifies other ways in which technology influences morality. Technology also influences our interaction with the world as it enables new ways to act, possibly resulting in new responsibilities as things that were up to chance at first, are now transformed into choices. An example is the development of prenatal diagnostics. As it is currently possible to test for hereditary diseases, prospective parents with a family history of a certain disease may perceive a moral obligation to test their fetus and can be held responsible if they decide not to (Verbeek, 2006). Technology is thus able to raise new ethical dilemmas, raising questions that were irrelevant or even impossible to ask before the introduction of a certain new technology. Answering those ethical questions might result in the re-evaluation of norms and values, and moral change.

Technology and morality can thus not be viewed as independent, autonomous factors; they are able to influence each other (Jasanoff, 2004). Swierstra (2013) called this process TechnoMoral Change, referring to the ongoing interplay between morality and technology. As innovative technologies are able to change how we interpret the world or to enable new ways to act, it can spark new moral issues. Resolving these issues can result in moral change, which in turn might alter the technological pathway.

To explain how moral change happens, Swierstra (2013) identifies four mechanisms in which technology can destabilize morality, thus starting the process of TechnoMoral Change. These mechanisms explain how technology changes morality, in this case our notion of privacy. As the mechanisms explain how this take place, they are possible answers to the research question. The four mechanisms will now be discussed, while the framework is further discussed in the methods section.

The first mechanism that Swierstra identifies, is the possibility that technology destabilizes morality by creating new practical opportunities, which can in turn create new responsibilities, obligations and rights. It may also cause a renegotiation of existing distributions of responsibilities (de Vries, 1989). An example, relevant to the goal of this research, follows from the new technologies that enable large scale data-collection, like the internet. Due to the introduction of the internet, it is possible to governmental bodies and companies to collect and store more and different data. This also obliges them to protect newly collected data against third parties in other ways than they were used to before digital data collection. Safe storage of digital data, and protection that data against hackers and data-breaches, has thus become a new responsibility for the government and for companies. The new opportunity thus brings up new moral questions, that are, in this case, resolved by assigning responsibilities.

As the research question is ‘how has our notion of privacy changed due to the technological changes in the field of data collection?’, the answer that follows from this mechanism is: ‘our notion of privacy has changed due the new practical opportunities and new responsibilities, obligations and rights that are created by the technological changes in the field of data collection’.

The second mechanism that Swierstra (2013) identifies, is the possibility that technology destabilizes morality by introducing new stakeholders. Stakeholders are parties that carry consequences of a certain activity or inactivity. An example, relevant to the goal of this research, is the introduction of technology that tracks and analyzes data flows between devices. This led to the introduction of data-brokers, companies that collect, auction and sell our data to other companies by using trackers and cookies (Martijn & Tokmetzis, 2016). The existence of those companies confronts users with a new moral dilemma, as they must decide whether they have issues with third parties accessing and selling their personal data and whether those issues are big enough to act upon. This decision concerns an evaluation of their notion of privacy and a possibility for moral change.

As the research question is ‘how has our notion of privacy changed due to the technological changes in the field of data collection?’, the answer that follows from this mechanism is: ‘our notion of privacy has changed due to the introduction of new stakeholders along with technological changes in the field of data collection’.

The third mechanism that Swierstra (2013) identifies, is the possibility that technology destabilizes morality by shaking up established ways of perceiving the world’s order, by changing the roles and relationships between the different actors in it. An example, relevant to the goal of this research, is the changed relationship between people and companies after the advent of data-driven companies. Most companies used to treat people as customers, while nowadays data-driven companies treat their users as a source for a most valuable product, data. New data-collection technologies thus changed the relationship between people and companies and the role that people play is changed from customers to data sources. This might have implications for whether we want to share our data with those companies or whether we want to use their services or products. This can involve an evaluation of our notion of privacy and possibly moral change.

As the research question is ‘how has our notion of privacy changed due to the technological changes in the field of data collection?’, the answer that follows from this mechanism is: ‘our notion of privacy has changed due changes in the relationships between and roles of actors, following technological changes in the field of data-collection’.

The fourth mechanism that Swierstra (2013) identifies, is the possibility that technology destabilizes morality by giving us new insights in the consequences of our actions, or blind us to those consequences. Technology can reveal previously unknown information, which may alter how we act or think about certain moral values. An example, relevant to the goal of this research is the use of data-collection and data-analysis by tax authorities to find tax evaders. It is possible to use data from multiple sources to compute the chance that an individual commits tax fraud, for example by looking at parking data to check whether an individual lives in the country that has been specified. This can lead to new consequences to certain actions. Technology like this, designed to compute the chance that a certain action has taken place of will take place, is also used in smart assistants like Alexa (Amazon) and Siri

(Google). People that are subject to analysis like this might have issues with the new implications of their action, which might result in moral change, for example in deciding that they desire the comfort of a smart assistant, even if this is detrimental for their privacy.

As the research question is ‘how has our notion of privacy changed due to the technological changes in the field of data collection?’, the answer that follows from this mechanism is: ‘our notion of privacy has changed due to the new insights in the consequences of our actions provided by technological changes in the field of data-collection’.

The mechanisms are part of the framework used for the analysis and are expected to aid with answering the research question, as they explain how technological change leads to moral change.

Privacy

Privacy is difficult to conceptualize, as there are several different sorts of privacy. Koops et al. (2016) defined nine types of privacy, eight of them being labeled as basic types. These are for example bodily privacy, the idea that people are not allowed to touch you if you do not want them to and are not allowed to restrict you in your movements. Another example is spatial privacy, referring to the privacy of the private space and the restriction that others have when willing to access or control that space. Someone’s home is the typical space where this type of privacy is most important.

The ninth type of privacy defined by Koops et al. (2016) is an overarching type of privacy that overlaps with the other eight, as is illustrated by figure 1. It is called informational privacy and is typified by preventing information about one-self to be collected and by controlling who has access to that personal information. Examples of this kind of information are someone’s phone number, buying behavior, search history, whereabouts and way of communication.

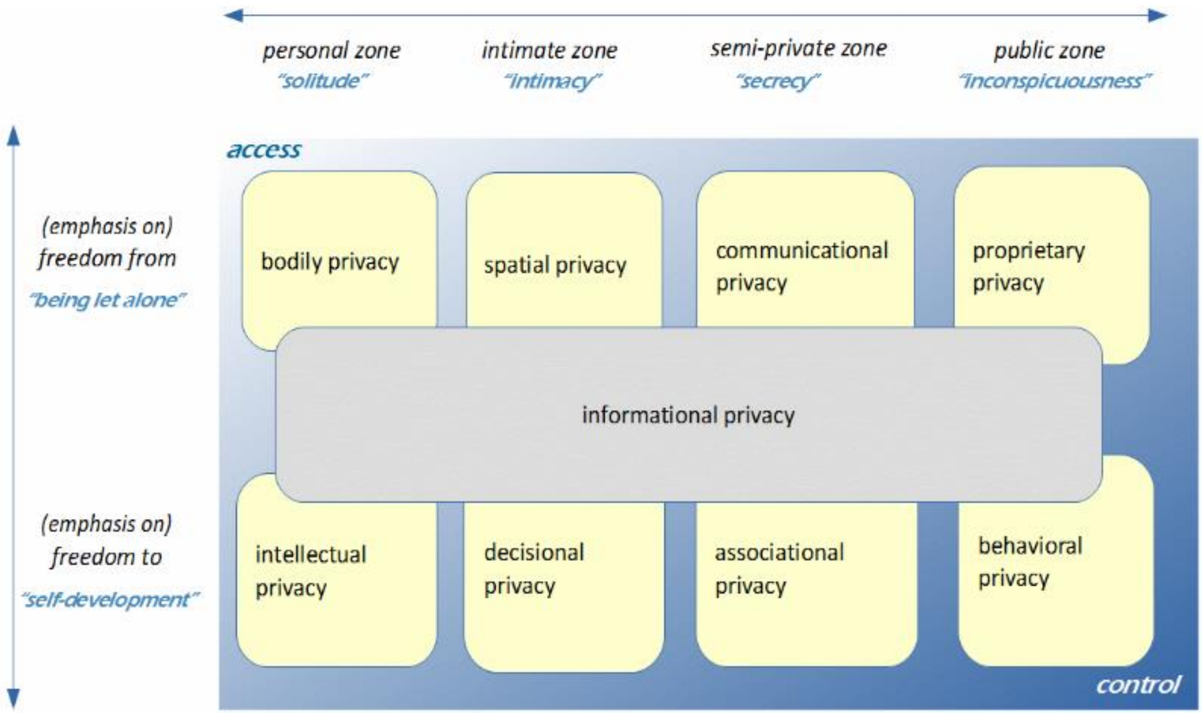


Figure 1. Classification of types of privacy (Koops et al., 2016, p. 484)

The conceptualization of informational privacy fits the research goals, as concerns data about one-self, which is the kind of data that can be targeted by data-collection technologies, . It also provides two different ways of violating informational privacy, not being able to prevent collection of personal information and not being able to control who has access to this information. Both are part of the second dimension in the framework that is used for the analysis, that consists of different ways to violate privacy and thus explains what kind of violation took place. During an initial analysis of the court cases, however, I encountered several instances of privacy concerns that could not be captured by these two categories (collection and control over access). I analyzed 20 court cases to test the coding scheme where I coded each court case along the lines of the different types of privacy violations. Because collection and control over access did not suffice, I developed two more categories of privacy violations on the basis of the empirical material: the storage of data and the analysis/usage of data. This results in four types of privacy violations: (control over) access, collection, storage, and analysis/use.

The identification of the kind of privacy violation involved in a court case depends on the way it is described by the accusing party. These descriptions are generally very specific and to the point, as this is a necessity in court and a custom among lawyers. As such, while the cause of the case might involve a multifaceted problem, a complaint has a very specific focus. As the multifaceted problem is not recorded in the court case, it is impossible to be sure of its nature. Due to this, the specific focus is used for the identification, while in some cases, one could suspect the existence of a larger, underlying problem.

The first way in which privacy can be violated is unauthorized access to personal data. It involves cases where the defendant is accused of unlawfully gaining or giving access to personal data or cases where an individual is unable to control who has access to his or her personal data, due to data-collection technologies. An example is a case where a governmental organization want to access a database owned by commercial party or cases where an individual is denied access to his or her own medical records by a hospital.

The second kind of violations is the unauthorized collection of data. It involves cases where the defendant is accused violating privacy by unlawfully collecting personal data, with the use of data-collection technologies. It may also involve cases where the accuser was unaware of the collection or changed its mind about their permission to collect data, which makes the collection a violation of privacy. Whereas '(control over) access' concerns privacy concerns over data that is already collected, this category is specifically about cases where the activity of collecting the data itself is the source of accusation. An example is a case where a governmental organization or company secretly tracks and collects data on internet usage from their citizens or customers.

The third kind of violation is unauthorized storage or registration of personal data. It involves cases where the defendant is accused of violating privacy by unlawfully storing personal data. It also involves cases where the accuser wants to see certain data removed from storage, or disputes over the validity of the stored data. Whereas the first and second type of violation concern having access to data and the act of collecting the itself, this type of privacy violation concerns cases where people disagree about the content or type of the information, and cases where the information stored is not right or needs to be updated. An example is a registration of a persons' credibility in a database, based on former problems with paying of loans. The financial situation of the individual might have changed, while the registration still impacts his private life, which can be considered a violation of his privacy.

The fourth kind of violation is the unauthorized use or analysis of personal data. It involves cases where the defendant is accused of violating privacy using or analyzing personal data. It can involve cases where data is used for other purposes than was intended. While the other kinds of violations mainly concern 'raw' data, this category mainly involves cases where collected data is second-hand or has been processed. An example of processed data is data that has been subjected to software that alters how it is presented, for example the algorithm that Google uses for their search engine. A court cases against Google involving a complaint about search results is within this category, as the presentation of the data is different due to the analysis done by the algorithm of the search engine. Another example of this category is identity fraud by using someone's data, for example name, address and photo, to make a fake online profile.

The aforementioned categories are part of the framework used for the analysis as they explain how privacy is violated.

Another important question to ask is who violates privacy. Differences between actors that violate privacy could indicate that our notion of privacy is different for different violators. It could, for example, be the case that we are okay with the government collecting personal data, while we are not okay with a company collecting the same kind of data. An initial analysis of the data showed that issues with data-collection are broadly classified in three types of actors, the government, companies and inidividuals. These three types are discussed briefly beneath.

The first type of actor is companies. Nowadays most companies collect data and data-driven companies like Facebook even collect, store and analyze data to gain a market advantage. Data is acquired, by themselves or by buying data from others, for example to offer advertisements more fit to the customer.

The second type of actor is the government. One of the main reasons that governments collect, store and analyze data is to fight crime. Tax authorities use data to track down tax evaders. Intelligence agencies use data to track down potential terrorists. There are also governmental bodies for healthcare, child protection and all sorts of allowances that make us of data. A lot of the data is collected from their citizens, possibly without them even being aware (Martijn & Tokmetzis, 2016).

The third type of actor is the individual. This category concerns, for example hackers that hack into a network to collect data or people that commit identity fraud.

The three types of actors are part of the framework used for the analysis as they explain what kind of actors were involved in the cases.

Technologies

A precondition to identify TechnoMoral Change is that there is technological change, which in turn can give rise to moral change. For data-collection technologies, this is clearly the case, as there has been a tremendous development in those technologies in the last 20 years, the timeframe of the research. It for example involved the dotcom bubble, a period between 1995 and 2000 where the internet flourished and stocks involving internet-based companies peaked (Wollscheid, 2012). The internet, the free exchange of data with people across the globe is one of the most dominant technologies nowadays and offers an enormous amount of possibilities to collect, share and access data. While 20 years ago, companies just started to explore what this means for their business operations, the last decade showed more and more companies that were able to convert data in to money, leading to the current situation, where the five biggest corporations in the world make money mainly by collecting, analyzing and selling data.

Next to companies, the government also increasingly uses technologies that collect data in their everyday work. In 2001, the ICTU was founded, which is Dutch organization that helps the government with the use of ICT (https://www.ictu.nl/). This eventually led to the digital government (https://www.digitaleoverheid.nl/), where dataflows between government and citizens are digitized. An example of this digitalization is the nationwide introduction of the DigID in 2005. A DigID is a digital way passport which allows citizens in The Netherlands to identify themselves online, for all kinds of governmental bodies, for example the Tax Authority. Another application of data-collection technologies by the government that is more invasive for citizens is the large-scale data-collection by intelligence agencies. While this was possible since the advent of telephone-cables, the increase in network speed over the years makes it way easier for governments to collect data, while the developments in technologies that store data, from floppies towards enormous digital-datacenters, makes it way easier to store and analyze data.

Laws

As mentioned before, the court cases that are selected for the data analysis must involve the application of the *Algemene Verordening Gegevensbescherming* (AVG) or its predecessor, the *Wet Bescherming Persoonsgegevens*. The AVG is the Dutch version of the European-wide General Data Protection Regulation.

In 2016, the European Union passed the General Data Protection Regulation, which was implemented as the *Algemene Verordening Gegevensbescherming* (AVG) in The Netherlands (Uitvoeringswet Algemene Verordening Gegevensbescherming, 2018). This law describes the responsibilities for organizations that handle data. The Autoriteit Persoonsgegevens is responsible for the enforcement of this law.

The main provisions in the AVG, as stated by the Autoriteit Persoonsgegevens (Autoriteit Persoonsgegevens, 2018) are about lawfully handling personal data. This means, for example that it must be clear for the individuals involved why and how personal data is processed. Next to that, the data can only be collected if there is a justified and clearly described goal, before the actual collection takes place. This goal must be clear to the individuals involved. The identity of the person or organization that collects or processes the data must also be clear to the ones involved.

Another important provision is that organizations, like commercial enterprises or governmental bodies, are obliged to collect as little data as possible. The data must be correct and if necessary, updated. The whole process must be properly protected, especially if the data consists of special data like race, information concerning health or someone's religion (ibid).

The AVG is the most important privacy-law in The Netherlands and is similar to the privacy-laws in other countries in the European implementation Union, as all are an of the GDPR. This makes it not only the best law to select case on due to the content of the law, but it also makes the results of this research more easily applicable to the other countries in the European Union.

Methodology and sources

The study is of an exploratory, qualitative nature. It builds upon the theoretical work by Swierstra (2013) and attempts use the mechanisms of his theory of TechnoMoral Change, to research if and how developments in data-collection technologies has changed our notion of privacy.. A framework is developed from literature and from an initial analysis of the cases. A timeframe of twenty year is chosen as a suitable period to measure change. This is considered to be the most suitable period due to the lack of data-collection technologies and the lack of relevant court cases. The research will thus start with cases from 1999.

There are several reasons why 1999 is a good starting point. 1999 is part of the period that became known as the dot-com bubble. This period, ranging from 1995 to 2000 was a period of excessive economic speculation, where the Nasdaq Composite stock market index, which included many companies that are mainly internet-based, peaked (Wollscheid, 2012). It marks a period in time where the use of the internet grew enormously. 1999 is also the year where the second Wi-Fi protocol, the 802.11b came out, which became one of the most widely used protocols and was a great leap forward for the wide accessibility of wireless internet. Apple, for example, launched their first iBook later that year, which had the 802.11b Wi-Fi protocol included as an optional feature. At the end of the year, Microsoft set a new market capitalization record, with a value of 618.9 billion US dollars. 1999 thus marks a year where internet became widely known and available, internet- and technology-based companies flourished and wireless internet as we know it became popular. The mass availability of internet made it way easier to collect all sorts of personal data.

1999 is also a relevant year from the perspective of privacy concerns, as it marked the birth of Big Brother, a Dutch reality tv-show where the contestants were constantly monitored. This was one the first television series with constant monitoring and led to a lot of controversy. The ease with which the contestants gave up a great deal of their privacy was to some people shocking and led to rethinking and redefining of privacy and personal boundaries.

Data Collection

As was mentioned above, this research uses court cases to assess morality, as it is argued that the complaint of the accused party in a court case reflects their opinions on what is good or bad. As morality is defined by Van de Poel and Royakkers (2011) as the totality of opinions on what is good or bad, it is argued that the totality of the complaints of accused parties concerning a certain subject in a certain period of time provides a good source for the morality about that subject in that period of time.

As time-constraints and differences in legal systems across countries made it possible to focus only on one country, the data will consist of court cases in The Netherlands. The Netherlands is a suitable country of focus due to the early adaptation of relevant technologies and a wide availability of these technologies, as was mentioned in the introduction. An additional reason is the used conceptualization of privacy, as the research by Koops et al. (2016) focused on Western countries and the conceptualization thus best fits Western countries.

The analysis will focus on court cases that revolved around issues of privacy in relation to data collection. These will be collected by using www.legalintelligence.com. This site provides an integration of several judicial database and is one of the most used databases among law students and practitioners. It is part of the Legal Intelligence Society, which has been founded by some of the biggest Dutch law firms and several government bodies such as the Dutch parliament to enhance their information- and knowledge management. The database consists of both court cases, court documents and reports of lawmaking. The documents provide detailed in-depth overview of the cases and are thus suitable for the analysis. Due to the integration of multiple databases, all relevant cases for the analysis can be found in the database.

As is mentioned before, the selected cases involve the application of the most important privacy law in The Netherlands, the *Algemene Verordening Gegevensbescherming* (AVG), which is an implementation of the European Union-wide General Data Protection Regulation. As some of the provisions described in the GDPR differ among countries, the AVG is accompanied by ty *Uitvoeringswet Algemene Verordening Gegevensbescherming* (UAVG). Cases involving the application of the UAVG are also selected, as are cases involving the preceding law, the *Wet Bescherming Persoonsgegevens* (WBP).

The database is unable to only select cases that involve a data-collection technology. This is, however, a condition for inclusion in the dataset. Due to this, all 316 initially selected cases had to be analyzed in order to ensure that all cases involving a data-collection technology were selected.

Data Analysis

As mentioned before, a framework was devised for the analysis, based on literature on TechnoMoral Change and privacy. To identify changes in morality, caused by data-collection technologies, the framework involves the four categories of privacy violations that are discussed in the theory section. With these four categories, changes in the type of privacy violation over time are identified. Also part of the framework are the four different mechanisms identified by Swierstra (2013). By analyzing the cases and identifying which mechanism is involved, it is answered how data-collection technologies impact our notion of privacy, as is explained in the theory section. Furthermore, the framework involves the three different possible actors, which answers who were involved in the cases. Lastly, the technology used for the violation of privacy is identified.

How did I code these court cases? As all cases are written by jurists, a thorough reading was necessary to fully understand the core problem of the dispute. After this initial reading of a case, I coded each complaint in the court cases along the lines of the four types of privacy violations (access, collect, storage and analyze). This was all written out within an excel-file. Subsequently every court case was coded for the mechanisms of TechnoMoral Change that were found, the types of actors violating the privacy, and the types of data-collection technologies used to violate privacy.. To ensure that no important information was lost due to the analysis, a small explanation of the case and the reason for the assignment to a specific category was included in the excel sheet. Other case-specific information that was part of this excel-file was a case-number, the date of the case, the hyperlink to the case and, if necessary, some additional remarks.

To assess TechnoMoral Change, it is necessary to compare differences within the categories of privacy violations over time and to compare between the categories. However, the results will start with an general overview. Next the privacy violation types are discussed separately, starting with the one involved in most cases. For every type of privacy violation, the TechnoMoral Change mechanisms involved, the actors involved, and the technologies involved are presented. At the end of every section, the results are summarized and compared with the other sections. This results in a detailed description of the cases over time, grouped by type of privacy violation.

Reliability and Validity

Due to the integration of multiple databases in the Legal Intelligence database, and the number of selected cases, the research is expected to be reliable. However, the reliability tends to increase year by year as the analysis is based on more cases in recent years, with up to 151 cases in 2018.

As the primary concept, privacy, is conceptualized as informational privacy, which is well embedded in literature, there are no expected issues concerning internal validity. The concept of informational privacy is well described, and the cases are selected to fit that description. The research from Koops et al. focused on Western countries, thus also impacting the external validity of this research. The conclusions of this research are suspected to apply for all Western countries that have experienced similar technological developments and similar laws through the years. Especially countries within the European Union are likely to show similar moral developments, as they share certain laws, such as the *Algemene verordening gegevensbescherming*, known as the General Data Protection Regulation (GDPR) throughout the European Union. This regulation applies to the whole European Union from May 25th, 2018 onwards.

Results

The initial dataset consisted of 316 court cases. As stated in the method section, these cases where selected by searching for cases concerning the Algemene Verordening Gegevensbescherming (AVG) or its predecessor, the Wet Bescherming Persoonsgegevens (WBP) in the time period ranging from January 1st, 1999 till December 31nd, 2018.

Not all of these cases involved data collection technologies, however. The main reasons for this were the lack of involvement of technologies or digitalized data in the cases, duplicates and other matters for which AVG was used as the abbreviation, such as Arts Verstandelijk Gehandicapten (Doctor for the Mentally Challenged). After scrapping these cases, 86 were left in the analysis. None of these cases where before 2011.

The results are structured by the different types of privacy violation. I will analyze changes in the number of cases, changes in the actors involved, changes in technologies involved and changes in the TechnoMoral Change mechanism involved.

General overview

As stated before, there are no relevant cases before 2011. This is an interesting finding by itself, as it means that despite rapid developments in data collection technologies, no court cases concerning privacy breaches due to technology were filed prior to 2011. The widespread use of internet and mobile phones and the introduction of several social media already happened several years prior to 2011 and are examples that data-collection was already possible and thus possibly happening during the first decade of the 21th century. Developments like these could reasonably be expected to give rise to privacy concerns. Yet this was not the case in the Dutch court cases. As can be seen in figure 2 below, the amount of cases spiked in 2018. 73,26% of the cases in the final dataset are from the year 2018. The figure shows a change in the amount of court cases that are filed through the years, especially between 2017 and 2018. Below, each of the four types of privacy violations is analyzed to find out what has changed in 2018, which actors are involved and which technologies are involved. To analyze how this change has happened, it is analyzed which of the four mechanisms of TechnoMoral Change is involved.

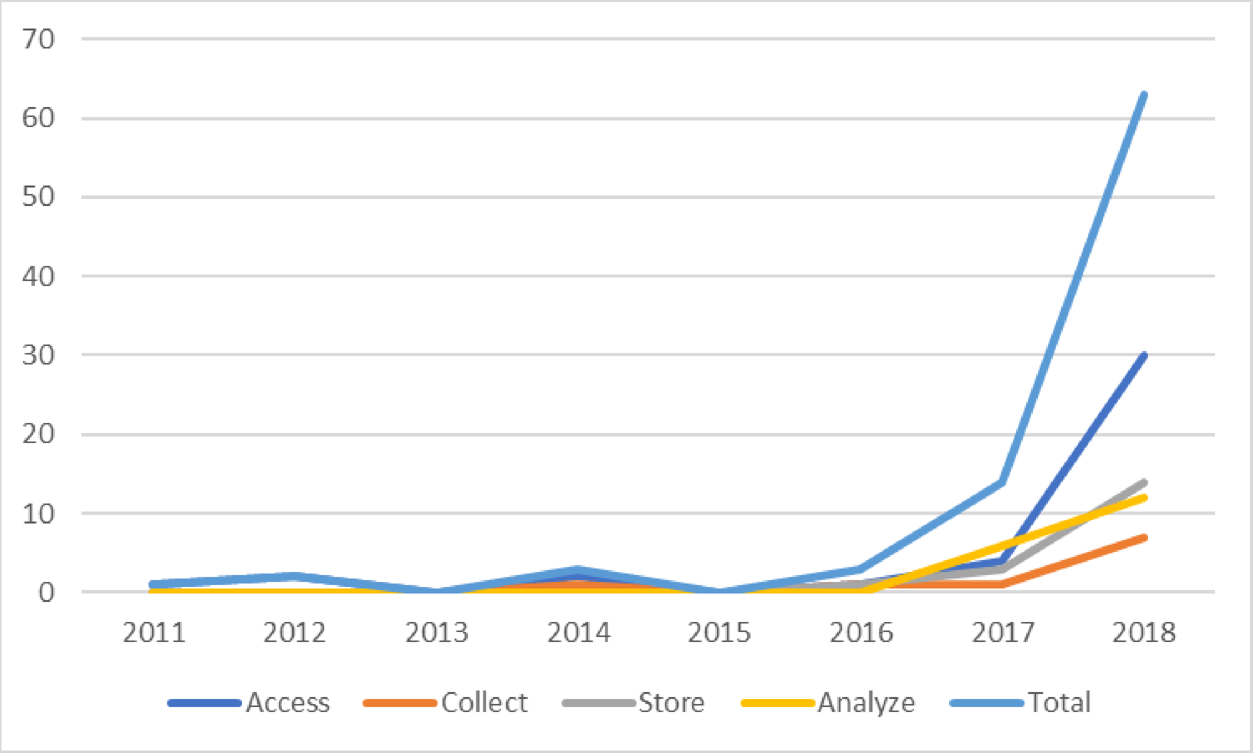


Figure 2. Amount of cases by Privacy Violation

Access

'Access' is the type of privacy violation that is the most apparent in the data. It refers to a dispute over the accessibility of information, for example if a government agency has unauthorized access to personal information. Another example are privacy violations where an individual is unable to gain access to his or her personal data, which may violate their privacy, for example in the case of medical information. Denying an individual access to such information also denies this individual the possibility to decide whether they want others to know that information, the possibility to act on it or to decide whether they agree with the information. As such, the denial of an individual to such important or private information can be considered a privacy violation.

The court cases contained numerous examples of privacy violations concerning accessing data. For example, in one court case the Dutch Tax Authority wants access to data from the Stichting Museumjaarkaart (a Dutch organization that supervises a card that allows users to visit museums with discount) regarding personal information of the card users. The Tax Authority sought access to this data to track down tax evaders, but the Stichting Museumjaarkaart considers this as a violation of the privacy of their users. Another example is a case where an individual wants access to medical information regarding the birth of her son, which is held by the hospital she gave birth in. She considers it a violation of her privacy that she is unable to know important and private details regarding the birth of her son. During birth, her son became handicapped. This is analyzed by medical specialists, she considers it her right to know how this could have happened, which is, to her, highly important and private information. Moreover, she is unable to act on the information, for example by using it in a court cases against the hospital or to cope with the incident.

Of all cases analyzed, 40 fit within the access category, which is 46,51% of all cases. This makes it the biggest category. Most of those cases are from 2018, as is shown in figure 2. There are 30 cases in 2018 which accounts for 75% of all cases within the category. This steep increase in the number of cases will be analyzed by looking at changes in the actors involved in the violation of privacy over time, changes in technologies and changes in the mechanisms of TechnoMoral Change that apply to the cases.

Figure 3 gives an overview of the changes in the actors that violate privacy by giving, gaining or denying access to personal data over time. In one of the cases, both a company and an individual was sued. Due to this, there is a total of 41 cases included in the figure.

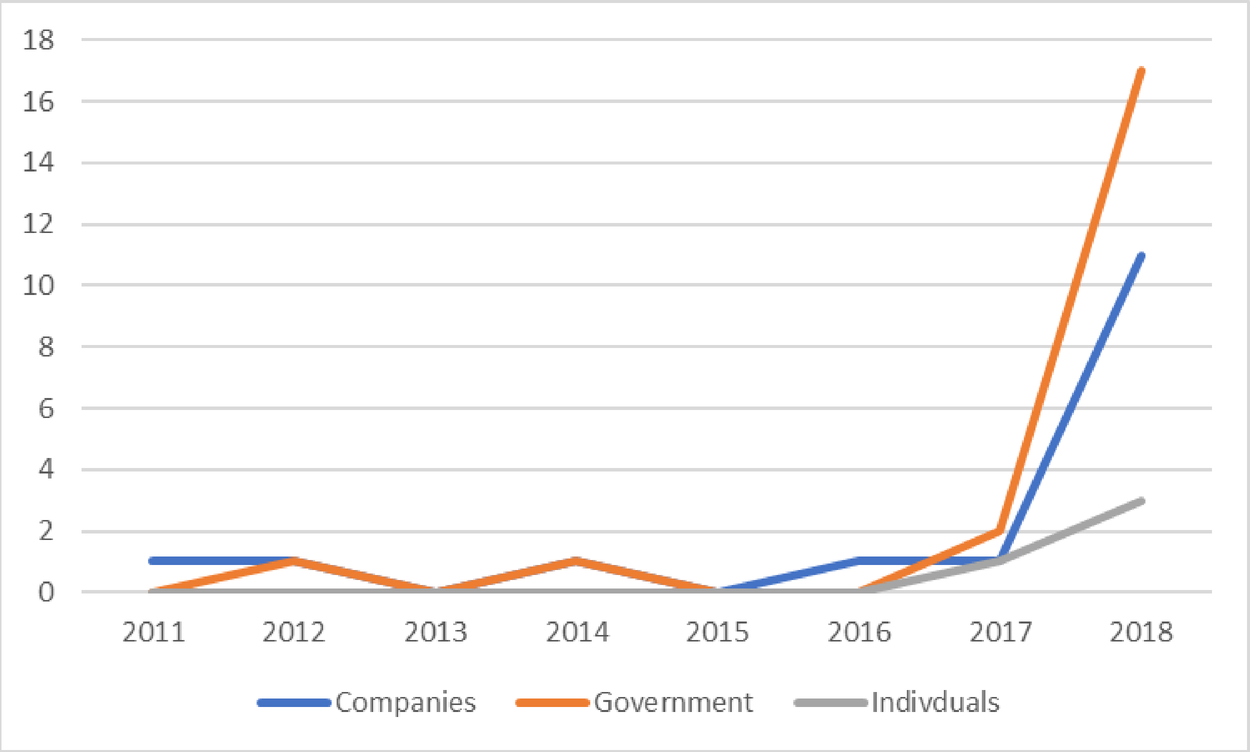


Figure 3. Amount of cases by actor for the category ‘Access’ over time.

As the figure shows, the government was the actor that violated privacy in most of the cases, followed by companies. Both show a steep increase in cases from 2017 to 2018. The least amount of cases is in the ‘individuals’ category. I will now go through all cases, starting with cases where the government was accused of violating privacy, which are 21 cases.

Of the 21 cases where the government was involved in the violation of privacy, only four occurred prior to 2018. All four cases involve the use of digital databases. The 2012, 2014 and one of the 2017 cases revolve around an individual being unable to gain access to his or her own data, which is stored in a database controlled by the government. In these cases, a governmental body stored certain personal information of an individual in a database. In the 2012 case, an individual seeks asylum, which is denied. He wants to know why and tries to gain access to the data where this decision is based on, which is personal information about him. The two other cases concern individuals that want to access their own personnel file, both are working for a governmental body. In all three cases, the storage of the data in a database takes the control over the data away from the individual, which is an example of the third mechanism of TechnoMoral Change: the ability of technology to destabilize morality by altering roles and relationship. There has been a power shift due to the technology to store data in databases. As digital storage makes it easier to store large amounts of data and to control who has access to that data, it can take the power to control who has access away from the individual. This also results in an inability for the individual to act on the data, for example in the case of the asylum seeker. The fourth case from before 2018 concerns a request for data within a governmental database. The data that is requested can possibly be traced back to individuals, which violates their privacy. This case is different from the other three, as in the former cases, privacy is violated because the government does not allow access to data, while in this case privacy is violated because the government does allow access. This is an example of the first mechanism of TechnoMoral Change, the ability of technology to create new opportunities, as the existence of a digital database makes it way easier to gain access to the stored data, compared to an analog one. The cases from before 2018 thus all involve database-technologies and the majority involves the third mechanism of TechnoMoral Change, the ability of technology to alter roles and relationships.

For the 17 cases within the category ‘government’ from 2018, the large majority, 14, also involve the use of a database. For 8 of those cases, the only TechnoMoral change mechanism involved was the first one, the creation of new opportunities, as these cases involve requests for data within a database. The technology that makes it possible to store information in a database and to control who has access to this data, creates the opportunity to request, give or gain access. These cases are like the last case mentioned in the previous paragraph where data is requested from a governmental database, as privacy is possibly violated as the government gives access to private, stored data.

Besides the first mechanism of TechnoMoral Change, 4 other cases involving giving or gaining access to databases by the government also involved the second mechanism of TechnoMoral Change, the introduction of new stakeholders. An example of these cases is a case where the Dutch Tax Authority wanted access to data from the users of Stichting Museumjaarkaart, to track tax evaders. In another case, the governmental body that supervises student loans requested travel data by a third party, the new stakeholder, to check whether a student was entitled to said loan. The other two cases involve a request towards the Tax Authority by a housing corporation. In these cases, a new stakeholder is included due to their database. Because of the digital database where the Stichting Museumjaarkaart stores the behavior of their card-users, the Tax Authority is interested in accessing their data to track tax evaders, as the visits to certain museums might indicate where a certain individual lives. Without the digital storage of data, it is impossible to easily track the behavior of card-users and to store and share this data. The technology thus enables the Tax Authority to access new data sources, from new stakeholders. This is a new use of technology and a new type of complaints compared to the earlier cases. Of the 2 remaining cases, one involves the third mechanism of TechnoMoral change and is alike the three cases from before 2018 where this mechanism was involved. The other one involves a request of access by the government for data on income, among other things. The individuals that receive these requests do not comply as they are afraid of the consequences this might have for their private lives. This is an example of the fourth mechanism of TechnoMoral Change, the ability of technology to gain insight into new consequences of actions.

There are 3 cases in 2018 in the category ‘government’ that do not involve the use of databases. This is a change compared to the earlier years, where all cases involved the use of a database. In 2018, 2 cases involve the publication of information on the internet, thus giving others access to the published data. In one of them, the cases file only states the publication of ‘personal information’ and the complaint of the appellant that this might lead to identity fraud. The case does not involve a more detailed explanation of this. In the other case, the government publishes about bad healthcare in order to inform the public about the quality of healthcare. One of the healthcare providers involved argues that, due to the reach of the internet, this has far-reaching consequences that will not result in better healthcare. The argue that their employees will also read the publication, which will negatively impact their motivation and because of the detailed information that is in the publication. Due to this, the publication has consequences for the private life of the employees and their privacy. In this case, due to a technology, the internet, there are new, or further-reaching, consequences of the actions of the healthcare provider, which is an example of the fourth mechanism of TechnoMoral Change.

The last case involves the use of an algorithm. In this case, the government uses an algorithm for automized decision making on giving out permits, for example for the construction of roads. However, the party involved, 'Natuurmonumenten', argues that they should be able to gain access and insight into this kind of decision making, due to the consequences the decision has for them and their property. The algorithm, the automized decision making and the technology behind it create new opportunities to have a more efficient way of decision making, but this makes it unclear for the disadvantaged party to know why this has happened. This is an example of the first mechanism of TechnoMoral Change, the ability of technology to create new opportunities and responsibilities.

In summary, 21 of the 40 cases in the category 'access' involve a privacy violation by the government. The vast majority of those cases, 17, are from 2018. Database-technology is the most common technology among the cases as it is involved in 18 cases, while the most common TechnoMoral Change mechanism is the first one, the ability of technology to create new opportunities and responsibilities, as it is involved in 11 cases. However, prior to 2018 the majority of the cases, three of the four, involved the third mechanism of TechnoMoral change, the ability of technology to alter roles or relationships. There has thus been a change over time, as in the majority of cases prior to 2018, privacy was violated due to the ability of databases to change who controls and has access to data, through the third mechanism of TechnoMoral change. In 2018, privacy was mainly violated due to the ability of databases to create new opportunities, as the existence of databases makes it possible to request data. Besides this, four cases involved the second TechnoMoral Change mechanism, the ability of technology to introduce new stakeholders. The least common way of violating privacy was by gaining access to databases from new stakeholders, violating the privacy of the people in the database.

The second biggest type of actors within the access category are companies. 16 cases involve a company, 10 of these cases are from 2018, the remaining five are from 2011, 2012, 2014, 2016 and 2017.

The first three cases, from 2011, 2012 and 2014, all involve the first mechanism of TechnoMoral Change, as they involve a technology that creates the opportunity to (more easily) access information, but all involve another technology. The case from 2011 is against a hospital. Several employees had gained access to the medical file of the accuser, possibly without professional reasons. This was a violation of the privacy of the accuser. She files a court case because she wants to know who had access to her file. The database technology made it way easier to access the file, compared to an analog system. The database technology also makes it easier to store more data for a longer period of time, thus making the file richer. The database technology thus creates an easier opportunity to access the data, which violates the privacy of the accuser, which is an example of the first mechanism of TechnoMoral Change. In the case from 2012 a website, Geenstijl, shared a link to non-published photos from a photoshoot. There is a dispute between the owner of the photo's (the publisher) and the website, about the copyright, while it is also considered a violation of the privacy of the person in the photos. The technology involved is the internet, which creates the opportunity to give a large amount of people access to the photos, and thereby, in this case, violating the privacy of the person in the photos. The 2014 case involves a dispute between an employee and their former employer. After the employee announced his resignation, the employer gained access to his mobile phone and laptop and read his personal emails and messages. The technologies involved are the mobile phone and the laptop and the email and message software on it. These technologies create an opportunity to communicate with others, but its misuse, in this case by unauthorized access, can be a violation of privacy. While these cases involve the first mechanism of TechnoMoral Change, the 2016 case involves the fourth mechanism, the ability of technology to result in new consequences of actions. The privacy violation concerns the publication of personal information on the internet, thus making it accessible for a large public.

While only one of the cases prior to 2017 involves a database, 10 out of the 12 cases in 2017 and 2018 involve database-technologies. 9 of those 10 cases, involve the first mechanism of TechnoMoral Change as they involve a database technology that creates the opportunity to more easily give or gain access to personal information. The case from 2017 concerns a complaint from several healthcare professionals and organizations against the company that is responsible for the ELPD, a new implemented digital way for sharing medical files. They are uncertain about the security of the system and argue that this causes the system to be a violation of the privacy of patients recorded in it. The technology of digital databases creates new opportunities in sharing and accessing information, as it becomes easier and more efficient. It however also creates new responsibilities, as the privacy of the patients in the systems is at stake if the system is not secure. It thus involves the first mechanism of TechnoMoral Change.

An example of the eight cases from 2018 that involved a database and the first mechanism of TechnoMoral Change is a case concerning a dispute between two companies where an employee moved from one company to the other and was asked by her new employer to copy the database with clients from her former employer. The database technology creates this opportunity, as it is nearly impossible do copy a full database of analog data. This also violates the privacy of the people in the database, as a third party is now able to access their data. The other seven cases also involve a database that creates new opportunities and responsibilities, which is the first mechanism of TechnoMoral Change. In all cases, this led to the violation of the privacy of the subject of the data in the databases.

Two other cases in 2018 involve the third mechanism of TechnoMoral Change, the ability of technologies to alter roles and relationships, for example a case from 2018 that concerns a dispute between an employer and a former employee, who wants to access his personnel file. The database where this file is stored is a technology that alters the role of owner of the personal data of the employee. In another case from 2018 that involved databases a former owner of a company became unable to access his own files, after selling the company, due to the secured digital database. This is an example of the fourth mechanism of TechnoMoral Change, as there are new consequences of actions.

In the final case of 2018, both a company and an individual are sued. It concerns a case where a private video of a Dutch celebrity went viral. The company, Geenstijl, and an individual shared a link to the video and Google keywords that would allow anyone to find the video. The internet is the technology that makes it possible to give and gain access to the video, it creates the opportunity to share it with a large amount of people, the creation of opportunities is the first mechanism of TechnoMoral Change. Due to the contents of the video and people that gained access to it, the privacy of the celebrity was violated.

To summarize, the majority of the cases, 12 out of the 16 cases, within the category ‘access’ that involve a privacy violation by a company involves the first mechanism of TechnoMoral Change, the ability of technologies to create new opportunities and responsibilities. The most commonly involved technologies are database-technologies, which is involved in 12 of the 16 cases. Four cases involve another technology and three of those cases occurred prior to 2017. Thus, the technologies the involved are subject to change over time, as databases become more common in later years being the technology responsible for the creation of new opportunities for companies to access data, resulting in the violation of privacy.

There are four cases in the category ‘individuals’. One of them was already discussed above, as it was also in the category ‘companies’. In this case the first mechanism of TechnoMoral Change is involved, as the opportunities created by the internet led to a privacy violation, as people gained access to private data. This was a case from 2018. Two other cases are also from 2018. In both an individual requires access to data that is in a database from a company. In one of the cases, the individual wants personal information from advertisers on Facebook. Facebook considers this a privacy violation and the request is denied. The information is stored in a database, which therefore is the technology involved. The database creates the opportunity to access the information, but providing this access is considered a privacy violation by Facebook. This thus involves the first mechanism of TechnoMoral Change. The other case is similar, it also involves a request from an individual to gain access to personal information, stored in a database by a company. The company denies this request, as they consider it a privacy violation of the people in the database. The last case is the only case in this category from 2017 and involves a request from an individual to gain access to personal information, stored in a database by a company, which is an investment company. This is denied by the company as they consider it a privacy violation of the people in the database. All cases thus involve the first mechanism of TechnoMoral change, the creation of new opportunities and responsibilities. Three cases involve database-technologies, one involves the internet and social media. There is no notable change over time.

To summarize, the vast majority of cases where technologies enabled privacy violations by enabling access to private data involved databases asout of 40 court cases, 33 involved a database. Over the years, the increase in cases where privacy is violated by giving or gaining access to personal information mostly involved the government, with 21 cases, and companies, with 16 cases. In 26 of the cases, the first mechanism of TechnoMoral Change was involved. It thus seems that database technologies are able to create new opportunities or responsibilities for accessing information. This results in the responsibility to secure the data and in the responsibility to critically evaluate who has access to certain data, as unlawful or unauthorized access could be considered a violation of the privacy of the people in the database. The steep increase in cases show that the occurrence of this type of issues has increased, especially in 2018.

Another mechanism of TechnoMoral Change that is apparent in the 'access' cases and is connected to the increase in database-related privacy violations is the second one, the introduction of new stakeholders. This mechanism is a result of databases due to the possibility for, for example, the Tax authority to use new data-sources with data that has been collected by third parties. The third mechanism of TechnoMoral Change, altered roles and relationships could also result from the use of databases. In the cases that involve this combination of technology and mechanism, the storage of data of an individual in a certain database leaves the individual unable to access the data or to control who has access to the data.

Other technologies that are less common in this category are for example the internet. However, the internet is relatively common among cases that involve the fourth mechanism of TechnoMoral Change, the ability of technology to result in new consequences of actions. Three out of four cases that involved this mechanism, also involved the internet. The cases show that the internet makes it possible to make information accessible to a large public, which leads, in this cases, to new consequences for the subjects of the information.

Store

The second biggest category, along with 'Analyze' is 'Store'. It refers to cases where the complaint was about the storage or registration of certain information. These complaints are about whether the registration is right or just. This can be a privacy violation if it has consequences for someone's private life, if stored information is outdated or if an individual no longer want his or her information stored. It also involves cases were stored data is supposed to be anonymous but can still be traced to individuals. Another example is a case were an individual wants information about her health, which is highly private, to be deleted from a governmental database, while the government insists that the data needs to be stored for ten years. Another example is a case where an individual is unable to get a mortgage, due to outdated stored data about his credibility. The complaints in this category are not about the initial collection of the data, they just don't want it registered anymore or want to see it changed.

There are 18 cases in this category, which is 20,93% of cases. 14 of those cases are from 2018, which is 77,78% of the cases within this category. Figure 4 gives an overview of the cases over time, grouped by type of actor.

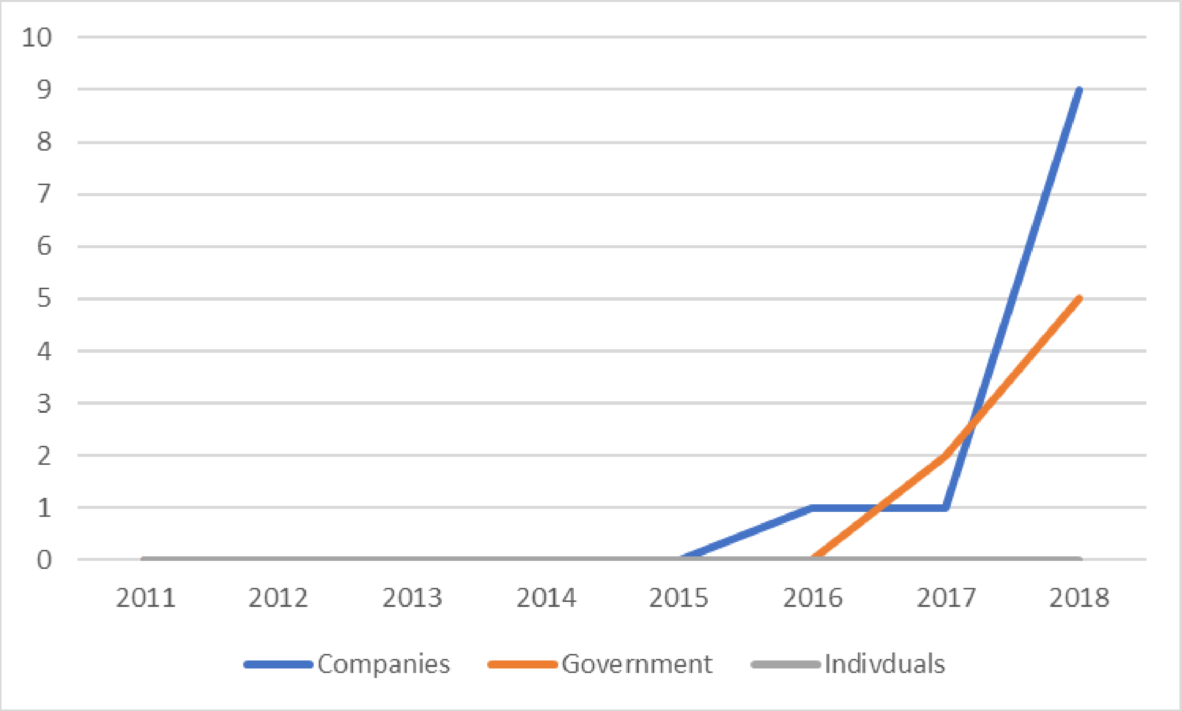


Figure 4. Amount of cases by actor for the category 'Store' over time.

Figure 4 shows that there is a steep increase in the amount of cases where a company was involved between 2017 and 2018. There is also an increase in cases where the government was involved between 2015 and 2018. None of the cases concern a violation by an individual. As most cases are within the 'companies' category, the analysis will start with these cases.

11 of the 18 cases within the 'store' category involve a privacy violation by a company. One case is from 2016, one case is from 2017 and the other cases are all from 2018. The cases from 2016 involves an unjust registration of medical information of an employee by an employer. The registration was stored without consulting a doctor and has impacted the employee's personal life. The employer insisted that the registration was necessary to ensure that the work schedule was filled, as the systems that make the schedule and the registration of sick leave are connected. This case involves the first mechanism of TechnoMoral Change, the ability of a technology to create new opportunities or responsibilities. While technology creates the opportunity to more effectively fill the schedule, the employer has the responsibility to register the right information. If this goes wrong, it might have consequences for the employee in his personal life, as the amount of sick leaves influences his credibility as an employee.

The case from 2017 and 6 of the cases from 2018 involve a dispute over a possibly unjust 'BKR-registration'. In the Netherlands, it is registered when someone takes out a loan.

Banks or other possible lenders can check within this system if someone is credible. If someone has a history of problems with paying off loans, a bank may not be willing to lend that person money. However, the registration may be outdated. It could be that the current financial situation of an individual is significantly better than what can be expected from the database of registrations. If this is the case, the stored data withholds the individual from getting a loan, as for example a mortgage. The technology to store this information, the database, thus impacts someone's private life. The TechnoMoral Change mechanism involved in cases like this is the fourth one, the ability of technology to result in new consequences. Due to the registration in databases, earlier actions by individuals, like being reluctant to timely pay off past loans, now have the consequence that they are unable to get a mortgage. The individuals in those seven cases argue that the stored information is outdated and want to see it removed, as it affects their private life. Two other cases are similar to this, but involve a registration in a register for fraud. This also impacts the private life of the individuals. Moreover, they argue that the registration is unjust and thus should be removed.

One case from 2018 involves a dispute between an employee from the Utrecht University and the university. The employee was registered within a certain department that was being disbanded. He insists that he was working within another department, that was still operational. Due to the way he was registered within the database with employees, he was dismissed. If he was properly registered, he would still have had his job. His state of employment effects his private live and wrong registration within the database with consequences like this is thus a violation of private life. The TechnoMoral Change mechanism involved is the first one, as using a database like this and basing decisions on it is an opportunity for the university to work more efficient. However, it gives the university the responsibility to make sure that the data is registered properly. Incorrect storage of data might impact the private life of the people in the database.

In summary, most cases involved an incorrect storage of data within a database, leading to new consequences of earlier actions and impacting the private life of the subjects of the data. Therefore, the fourth mechanism of TechnoMoral Change was most common in these cases.

There are 7 cases where the government was involved as the accused party. Of which, two cases are from 2017. One of the two involves a dispute between a woman and the Dutch Health Care Inspection. The Inspection has stored medical information of the woman. This type of data usually gets stored for ten years before being removed. The woman argues that she was not made aware of this time period and thus did not gave permission to do so. She wants to see her data removed as she considers it a violation of her privacy. This involves the first mechanism of TechnoMoral Change, the creation of new opportunities, as the database technology created the opportunity to easily store this kind of data for a long period of time. This violates the privacy of the subject in this case. The other case from 2017 also involves the first mechanism of TechnoMoral Change, as it involves a privacy violation of people within the mental healthcare. Two health interest groups file a case against the governmental body that registers personal information of those people in mental healthcare The governmental body state that the data within the database is anonymous, while the interest groups argue that the data can be traced to individuals. This violates the privacy of the individuals in the database. The database technology creates new opportunities for the storage of data, but if the registration is unjust, it might violate the privacy of the people within the database.

Three of the five cases in 2018 where the government was accused of a violation concerning the storage or registration of data concern cases where the registration leads to new consequences of actions, which is the fourth mechanism of TechnoMoral Change. Two of those cases involve a registration of aggressive behavior. In both cases, the appellant argues that the registration is unjust and that it impairs them in their personal life, as several other governmental institutions are able to look them up in the database. The database technology makes it easier to store information that is accessible by multiple institutions, in these cases resulting in new consequences of their actions. If this registration is unjust, it is a violation of the personal life of the subject, as it might heavily impact their life. In the third case where an unjust registration leads to new consequences, the UWV, the Dutch Employee Insurance Agency, improperly registered the medical conditions of a woman. As she has an upcoming court case concerning personal injuries, she wants the conditions removed from the registration of the UWV. The improper registration of the medical data has new consequences, as it will be used in the upcoming case, thus impacting the personal life of the woman.

The other cases from 2018 concern the creation of new opportunities, the first TechnoMoral Change mechanism. One is a case against the government from a woman that is unable to get a visa. When applying for a visa within the European Union, you get registered in a database (VIS). Countries within the EU can deny a visa based on the information in that database, even if you plan on visiting a different country. The woman filed a case against the Dutch government because she was denied access to The Netherlands by Hungary, based on the registration in the database. She considered it a violation of her privacy that The Netherlands stored her data in the database. The database technology creates the opportunity to easily store data and share it between countries, which in this case results in a violation of privacy. The last case concerns a case against the mayor of Den Haag, who wanted to implement a registration system where data concerning sex workers could be stored. The Authority for Personal Data argues that this violates the privacy of those sex workers, as they are obligated to comply. Database technology creates the opportunity to efficiently store data, but in this case, this violates the privacy of the people in it.

Again, all cases involved a database, mainly in combination with the fourth mechanism of TechnoMoral Change, the ability of technology to give insight in new consequences to actions. The registration of individuals in databases by the government impacts their life, as it creates new consequences of actions.

To summarize, all of the cases in the 'store' category involved the use of a database, which makes sense as this is where information is stored. The increase of cases in 2018 is mostly due to an increase in cases involving the fourth mechanism of TechnoMoral Change, the ability of technology to give new insight into the consequences of actions. Before 2018, this mechanism was involved in 25% of the cases, while in the involvement of this mechanism in 2018 was 78,57%. This contrasts with the category of 'access', where there was an increase of cases involving database technology that created new opportunities and responsibilities, which is the first mechanism of TechnoMoral Change.

Analyze

Along with 'Store', 'Analyze' is the second biggest category of privacy violations. It refers to cases where personal data has been analyzed or used for another purpose than initially intended. It differs from the other categories because the data is usually processed. The other categories usually concern accessing, collecting or storing 'raw' data. Complaints within this category are thus specifically about processed data or data used for another purpose than intended. This, for example involves complaints about Google search results, as Google uses an algorithm to determine which result comes first, and therefore processes the data before displaying it. It also involves cases of identity fraud, as this involves the use of data for another purpose than intended and violates the victim's privacy. Another example is a case where a municipality wants to analyze every product of a company that processes metal, to ensure that it is not stolen. For the analysis, the owner of the company is obligated to hand over personal data of himself and his customers. The owner does not want to be part of the analysis due to this, as he considers it a violation of his privacy and the privacy of his customers.

There are 18 cases in this category, which is 20,93% of the total amount of cases. 12 of those cases are from 2018, which is 66,67% of the cases within this category. Figure 5 gives an overview of the cases over time, grouped by actor.

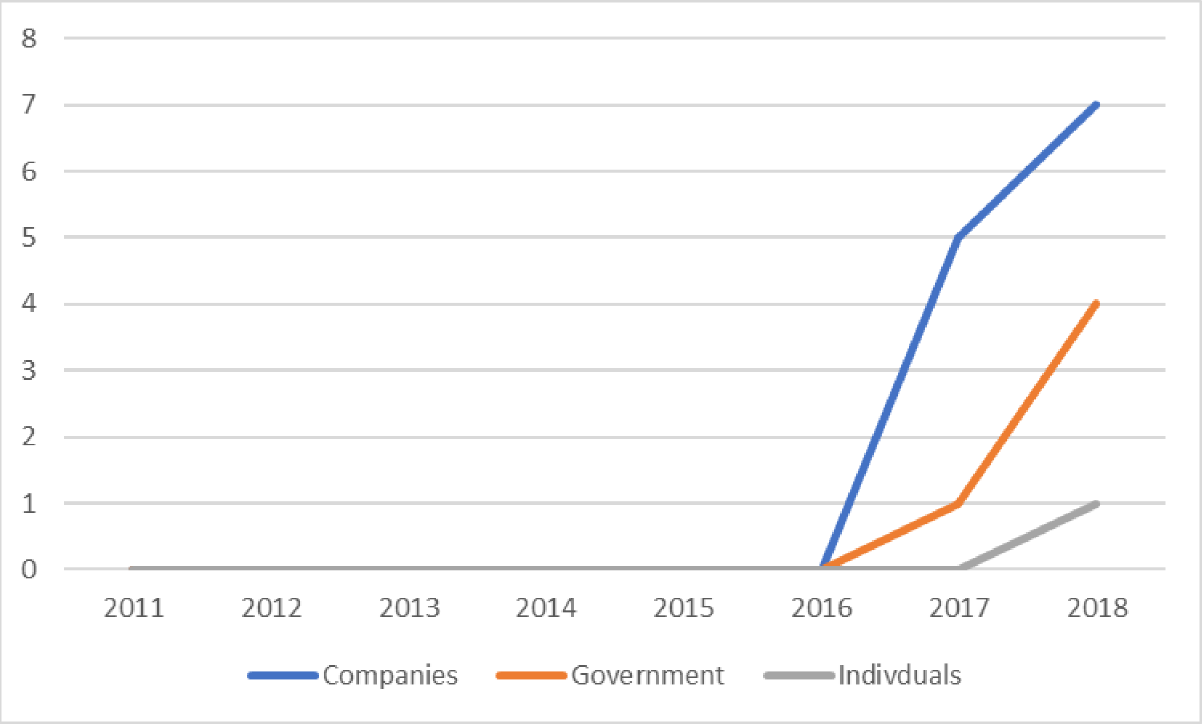


Figure 5. Amount of cases by actor for the category 'Analyze' over time.

Figure 5 shows that the biggest increase is between 2016 and 2017, for cases where a company was involved. There is a slight increase for cases where the government was involved between 2016 and 2017. All three types of actors show an increase in the amount of cases between 2017 and 2018. As most cases involve companies, this category is analyzed first.

Of all the cases within the 'analyze' category, 12 involve a case where a company was accused of violating privacy by analyzing data or using it for another goal than was intended. This equals 66,67% of the cases. Five of those 12 cases are from 2017. Three of those cases are against Google. The appellants in these cases sue Google because of search results that are shown after googling their name. They want to see these results removed and sue Google because the algorithm they use results in displaying unwanted hyperlinks that involve their names. Due to the search algorithm, a technology, their actions have new consequences, as certain personal information can more easily be found online. The creation of new consequences is the fourth mechanism of TechnoMoral Change. The accusers argue that the ease with which their data can now be found has consequences for their personal or professional life and can thus be considered a violation of their privacy. Another case from 2017 involves a complaint against a law firm. The law firm analyzed governmental documents in search for possible clients that might need legal counsel. If they found a possible client, they would send a letter to inform the possible client about possible legal counsel. One of the people that received a letter filed a case against them. She did not like it that the law firm used the data from governmental documents to contact her and was very upset when she received the letter. She considers it a violation of her privacy that they processed her data. The possibility to efficiently analyze documents is an opportunity that is created by technology, which in this case result in a violation of privacy. The creation of opportunities, or responsibilities, by technologies is the first mechanism of TechnoMoral Change. The other case from 2017 that involves the first mechanism of TechnoMoral Change concerns a dispute between an association of general practitioners and a couple of healthcare providers, who set up a system to process and analyze medical information from patients. The association considers this a violation of the privacy of the patients. Through technology, it is possible to process and analyze this data, but it can be considered a violation of privacy. For the latter two cases, it was unclear what kind of technology was used to analyze the data. It could be that there was specialized software to do this, but this is unclear.

Of the cases where a company was accused of analyzing data or using data for other purposes than intended, seven are from 2018. Six of those cases are against Google, involving a complaint about the search results that are shown after searching for the name of the appellant. They all involve the use of an algorithm that results in new consequences to former actions. The last case from 2018 is between an individual and a television studio. For a television program on fraud, someone went undercover to expose the individual. The television studio uses different kinds of data for their program and while the individual is a fraud, she feels like she is entitled to decide what kind of data will be shown in what way. She, for example, wants her head to be blurred and her voice to be distorted. She does not sue the company because of the collection of the data, she is okay with broadcasting the data, but she wants the data to be processed in a certain way. Without these alterations, she considers it a violation of her privacy, as there are new consequences to her actions if the unaltered version is broadcasted.

For the 12 cases where a company violates privacy by analyzing or using personal data, 10 involve the fourth mechanism of TechnoMoral Change, the ability of technology to give new insights and thus result in new consequences of actions. This is mostly due to the 9 cases against Google. Those cases involve a technology, the algorithm of the search engine, that results in new consequences of actions. Both cases that involve another mechanism of TechnoMoral Change involve the first one, the creation of new opportunities and responsibilities and both are from 2017.

There are 5 cases that involve a privacy violation in the 'analyze' category by the government. Four of those cases are from 2018 and one is from 2017. The case of 2017 is one of the most important cases regarding automatic decision making in The Netherlands. The case involves a dispute between a foundation and a governmental body regarding the use of a computer program to decide whether certain permits should be granted. As this is one of the first times automatic decision making is used in processes like this, the foundation is concerned about the rightful use of the technology. They argue that in cases like this, where data is analyzed and processed to come to a decision, it should be clear for the subjects that are impacted by that decision how the program works. If stakeholders that are impacted by the decision are unable to know how the program works and thus how the decision is made, they are unable to act on it, which can be considered as a violation of their private life. The technology that makes the automatic decision making possible hereby creates new opportunities for a more efficient way of decision making, but also gives the users of the technology new responsibilities. This is an example of the first mechanism of TechnoMoral Change, the creation of new opportunities and responsibilities.

Of the four cases from 2018 in the 'analyze' category where the government was involved as the accused party, two concern the use of data that is collected by the NSA, an American intelligence agency, by the Dutch government. In both cases, the complaint against the Dutch government is about them using it for their own analyses. In both cases, the accusers argue that using the data is a violation of the privacy of the people that are in the NSA-databases. Technological developments have made it easier to analyze large amounts of data, this is a new opportunity created by the technology, which is an example of the first mechanism of TechnoMoral Change. However, carelessly analyzing and using those data might result in a violation of the people whom the data is about. This is what the accusers in both cases are afraid of. The other cases from 2018 also involve the first mechanism of TechnoMoral Change. Central to these cases is a dispute between the government and a former governmental employee, who argues that the data-analysis, involving his personal data, that led to his release was unlawful. This is also a case that involved a data-analysis technology, which created new opportunities for the government to efficiently assess their employees' performance. Without this technology, it probably took more time to do assess the performance of their employees. In the last case from 2018, a company is asked to comply in an analysis by a municipality to ensure that their wares are not stolen. Personal data from the company and their customers is one of the kinds of data that have to be analyzed. The company considers this a privacy violation and does not comply. Technology that makes it possible to analyze this sort of information, presumably databases and software that compares between databases, includes the company as a new stakeholder in fighting crime. The inclusion or introduction of new stakeholders is the second mechanism of TechnoMoral Change.

There is one case from 2018 in the 'analyze' category where an individual is the accused party. This is an identity-fraud case, where the accused party used photos from the victim for its own social media account. This violates the privacy of the victim. Technology like the internet and social media creates the opportunity to violate privacy like this. This is an example of the first mechanism of TechnoMoral Change.

To summarize, two-thirds of the cases in the category 'analyze' are cases where a company was the accused party. This is mainly due to the cases against Google. These cases all involve an algorithm, which is the main technology involved. This technology is also seen in the cases where the government is the accused party, as one of those cases involves automatic decision making. Analyzing data using algorithms therefore might violate the privacy of the individuals whose data is used or whose lives are impacted by the outcome of the algorithm. In most cases, the TechnoMoral Change mechanism involved is the fourth one, the ability of technology to give insight in new consequences. A lot of the cases that involve an algorithm eventually lead to new consequences for the parties involved. Another important mechanism in this category is the first, one, the creation of new opportunities and responsibilities. It seems that data-analysis technology creates new opportunities for companies and governments, mainly to more efficiently operate their businesses. However, this may pose a threat for privacy, for example because it is unclear how certain analyses or algorithms work, while their impact might be considerable.

In comparison to ‘access’ and ‘store’, the technology that this category highlights is the algorithm, whereas the former categories mostly involved databases. The TechnoMoral Change mechanism that is mostly involved is the fourth one, new insight in the consequences of data. This is similar to ‘store’. The second most involved mechanism is the first one, which is similar to ‘access’.

Collect

‘Collect’ is the smallest category of privacy violations. Collect refers to cases where the complaints of the accusers focused solely or mainly on the collection of the data. It differs from the other categories as it involves cases where there has been an unjust collection of data and the collecting itself, whether the right data is collected or the way of collecting is disputed. Thus, it involves data that is newly collected, ‘first-hand’-data, collected for a specific use. An example is a case where an insurance company asks another company to monitor someone suspected of fraud. Another example is the collection of biometric data, like fingerprints, by the government. Both cases can be considered a violation of privacy if the subjects are unknowingly being monitored or if the collecting is mandatory. It also involves cases where the collected data was already freely available. An example is a case where the retail price of a car is collected by the Dutch tax authority, which can be considered a privacy violation as this affects the financial situation of the owner of the car, which impacts his private life. He argues that the collected data is wrong, as his car has been used and is no longer worth his retail price.

There are 10 cases in this category, which is 11,63% of the total amount of cases. 7 of those cases are from 2018, which is 70% of the cases in this category. Figure 6 shows the distribution of the cases over time, grouped by actor.

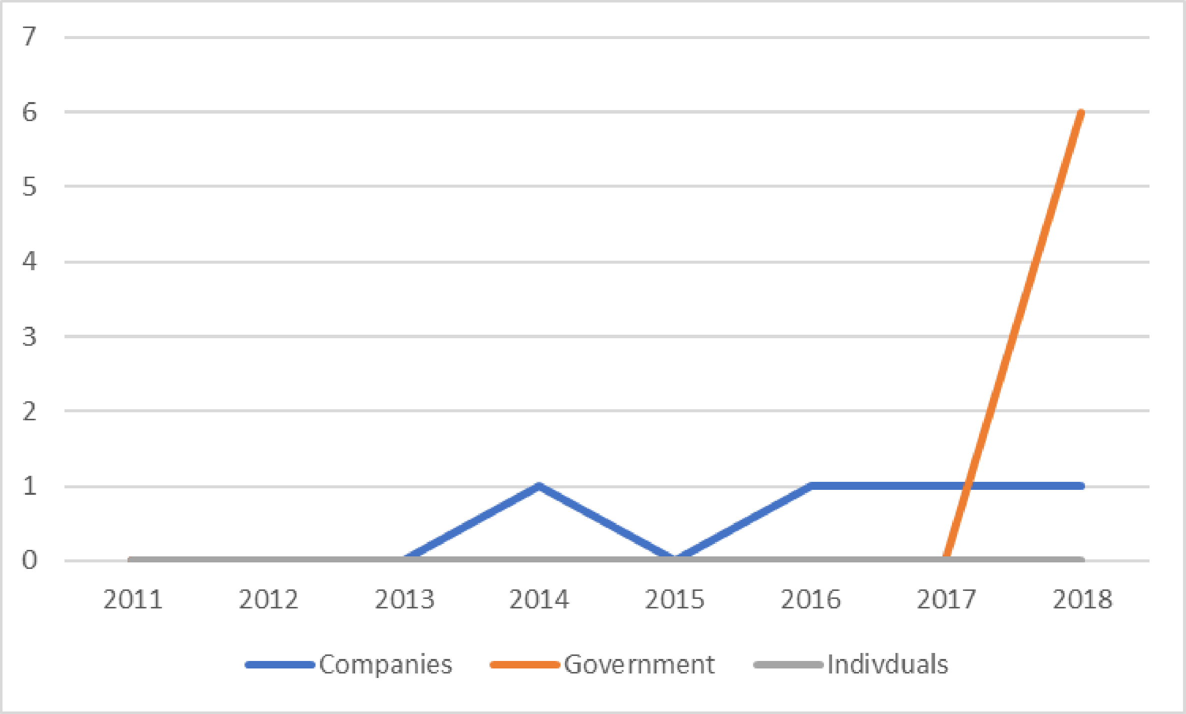


Figure 6. Amount of cases by actor for the category 'Collect' over time.

Figure 6 shows that all cases in this category involve violations by the government or by companies, with respectively 6 and 4 cases. It is notable that all of the cases involving the government are from 2018, while the cases involving companies are spread out over 4 years. This is the biggest relative difference between both actor-categories along all privacy violation-categories. As most cases involve the government, these will be analyzed first.

Of the 10 cases in the 'collect' category, 6 involve a privacy violation by the government through the collection of data. All of these cases are from 2018. The technology most apparent is databases, as 4 cases concern a collection of data that is already available and accessible. An example is the case where the Dutch tax authority collects the retail price of a car to work out taxes. The owner of the car argues that the data collected is not the right price, as his car is worth less. Due to the impact this has on his financial situation, he considers it a violation of his private life. Three of those cases involving a database involve the Dutch tax authority. The fourth case concerns the collection of data by the Competition Authority. This authority collects data from companies and selects part of the data to assess for their research. The companies are able to object if they think that this collection or selection does not comply with the law. In this case, the company objects, as they argue that the collection violates the privacy of its employees, among other things. All 4 cases that involve a database are an example of the first TechnoMoral Change mechanisms, the ability of technology to create new opportunities, as the database-technology makes it easier to collect data. However, it also creates new responsibilities, as the collector must ensure that the right data is collected from the databases.

The other two court cases where the government is accused of violating privacy are cases where first-hand data is collected. One of the cases concerns the legality of collecting biometric data, like digital facial images and fingerprints. Technological developments like face- and finger-scanners create the opportunity to collect biometrical data but can be considered a privacy violation. The technologies involved are scanning devices, while the TechnoMoral Change mechanism involved is the first one, the creation of new opportunities and responsibilities. In the other case, the government collected data on the use of electricity as evidence in a case against a suspected hemp grower. This collecting was considered unjust and thus a violation of privacy. Technology that tracks the flow of electricity makes it possible to collect this data, it is thus an example of the first mechanism of TechnoMoral Change, the ability of technology to create new opportunities and responsibilities.

The cases that involved a privacy violation by the government in the category ‘collect’ thus all involved the first mechanism of TechnoMoral Change, the ability of technology to create new opportunities and responsibilities. Most cases involved database-technologies, while other notable technologies are technologies that make digital scans of body parts and tracking technologies. As all cases are from 2018, the only change over time is in the amount of cases.

Of the 10 cases in the ‘collect’ category, 4 involve a privacy violation by a company by collecting data. The cases are from 2014, 2016, 2017 and 2018. The three cases from 2014, 2017 and 2018 are alike, as all involve firsthand-data collection of an individual by a company. In the case from 2014, an insurance company suspects fraud and hires an agency to investigate her. They observe her, film her and collect data concerning her internet-usage. She considers this collection of data a privacy violation. This case involves the first mechanism of TechnoMoral Change, the ability of technology to create new opportunities and responsibilities, as technological developments like internet-trackers create the opportunity to collect data concerning her internet-usage. It also involves the second mechanism of TechnoMoral Change, the introduction of new stakeholders, as the agency that is hired specializes in these kinds of data-collection, which is possible due to developed technologies.

The 2017 case involves the same kind of collection, as an employer hires an agency to collect data from an employee. The same kind of technologies and the same TechnoMoral

Change mechanisms are involved. In the 2018 case, an insurance company investigates an individual by itself, without help of another stakeholder. Thus, the case has the same characteristics but does not involve the second mechanism of TechnoMoral Change.

In the 2016 case, the messenger application WhatsApp is accused of collecting data from their users concerning personal information from their contact lists, even if the individuals in that contact list do not use WhatsApp. They are thus collecting data from non-users, who are quite unable to do anything about it. This is considered a privacy violation. WhatsApp, mobile phones and other technologies that are used by WhatsApp to collect the data are the result of technological developments. These developments are able to create new opportunities, which are used by WhatsApp to collect the data of non-users, which includes them as new stakeholders. This case thus involves both the first TechnoMoral Change mechanism, the creation of new opportunities and responsibilities, and the second one, the introduction of new stakeholders.

The cases that involve a privacy violation in the category ‘collect’ by a company are thus al quite alike, as all involve the first mechanism of TechnoMoral Change, the ability of technology to create new opportunities and responsibilities, and most of them involve the second mechanism, the introduction of new stakeholders. In three of the cases, data from an individual is collected by a company that has a reason to investigate that individual, this involves technologies like tracking devices and video cameras. The fourth case concerns large-scale data-collection by a mobile phone application, which is different from the other three and involves different technologies, like mobile phones and applications.. There are no notable differences over time, as the cases are relatively equally distributed over time, compared to other categories, and the majority of cases involve the same kind of technologies and TechnoMoral Change mechanisms.

To summarize, 6 of the 10 cases in the category ‘collect’ involve a privacy violation by the government, mainly due to cases against the Dutch tax authority. All of the cases are from 2018 and mainly involve database-technologies that create new opportunities and responsibilities, which is the first TechnoMoral Change mechanism. The 4 cases that involved a privacy violation by a company involved other technologies, like tracking technologies and cameras. They also involve the second mechanism of TechnoMoral Change, the introduction of new stakeholders. The cases are more equally distributed over time and show no increase in later years, which contrasts with the 6 cases where the government is accused of violating privacy.

In comparison with the other three categories of privacy violations, the database technology is also most apparent in both ‘access’ and ‘store, while in ‘analyze’, algorithms are the most common technology. While for ‘analyze’ and ‘store’ the fourth mechanism of TechnoMoral Change, gaining new insight in consequences of actions, was most common and for ‘access’ the first mechanism, the creation of new opportunities and responsibilities was most common, ‘collect’ involves both the first mechanism and the second one, the introduction of new stakeholders. It seems that technological developments that create the opportunity to collect certain data, or to make this easier, also introduces new stakeholders, for example agencies that specialize in data-collection, possibly resulting in the violation of privacy.

Conclusion and discussion

As is mentioned before, the increase in data-collection technologies and the use of those technologies by both governments and companies poses a threat to privacy. The theory of TechnoMoral Change states that technological change is able to influence morality and vice-versa. This research aims to answer whether our notion of privacy has changed due to the technological developments in the field of data-collection technologies in the last 20 years.

To answer this question, I developed a framework that involves four types of privacy violations, four mechanisms of TechnoMoral Change, three types of actors and several data-collection technologies. Court cases involving the application of the most important law on privacy and involving a technology were analyzed and coded in line with the framework. As the court cases are argued to represent morality, changes in the kind of privacy violations in the cases over time could show moral change. Changes in the mechanisms involved explain how technology changed morality, changes in the actors involved explain who violated privacy and changes in technologies involved explain which technologies were responsible for those changes.

While the last 20 years are analyzed, no cases were found prior to 2011, while data-collection technologies did exist prior to 2011. It thus seems that moral change takes more time to occur, compared to technological change. Technological changes generally happen very fast, while morality concerns established opinions on what is good and what is bad. It seems to take time for those opinions to change, possibly because people do not easily change existing values. This difference is also visible in the laws. The GDPR, which included regulations for a large number of newly developed data-collection technologies was implemented in 2018, years after the introduction those data-collection technologies. This research thus shows that it takes time for morality to catch up with technology.

Of the court cases involving privacy violations and data-collection technologies, the vast majority, 73,26%, is from 2018. This spike possibly shows a moral change. To analyze the cause of this spike, changes within the different categories of privacy violation over time will first be summarized.

40 of the 86 cases are in the ‘access’ category, which involves giving or gaining access to personal data or controlling who has access to personal data. Most cases concern a violation by the government. The technology most involved, both prior to and in 2018 is a database technology. However, the TechnoMoral Change mechanism that is most common in the cases changes over time, as prior to 2018 the third mechanism of TechnoMoral Change,

the ability of technology to alter roles and relationships, was the main mechanism involved. In these cases, database-technologies enable the violation of privacy by altering roles, as the technology changed who was in control of deciding who could access certain information. In 2018, the most common TechnoMoral Change mechanism was the first one, the ability of technology to create new opportunities and responsibilities. In these cases, database technologies enable the violation of privacy by giving or gaining access to personal data. This possibly shows a moral change as prior to 2018, we considered our privacy violated when we lost control of our data and handed it over to the government, due to database technologies. In 2018, it was considered a privacy violation when the government tried to gain access to other databases. However, an alternative explanation could be that the government did not try to gain access to other databases prior to 2018, this was however already possible long before 2018.

The cases where a company was accused of violation privacy by giving or gaining access to personal data or controlling who has access to personal data showed no difference in the TechnoMoral Change mechanisms involved prior to 2018 and in 2018. Both timeframes mainly involve the first one, the creation of opportunities and responsibilities. It did however show a shift in the technologies that create those opportunities. Prior to 2018, only two out of five cases involve a database, the other technologies involved are the internet and mobile devices. This shows that before 2018, companies violated privacy by giving access to others through the internet, by gaining access to mobile phones and by using databases, while in 2018 privacy violations were mainly due to database-technologies.

The spike of cases in 2018 for the category access is thus mainly due to an increase in cases involving the violation of privacy by giving or gaining access to a database, as database technologies offer new opportunities and responsibilities. It is possible that due to moral change, this became less morally acceptable. It could also be that there was an overall increase in the use of databases, this technology however already existed before 2018.

18 of the 86 cases are in the ‘store’ category, which involves the storage of data or the registration of data. All of these cases involved a database. For both actors in this category, the government and companies, there was a difference in the amount of cases that involved the fourth mechanism of TechnoMoral Change, the ability of technology to give new insights into consequences of actions, prior to 2018 and in 2018. Of the cases prior to 2018, only one involves the fourth mechanism, while the others involve the first mechanism, the creation of new opportunities and responsibilities. Of the 14 cases in 2018, this has changed, as only three cases involve the first mechanism and the other 11 the fourth mechanism. It shows that

privacy was initially violated due to the new opportunities and responsibilities that databases offered for the storage of data. In 2018, the storage of data in databases led to new consequences for actions, which was considered privacy violation. It could be that the storage of data was no longer considered morally acceptable because of the consequences that could impact someone's private life. An alternative explanation could be that it takes time for those consequences to emerge. The majority of the cases involved an outdated registration. The process of storing thus possibly happened way before the subject of the data became aware of the consequences.

18 of the 86 cases are in the 'analyze' category, which involves the violation of privacy by analyzing data or using data for other purposes than was intended. This category mainly involves cases where Google is accused of violation privacy by showing certain search results. This involve the fourth TechnoMoral Change mechanism, the ability of technology to give insight in new consequences. Due to the algorithm that Google uses to compute which search results should be shown, former actions result in new consequences. As all cases in this category are in 2017 and 2018, it is possible that data-analysis was deemed morally acceptable before. However, alike the cases that involved the fourth mechanism of TechnoMoral Change in the 'store' category, an alternative explanation of the increase of cases involving the fourth mechanism is that the new consequences take time to emerge.

All of the ten cases in the last category, 'collect', referring to the second-hand collection of data, involve the first mechanism of TechnoMoral Change, the creation of new opportunities and responsibilities. The most important change over time is a change in the actors involved. The cases before 2018 mainly involve companies, while the cases in 2018 mainly involve the government. This could suggest that collection by the government was considered morally acceptable for a longer time compared to collection by companies. An alternative explanation could be that companies were the first to collect data, followed by the government. However, this does not agree with the observations of for example Greenwald (2014) and Martijn and Tokmetzis (2016), as they both state that governments already used data-collection technologies well before 2018, in the book of Martijn and Tokmetzis, this concerns the Dutch government.

While for the 'access', 'store' and 'analyze' category, the increase in cases can be explained by both a moral change and alternatively by an increase in the amount of times that the relevant technologies are used, the change observed in the 'collect' category is very likely to be a result of moral change. The cases show a shift from privacy violations by companies to violations by the government in 2018 while the literature shows that the government

already collected data well before 2018. This thus rules out the alternative explanation in the other categories, that there might have been an increase in the total amount of times a technology was used. It seems that our notion of privacy has changed during the past years as deem collection by the government less morally acceptable than we used to.
This answers the research question.

The introduction of GDPR/AVG in 2018 and the media coverage at that time might be another suitable explanation for the spike in court cases. It might be that the attention it gained at the time resulted in moral change. It could also be that the inclusion of regulations for new technologies made it easier to go to court. To rule out this explanation, more research is necessary, ideally with data that has no affiliation with the law, like the complaints filed to the Autoriteit Persoonsgegevens mentioned earlier. While I was unable to use these complaints as the data for the analysis, I expect them to be more suitable for the goals of this research, as the court cases used have limitations.

While the court cases provide insight in what the accusers deem morally wrong or right, they are biased towards the law. Before a complaint results in a court case, the feasibility of the case and the possible outcomes of the cases are taken into consideration. If the lawyer of the accusing party believes that there is a big chance that they will lose the case, it is highly probable that they will not go to court. Using the court cases as a data source thus only involve possible privacy violations that are thought to be unlawful by a lawyer. While the law can be considered an operationalization of common values, it is highly probable that there are problems concerning privacy that do not violate the law, but are still considered morally unjust by certain people. Moreover, going to court has risks, as one could lose money if they lose the case. Submitting a complaint to the Autoriteit Persoonsgegevens is both risk-free and always a possibility. Thus, these complaints are expected to give more valuable results.

One of the other goals of the research, next to answering the research question, was to empirically test the mechanisms of TechnoMoral Change. The mechanisms provided useful explanations for the observed changes. For most cases, it was relatively easy to see what mechanism was involved. However, for a number of cases the mechanism overlap, mostly because some technologies tend to fit in multiple categories. This makes it harder to come to conclusions as the mechanisms offer multiple explanations for the same observation. However, the mechanism did in the end provide an explanation for the observed changes and help with answering the research question, thus proving their worth.

References

Autoriteit Persoonsgegevens. (2018). Algemene verordening gegevensbescherming (AVG). Retrieved July 8, 2019, from https://www.autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg

Bijker, W. E. (1987). The social construction of Bakelite: Toward a theory of invention. *The social construction of technological systems: New directions in the sociology and history of technology*, 159-187.

Bijker, W. E., & Law, J. (1992). *Shaping technology/building society: Studies in sociotechnical change*. MIT press.

Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. *The Cambridge handbook of artificial intelligence*, *316*, 334.

Brandt, R. B. (1954). Hopi ethics: a theoretical analysis.

Centraal Bureau voor de Statistiek. (2018). Internet; toegang, gebruik en faciliteiten [Dataset]. Retrieved July 8, 2019, from https://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83429NED&D1=0,2-5&D2=0,3-6&D3=0&D4=a&HDR=T&STB=G1,G2,G3&VW=T

De Beaufort, I. (1998). Als twee druppels water? Van Fuchsia via Dolly naar Elvis? Het kloneren van mensen naderbekeken. *H. Bout (red.), Allemaal klonen. Feiten, meningen en vragen over kloneren. Amsterdam and Den Haag: BoomlRathenau Instituut*, 91-119.

Edwards, C. P. (1987). Culture and the construction of moral values: A comparative ethnography of moral encounters in two cultural settings. *The emergence of morality in young children*, 123-151.

Fairfield, J., & Shtein, H. (2014). Big data, big problems: Emerging issues in the ethics of data science and journalism. *Journal of Mass Media Ethics*, *29*(1), 38-51.

Goodall, N. J. (2016). Can you program ethics into a self-driving car?. *IEEE Spectrum*, *53*(6), 28-58.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan.

Heidegger, M. (1954). The question concerning technology. *Technology and values: Essential readings*, *99*, 113.

Van Helden, J.(2018). *Een kleine geschiedenis van de privacywetgeving*. Retrieved July 8, 2019, from https://www.declercq.com/kennisblog/een-kleine-geschiedenis-van-de-privacywetgeving/

Jasanoff, S. (Ed.). (2004). *States of knowledge: the co-production of science and the social order*. Routledge.

Ketting, E. (2000). De invloed van orale anticonceptie op de maatschappij. *Nederlands Tijdschrift voor geneeskunde*, *144*(6), 283-286.

Keulartz, J., Schermer, M., Korthals, M., & Swierstra, T. (2004). Ethics in technological culture: a programmatic proposal for a pragmatist approach. *Science, Technology, & Human Values*, *29*(1), 3-29.

König, M., & Neumayr, L. (2017). Users' resistance towards radical innovations: The case of the self-driving car. *Transportation research part F: traffic psychology and behaviour*, *44*, 42-52.

Koops, B. J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2016). A typology of privacy. *U. Pa. J. Int'l L.*, *38*, 483.

Koppelaar, R., & Middelkoop, W. (2017). *De Tesla-revolutie: waarom de olie-industrie haar macht verliest*. Amsterdam University Press.

Latour, B. (1999). *Pandora's hope: essays on the reality of science studies*. Harvard university press.

Van Lieshout, M. (2018). Belastingdienst eist inzage Museumkaart om belastingplichtige kaarthouder op te sporen. Retrieved August 9, 2019, from https://www.volkskrant.nl/nieuws-achtergrond/belastingdienst-eist-inzage-museumkaart-om-belastingplichtige-kaarthouder-op-te-sporen~bf250db4/

Ma, A. (2018, 30 oktober). China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you. Retrieved February 22, 2019, from https://www.businessinsider.nl/china-social-credit-system-punishments-and-rewards-explained-2018-4/?international=true

Martijn, M., & Blauw, S. (2019). In de stad van de toekomst praten lantaarnpalen mee en burgers niet. Retrieved February 22, 2019, from https://decorrespondent.nl/9148/in-de-stad-van-de-toekomst-praten-lantaarnpalen-mee-en-burgers-niet/281355888-bb6d0161

Martijn, M., & Tokmetzis, D. (2016). *Je hebt wél iets te verbergen: over het levensbelang van privacy*. De Correspondent.

Miller, C. C. (2013). Google searches for style. *The New York Times*, *20*.

Milt, K., & European Parliament. (2019). *Personal Data Protection*. Retrieved July 8, 2019, from https://www.europarl.europa.eu/ftu/pdf/en/FTU_4.2.8.pdf

Oudshoorn, N. E. (1995). Technologie en zorg: vriendinnen of vijanden? Het voorbeeld van nieuwe anticonceptiemiddelen voor vrouwen en mannen. *Gezondheid: theorie in praktijk*, *3*.

Uitvoeringswet Algemene Verordening Gegevensbescherming (2018). Retrieved July 8, 2019, from https://wetten.overheid.nl/BWBR0040940/2019-02-19

Van de Poel, I. (2011). *Ethics, technology, and engineering: An introduction*. John Wiley & Sons.

Swierstra, T. (2013). Nanotechnology and technomoral change.

Verbeek, P. P. (2006). Materializing morality: Design ethics and technological mediation. *Science, Technology, & Human Values*, *31*(3), 361-380.

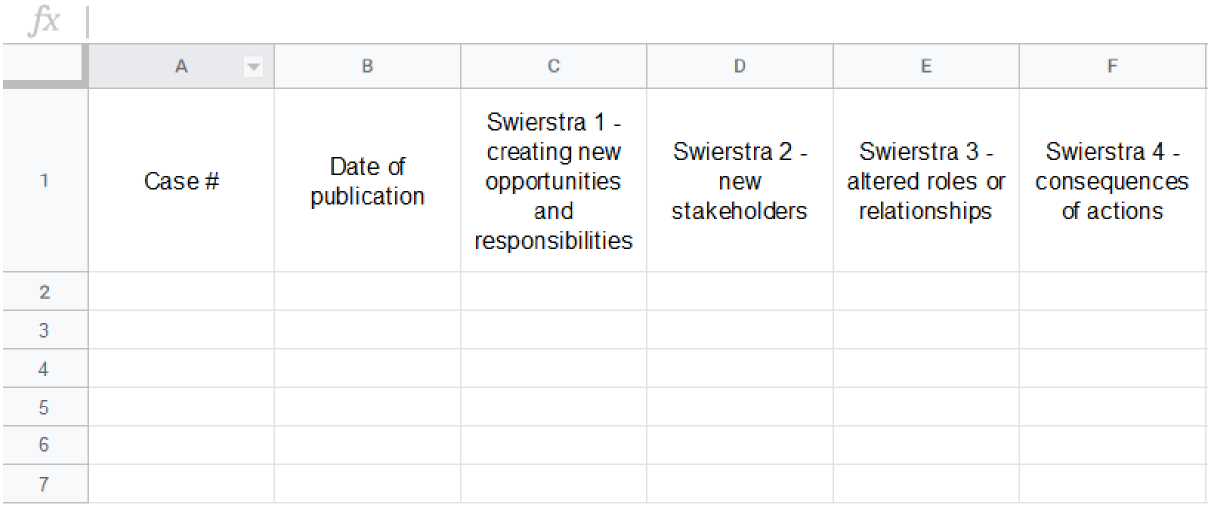
De Volkskrant. (2019). Cambridge Analytica | De Volkskrant. Retrieved August 9, 2019, from https://www.volkskrant.nl/tag/Cambridge+Analytica?referer=https://www.google.com/

De Vries, G. (1989). Ethische theorieën en de ontwikkeling van medische technologie Théories éthiques et développement de la technologie médicale. *Kennis en Methode*, *13*(3), 278-294.

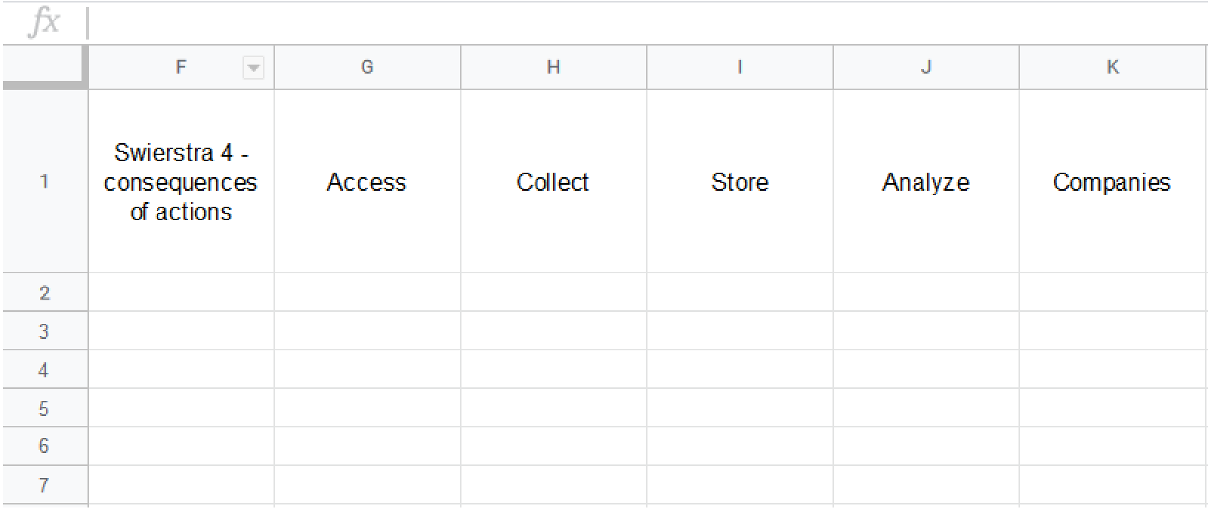
Wet Bescherming Persoonsgegevens (2001). Retrieved July 8, 2019, from https://wetten.overheid.nl/BWBR0011468/2018-05-01/

Wollscheid, C. (2012). *Rise and burst of the dotcom bubble: causes, characteristics, examples*. GRIN Verlag.

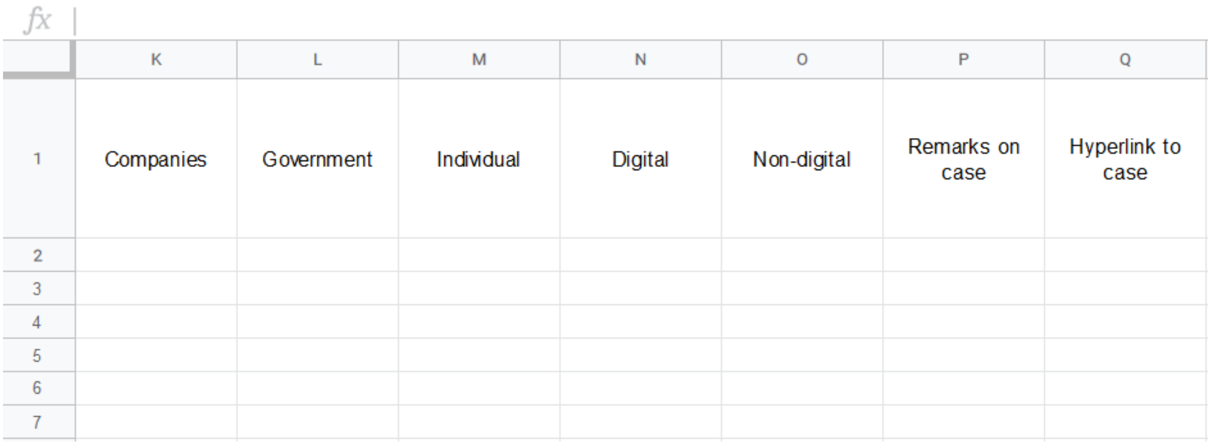
Appendix – Excel Sheet used for the analysis.



	A	B	C	D	E	F
1	Case #	Date of publication	Swierstra 1 - creating new opportunities and responsibilities	Swierstra 2 - new stakeholders	Swierstra 3 - altered roles or relationships	Swierstra 4 - consequences of actions
2						
3						
4						
5						
6						
7						



	F	G	H	I	J	K
1	Swierstra 4 - consequences of actions	Access	Collect	Store	Analyze	Companies
2						
3						
4						
5						
6						
7						



	K	L	M	N	O	P	Q
1	Companies	Government	Individual	Digital	Non-digital	Remarks on case	Hyperlink to case
2							
3							
4							
5							
6							
7							