The Philosophical Background of the General Data Protection Regulation

Privacy in European Policy

By: Eline Elstgeest

Student Number: S1065904

Turn in date: 31 May 2018

Supervisor: dr. D.M. Mokrosinska

Contents

Introduction

The computer era has changed many aspects of everyday life. The way we communicate with each other, the way information is stored and processed, the way traditional media functions and the emergence of new forms of media, to name a few. This has given society a big question: how do we combine these changes with long standing and undeniable philosophical values? Technology allows us to perform activities in new ways, and because of this situations may arise for which we have no adequate policies to guide us in the combination of technological changes and values. This can be called a policy vacuum.[1]

This policy vacuum becomes extra visible when scandals occur that hurt our values and interest. One of the values that is frequently challenged by new technologies is the value of privacy. A recent privacy scandal that got world wide attention is the data leakage from Facebook to Cambridge Analytics, a corporation analysing (personal) data and using it to further political and financial interests. This was followed by international outrage as people felt that their privacy was being violated by the transmission of their personal data to a unknown third party. A violation like this could not have happened without technology developed in the past decade or so. The leaked data was collected digitally, both by voluntary submission of the data and by more invisible ways like trackers on websites. The data could not have been leaked, analysed, and (mis)used without the use of modern technologies and data systems.

Society tries to prevent such scandals by law making, thereby filling the policy vacuum. New laws are constantly made to update the legal system to the new technologies and the new possibilities that arise along with them. However, designing such laws comes with some difficulties. Not only do the lawmakers need a firm grip on technology and a prospect of what the future holds, they also need a clear understanding of the values they are trying to protect. This research aims to evaluate how well lawmakers succeed in understanding values and incorporating them in law. To do this, I will use a case study, in which a new law is being tested against a prominent conception of an important value. The value being discussed is privacy, one of the values that is most acknowledged to be threatened by new technologies. The law being examined is the General Data Protection Regulation, a law by the

[1] James Moor (2005). 'Why we need better ethics for emerging technologies' Ethics and Information Technology, 7(3). 111-119: 115.

European Union which aims to unify all European data protection laws, making it easier for businesses to exchange data, but also to protect citizens valuable personal data and privacy.

I chose this law for my case study, because it is very topical – it will be in effect from May 25th 2018 – and because it will have a lot of effect on organisations in- and outside Europe. The data of more than half a billion European citizens will be protected by this law. Organizations that don't comply could suffer fines up to 20 million Euro or 4 % of the annual worldwide revenue, whichever one is higher. It is deemed to be one of the most extensive privacy laws of recent years.

As for privacy, there are many different conceptions of privacy among philosophers. I chose to focus on one of those, Helen Nissenbaums conceptualisation of privacy as contextual integrity, as is explained in her book 'Privacy in Context.[2] A detailed description of Nissenbaums idea of contextual integrity and how Nissenbaums ideas about privacy compare to other conceptualisations of privacy will be discussed in another part of this thesis.

The central question of my thesis will be: **'Does the General Data Protection Regulation succeed in protecting contextual integrity in different contexts?'**.

Of course, the law wasn't made to be applicable in all contexts, the sharing of information between friends or family is not something that can – or should – be policed. More so, if it were, people would likely think that to be a violation of their privacy. So I chose three contexts, all mentioned by Nissenbaum, in which the law would be applicable. These contexts are: business, healthcare and education.

Relevance

So why is this research academically and socially relevant? Drafting privacy regulations can be very difficult because of the conceptualisation of privacy. Daniel Solove points out that legal protections of privacy often have a poorly theorized underlying conception of privacy and that these protections are rarely examined.[3] This research aims to be one of the rare examinations of a legal protection of privacy. Since the General Data Protection Regulation was drafted with the intention to protect the privacy of more than a half a billion people and will have big consequences for all the organisations that have to comply to it, it is paramount that it does so based on a decent conceptualisation of privacy.

[2] Helen Nissenbaum, (2009) *Privacy in Context. Technology, Policy, and the Integrity of Social Life*.

[3] Daniel J. Solove (2008). *Understanding Privacy*, 4.

This leads to the following question: what is the right conceptualisation of privacy? Why should Nissenbaums theory of privacy be taken as the yardstick against which we measure this law? First of all, Nissenbaums theory is relatively recent and designed to deal with emerging privacy issues from new technologies, which makes it preferable to older and perhaps outdated privacy conceptualisations. As a theory developed to deal with emerging socio-technological systems and their effect on privacy, the theory lends itself well to evaluate a law that is also designed to protect privacy in the light of socio-technological systems.

Secondly, Nissenbaums theory on privacy is already used as a reference for a similar law on the other side of the Atlantic. The Consumer Privacy Bill of Rights in the United States – stating the way companies should handle personal consumer data – specifically cites her book as one of the inspirations for the law.[4] Although this of course doesn't directly validates her theory, it does show its prominence and the applicability of this theory in law making.

Lastly, both Nissenbaum and the General Data Protection Regulation use similar terminology. By privacy they mean the protection of personal data of individuals and Nissenbaum cites the European Union Directive, the General Data Protection Regulation's legal predecessor, as her definition of personal data. This definition being: 'any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his [or her] physical, physiological, mental, economic, cultural or social identity'.[5]

Structure of this thesis

The first chapter will concern the case in this thesis: the General Data Protection Regulation. In this chapter I will discuss the history and a description of this legal instrument. Also I will argue how the law which only concerns data protection is connected to privacy.

The second chapter is about Helen Nissenbaums theory and her definition of contextual integrity. To be able to use this theory as a benchmark for privacy under the General Data Protection Regulation, we need to grasp what is exactly is that she means by contextual integrity, how this protects our privacy and what conditions need to be met for the contextual integrity to be respected.

The third chapter will discuss the first of the contexts and how well the General Data Protection Regulation would respect contextual integrity in it. The context which will be discussed first is a

[4] NYU website: https://steinhardt.nyu.edu/site/ataglance/2012/02/inside-nyu-steinhardt-helen-nissenbaum-on-the-white-house-bill-to-protect-consumers-online.html

[5] Nissenbaum, *Privacy in context*, 4.

healthcare context. This is a context that Nissenbaum also regularly calls upon when giving examples in her book, probably because healthcare is an especially interesting context since information concerning one's health is usually deemed to be very sensitive and thus in need of protection.

In the fourth chapter will discuss a second, namely education. This is also a context that Nissenbaum sometimes uses as an example to illustrate the mechanisms of contextual integrity. The context of education is interesting because a lot of personal (student)information is present in this context. Students can also be vulnerable data subjects since they often are children in a critical period of their development. They are also very reliant on protection by others since young children are not capable of defending their own rights to privacy.

In the fifth and final chapter the context of business will be discussed. I will use a very broad definition of business, taking it to mean governmental organisations, corporate organisations, and everything in between like NGO's, clubs and associations with or without profit objectives.

The thesis will end with a conclusion in which I will give a final judgement on how well the General Data Protection Regulation respects contextual integrity in the three different contexts. In this section I will give an answer to my research question and decide whether the Regulation is sufficiently protecting contextual integrity.

About the General Data Protection Regulation

This chapter will review the General Data Protection Regulation (from here on: GDPR). I will discuss the history and give a description of this legal instrument. Also I will argue how the law is connected to privacy.

History and background of the GDPR

The GDPR was introduced in the European Parliament in October 2013, and was adopted on April 14th 2016. After this an implementation period stated, lasting until May 25th 2018 when the regulation it to apply to all the member states of the European Union and all organisations operating in the European Union or with data or European citizens will be held accountable if they don't comply.

The regulation is meant to unify data protection in the European Union. This is beneficial both to the EU citizens as it is to businesses. The latter because a general regulation covering the entire European Union will make data transactions among member states easier, lowering the legal burden of checking compliance with different legislatures. The former because the GDPR aims to better protect personal data of citizens, solidifying their right to protection of their data.[6]

This regulation is not the first action of the European Union to protect the data of its citizens. In 2000 the European Union stated the Charter of the Fundamental Rights of the European Union. This document combined several older documents and treatises concerning the rights of citizens. Article eight of this charter specifically covers the right to the protection of personal data:

"Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

[6] See Handvest van de grondrechten van de Europese Unie, chapter 2, article 8, http://www.europarl.europa.eu/charter/pdf/text_nl.pdf.

3. Compliance with these rules shall be subject to control by an independent authority"[7]

So, the GDPR is based on the assumption of data protection being fundamental human rights.[8] Besides it being a fundamental right, Europe-wide agreements have been made before the declaration of the fundamental rights. In 1995 the Data Protection Directive was adopted. It was meant to safeguard citizens' privacy in a time of increased computer use, with the key objective of preventing personal data from being misused or unnecessarily collected.[9]

The Data Protection Directive can be seen as the predecessor of the GDPR. It has many commonalities in the scope and content, but differs from the GDPR in several ways. The most important being the juridical difference between a directive and a regulation. The directive provides the member states with more freedom and leeway on how to implement the directive into their national law. In The Netherlands for instance, the directive ultimately resulted in the Wet bescherming persoonsgegevens (Wbp; translation: Data Protection Law) and the institution of the Autoriteit Persoonsgegevens: the Dutch data protection authority.[10] Both of which are specifically Dutch instruments and institutions, albeit based on directions from the European directive. The GDPR, being a regulation, is self-executing. This means the member states can't implement it as they see fit, in fact it is forbidden to alter the GDPR for adoption in national law.[11] The GDPR is the new law for all member states. For The Netherlands this means the GDPR replaces the Wbp.

Differences between the GDPR and the Data Protection Directive can also be found in the content of the texts. The GDPR is better equipped to deal with new technological advances like social media and big data, which left gaps in the previous legislature.[12] Another difference is the basis for the directive and the regulation, Laima Jančiūté argues that the directive was more of a market-making tool, due

[7] http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[8] Maciej Sobolewski, Joanna Mazur & Michal Paliński, (2017) 'GDPR: A Step Towards a User-centric Internet?' *Intereconomics* vol. 52, 207-213:208.

[9] Lawrence Rys and Lauren Grest (2016) 'A New Era in Data Protection' *Computer fraud and security* Vol. 3, 18-20: 18.

[10] Website Autoriteit Persoonsgegevens, accessed on 17-3-2018, https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens.

[11] Sobolewski, Mazur & Paliński, 'GDPR: A Step Towards a User-centric Internet?' 208.

[12] Rys and Grest (2016) 'A New Era in Data Protection', 18.

to the absence of fundamental rights primary law at the time of the draft, while the GDPR is more based on fundamental rights, backed by the Lisbon Treaty.[13]

Content of the GDPR

In this part I will broadly review the content of the GDPR.

Probably the first question we should answer is: what is the GDPR about? To answer this we will analyse the four words it is made up of: General Data Protection Regulation. The final word is already taken care of in the previous section: it's a legal term indicating how the law should be implemented in the member states. The first word, general, means it's applicable to everyone and everything within its jurisdiction. Even non-European organisations possessing data about European Citizens must comply to the Regulation. It doesn't matter where the data is stored, if it's about European Citizens it's subjected to the GDPR.[14]

This leaves us with 'Data' and 'Protection', which are not as easy to explain. Let's start with 'data'. What data is in need of protection and why must this data be protected? The GDPR aims to protect personal data. It defines personal data as:

> *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*[15]

This includes data such as for instance names, passport numbers, (IP) addresses, birthdates and more.

Within the term personal data there is also a section of special categories of personal data, which should be handled with extra care, and in many cases isn't allowed to be processed at al. This concerns data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs,

---

[13] Laima Jančiūté (2016) 'EU Data Protection and 'Treaty-base Games', in: *Data Protection and Privacy*, Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul de Hert (ed), 1-31: 25.

[14] Colin Tankard (2016) 'What the GDPR means for businesses' *Network Security* No. 6, 5-8: 5.

[15] General Data Protection Regulation, article 4, paragraph 1, as found on https://gdpr-info.eu/art-4-gdpr/, accessed on 25-3-2018; Tankard, 'What the GDPR means for businesses' 5; Sobolewski, Mazur & Paliński, 'GDPR: A Step Towards a User-centric Internet?' 208; Rys and Grest 'A New Era in Data Protection', 19.

trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[16] This data belongs to a special category because it can easily be used for discriminatory decisions and actions, and needs extra protection to ensure it is legitimately collected and used.

Now the word data has meaningful substance to us, we will head on to the final word: protection. The protection of this data is one of the two core objectives of the GDPR (the other being simplifying regulatory environments).[17] So, how does the GDPR propose to protect citizens data? Due to the scope of this research I can't go into too much detail here, so I will focus mostly on the rights of the data subject and skip the more technical prescriptions concerning information security systems.

The GDPR gives six central rights to the data subjects. The first one is the right to access by the data subject. If the subject wishes to know what data about him or her is being processed, the controller must provide an overview of all the personal data they control. The second one is the right to rectification, if the data subject finds the data to be faulty, he or she can request the data to be rectified. The third is the right to erasure, also called the right to be forgotten. The subject can ask to have all the data about him or her erased, unless there is legitimate ground to retaining it. The fourth is the right to restriction of processing. Less drastic than the previous right, this gives the data subject the right to ask a controller to stop processing their data until they consent to processing once more. The controller will still be storing the data. The fifth is the right to data portability. The subject should be able to freely transfer personal data from one service to another, in this case the controller will provide the data in a structured, commonly used and machine readable format. The sixth and final right is the right to object, if the subject objects to the processing of their data, the controller shall no longer process it, unless he can demonstrate legitimate grounds for processing.[18]

Aside from these six rights of the data subject, there are some more issues in the GDPR deserving of our attention. The first one is the issue of consent. Data subjects must give consent to their data being processed. This consent must be informed – giving the controllers the duty to adequately inform the subjects and ask unambiguously for their consent – and given voluntarily.[19] Should data

[16] General Data Protection Regulation, Article 9, paragraph 1, as found on https://gdpr-info.eu/art-4-gdpr/, accessed on 25-3-2018.

[17] Jesper Zerlang (2017) GDPR: a milestone in convergence for cyber-security and compliance' Network Security No. 6, 8-11: 8.

[18] General Data Protection Regulation, Article 15- 21, as found on https://gdpr-info.eu/art-4-gdpr/, accessed on 25-3-2018.

[19] Tankard, 'What the GDPR means for businesses', 5; Rys and Grest, 'A New Era in Data Protection', 18.

be put to uses other than those to which the data subject gave his or her consent, the data subject may seek redress in the form of compensation.[20] An exception to this are organisations that need personal data to execute legally required tasks and are mandated to collect personal data without the direct consent of the data subject. Tax authorities for instance collect a lot of personal information, but don't need the consent of citizens to do so.

The second one concerns data breaches. The Data Protection Directive left some leeway for the member states to decide whether organisations should notify subjects and a data protection authority in case of a data breach. In The Netherlands this resulted in mandatory notifications to the Autoriteit Persoonsgegevens. The GDPR prescribes the organisations to notify data protection authorities within 72 hours of the discovery of the data breach. [21]

The connection with privacy

The GDPR is popularly named a 'new privacy law', but the above doesn't clearly state the connection between data protection and privacy and in the entire juridical text the word privacy isn't mentioned at all. However, many actors involved – amongst whom politicians, media, the Dutch consumer authority and even the data protection authority who will be charged with the control of compliance – still call it a privacy law. Is this a mere confusion of concepts or is there more to it?

Calling data protection a privacy issue isn't that farfetched. The idea of privacy as control over personal information is one of the most predominant theories of privacy.[22] One of the most well-known authors on privacy as data protection, Alan Westin, defines privacy as the 'claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[23] He also calls out curiosity and invading the privacy of others to be universal human traits, resulting in the need to defend ones privacy from others, and in a developed society, from surveillance by authorities.[24]

It is likely with this conception of privacy in mind that people refer to the GDPR as a privacy law. An obvious reason for making this connection is because of the focus on 'personal data' and the individual citizen. The GDPR does not aim to protect all kinds of data, it is not in place to protect

[20] Tankard, 'What the GDPR means for businesses', 7.

[21] Ibidem, 5.

[22] Solove, *Understanding Privacy*, 24.

[23] Alan F. Westin (1970). *Privacy and Freedom*, 7.

[24] Ibidem, 19.

financial data or state secrets, it focusses on individual persons and the data that can be used to identify a natural person.

Also, the six central rights that the GDPR gives to citizens are all designed to enhance control on personal information. The rights to access, rectify, restrict processing and erase data are all ways for individuals, groups or institutions to determine when, how and to what extend data about them is being communicated. So in the conception of privacy as control over personal information the GDPR can certainly be called a privacy law.

However, in this thesis I aim to use a somewhat different conception of privacy, namely Nissenbaums conception of contextual integrity. I would like to argue that in Nissenbaums conception, the GDPR would also be recognised as a privacy law. Mostly because her conception is comparable with the conception of protection of personal data. Both conceptualisations concern themselves with information flows and personal data. But while the classic data protection conceptualisation claims a need to control the flow of information to respect privacy, Nissenbaum says that complete control of personal data is not necessary, as long as the information flows are appropriate.[25]

Information flows are appropriate as long as they abide by context-relative norms which prescribe the flow of personal information in a given context.[26] A law governing the flow of personal information, such as the GDPR, can be seen as (part of) a norm. Nissenbaum sees such laws as a mechanism which imposes explicit governance over a context combined with formal sanction.[27] Law sets out a basic framework for certain types of contexts, but these frameworks should be 'further fleshed out by rules or professional codes applying to particular corporations or professional societies'.[28] More about this in the next chapter.

To conclude, in both the privacy as control of personal data and Nissenbaums privacy as contextual integrity conceptualisations, the GDPR can be seen as a privacy law. Some privacy scholars may say that both these conceptualisations fail to completely define privacy, as they see this definition of privacy as either too narrow or too broad.[29] In this thesis however, I do not want to conduct this discussion about the perfect definition of privacy, since the answer is unlikely to be found. I side with

[25] Nissenbaum, *Privacy in Context*, 2.

[26] Ibidem, 127.

[27] Ibidem, 135-136.

[28] Ibidem, 136.

[29] Solove, *Understanding Privacy,* 24-29.

Nissenbaum in saying that we need not to exactly define privacy to address critical challenges to it.[30] As already stated in the introduction, Nissenbaums conception is well suited for the cause of this research, because of its prominence and its focus on new technologies.

The next chapters will give a more detailed account of contextual integrity and how it is supposed to be maintained, and test if the GDPR succeeds in protecting privacy in the three different contexts of healthcare, education and business.

[30] Nissenbaum, *Privacy in Context,* 2.

Chapter 2: Contextual integrity

In this chapter I will give an overview of Helen Nissenbaums theory of contextual integrity and its place in privacy theory. To be able to use this theory as a benchmark for privacy under the General Data Protection Regulation, we need to grasp what is exactly is that she means by contextual integrity, how this protects our privacy, and what conditions need to be met for the contextual integrity to be respected. A solid grasp on her theory is needed for the description of the contexts in next chapters and to evaluate how the GDPR does or does not respect contextual integrity.

Privacy as contextual integrity

To start this chapter, I will first explain how Nissenbaums theory relates to other and perhaps more common theories of privacy. In doing so, I will only take into account other theories that define privacy in a similar way, namely privacy as sufficient protection, control, or handling of personal data. This does not take those definitions of privacy into account that have a broader definition of privacy, like the privacy one may get when being free from intrusive smells or sounds or the privacy one may experience when limiting access to the physical body.

Nissenbaums theory of contextual integrity as a benchmark for privacy differs greatly from previous theories of privacy. In her conceptualization of privacy as contextual integrity, she breaks with what she calls the public/private dichotomy. This dichotomy is shown when theorists claim that there is a strict difference between what is private and what is public. This line between private and public can be drawn in three different dimensions: the dimension of actors, divided into government and private actors; de dimension of realm, which can be divided into the public and the private; and the dimension of information, which can be divided into the public and the personal.[31]
The difficulty with this dichotomy lies in the belief that once information is out in the open, it loses all its claims on privacy. So in the example of the Facebook scandal described in the introduction: people that are filling in personality tests on Facebook and are giving Facebook information about their likes and dislikes, put this information out in the open freely and of their own will, and therefore can't call this information personal anymore and can't complain when this information reaches other parties in the public realm. Nissenbaum however, would object to this assessment since it doesn't explain the outrage that occurred when the scandal became public. It is counter intuitive that so many people would be outraged when no real claim on privacy was violated.

[31] Nissenbaum, Privacy in Context, 102.

In this idea of privacy, privacy is respected when people can exercise control over their information, deciding for themselves what information to share with who. However, this leads to some problems, besides the difficulty in explaining outrage over leaked personal data in the public sphere, the privacy paradox is a well-known problem that results from this conception of privacy. The privacy paradox entails that people claim to value their privacy, but when it comes to it, they freely give (private) information up in exchange for goods and other values. For instance filling out forms in exchange for free goods, or allowing more monitoring by the government in exchange for the value of security.

In her book, Nissenbaum addresses these problems and sets out to solve them by providing a new framework. One in which information is not just private or public. She opposes the public/private dichotomy by creating her framework of contextual integrity. Contextual integrity holds that privacy is respected if there is an appropriate flow of information, and is breached when the norms that govern this flow are violated. What an appropriate flow of information is, is defined by the context in which the information flows. Contextual integrity serves as a benchmark for privacy, when the appropriate flow is maintained, privacy is respected. Control is no longer an issue in this framework. Individuals don't need extensive control and an exact track record of what information is public and what is private, as long as they can count on an appropriate flow of information.

Context appropriate flows of information

So, what defines an appropriate flow? Since much of this is dependent on the context in which the information is flowing, we will first need a definition of what a context is. A context in Nissenbaums framework is defined as a 'structured social setting characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)[32]. While social settings are diverse, there are some elements to social settings that can be used to define a specific context. For instance, in the context of healthcare there is a patient looking for care from a health professional like a doctor or a nurse. This is an element that is canonical to the social setting of the context of healthcare. Another example could be an education context in which a canonical setting would be a teacher transferring knowledge to students.

However, defining a context is not always easy for not all contexts that are called the same are exactly the same. There can be differences in context due to disparities across societies, cultures and the point in history in which the context is set. A context is shaped by society, and aspects of it can change over time. A healthcare context in 21st century Western-Europe can and will change from a healthcare context in mid-1900 sub-Saharan Africa, despite them both being healthcare contexts.

[32] Nissenbaum, *Privacy in Context*, 132.

Contexts can also overlap. To stick with the healthcare example: say a medical student gets sick and gets treated in the teaching hospital she also receives her education in. She might get treated by her teachers or fellow students. Parts of the education context and healthcare context will overlap for her.

Key elements defining a context are roles, activities, norms, and values.
Roles are typical or paradigmatic capacities in which people act in contexts.[33] This can be a job, like doctor, teacher, manager, or another function like parent, friend or partner.
An activity is a canonical practice in which the people engage in a context. Examples are giving a lecture in a college course, getting an eye exam at the doctor, doing a job interview, etc.
Norms are a more difficult element to define. Nissenbaum states that norms: 'prescribe and proscribe acceptable actions and practices' and 'define the duties obligations, prerogatives, and privileges with particular roles, as well as acceptable and unacceptable behaviors'.[34] A norm could be being expected to keep a friends secret or being expected to follow traffic rules, anything that explicitly or implicitly governs social interactions.
Finally, values are what Nissenbaum calls the crucial, defining features of contexts. It is the reason a context exists. The context of healthcare exists because people value living a healthy life, and desire to be healed when they are sick. The context of education exists because an educated workforce is wanted and people value learning and the personal growth that comes with it.

Contexts can differ in the degree in which they are formalised or institutionalised. Law is a mechanism to institutionalise a context. For instance, the context of friendship is unlikely to be very formalised, while the concept of employment is quite formalised since there are contracts between employer and employee and there are many formal laws and regulations a employer must comply to in treating his employees. This doesn't mean there aren't any rules in the context of friendship, but those rules will probably not be written down or even said out loud in any part of the friendship. These rules, or norms, are implicitly governing the context of friendship.

This above example leads us to the concept of norms, which I would like to dig into a little deeper since norms are central to the account of contextual integrity.[35] As is also the case with the term concept, Nissenbaum doesn't describe what should be the exact meaning of the term norm. To use in her theory she just picks a robust interpretation of the term: the prescriptive interpretation.[36] This

[33] Nissenbaum, *Privacy in Context*, 133.

[34] Ibidem, 133.

[35] Ibidem, 137.

[36] Ibidem, 138.

means that a norm is something that people generally believe to be something that ought to be done. She says: 'when I say that an action is norm governed, I mean not only that most people generally follow it but they do so because they believe they ought to.[37]

Nissenbaum does give an anatomy of norms, adapted from the theory of George Henrik von Wright, and attributing four key elements to norms[38]:

1. A prescriptive ought element
2. A norm subject – one upon whom the obligation expressed in the norm falls
3. A norm act – the action prescribed in the norm
4. A condition of application – the circumstances in which the norm act is prescribed for the norm subject

So for instance, in the context of friendship there could be a norm that prescribes that you ought to keep your friends secret (element 1). The norm subject in this case is you, the one keeping the secret for your friend (element 2). The norm act would be not talking about the secret to anyone except the friend whose secret it is (element 3). The condition of the application would be the existence of the friendship. You aren't obligated to keep the secrets of a stranger with whom you have no further connection (element 4).

When speaking about data protection and privacy, not all norms are relevant. Only those norms dealing with the flow of personal information are important. When we speak about norms that govern the flow of personal information – the transmission, communication, transfer, distribution, and dissemination of information from one party to another – they are called context-relative informational norms or, when we speak of them in a specific context, simply informational norms.

Context relative informational norms are characterized by four parameters: contexts, actors, information types, and transmission principles.[39] Contexts are already discussed above, so I wont go into any more detail about them here. It suffices to say that they are the backdrop to the norm. The actors in informational norms can be categorized into three kinds: the senders of information, recipients of information, and the information subjects. The information subject is in this framework of contextual integrity – and in the GDPR which uses this same lingo to describe actors – a single individual or natural person. The senders and receivers of information can also be individuals, but it can also be multiple individuals or a collective of individuals, like an organisation. Information types,

[37] Nissenbaum, *Privacy in Context,* 138.

[38] Ibidem, 139.

[39] Ibidem, 140-147.

or attributes, are all the sorts of information that can be governed under a norm. It can be anything, ranging from a name to a phone number to religious belief. Nissenbaum doesn't give a precise definition nor a definitive list of information types, but she relies on an intuitive sense to grasp this concept.[40]

The transmission principle is probably the most important parameter to the framework of contextual integrity. A transmission principle is a constraint on the flow of information. It expresses the terms and conditions under which information transfers ought to occur. A transmission principle may state that information must be shared voluntarily, or that sharing the information requires the permission of the data subject.

So to answer the question at the beginning of this paragraph: an appropriate flow is maintained when the information flow aligns with the context relative informational norm. The appropriateness is dependent on the context in which the information flows, what information is flowing and, from and to whom it flows under what constrains.

According to the framework of contextual integrity, there are many different possible contexts with many different norms. This opposes the public/private dichotomy against which Nissenbaum sets up her theory of contextual integrity. According to the public/private dichotomy there are only two contexts: public and private. Nissenbaum calls this a crude version of contextual integrity.[41] In this crude version the flow of information is appropriate when the private doesn't flow to the public. Privacy is maintained when one can keep control on the private to keep it in the private context and out of the public one. In the framework of contextual integrity it is more complex to maintain privacy. Because there are more contexts, it is not a simple issue of control on the information flowing from the one context to the other. The information flows must be appropriate in all contexts.

Analysing contextual integrity

To check whether contextual integrity is respected, and to predict if a new socio-technological system or practice will give rise to privacy issues, Nissenbaum developed the Contextual Integrity Decision Heuristic.[42] Following the steps in the heuristics will lead to a conclusion on whether a new practice will respect contextual integrity and therefore privacy.

[40] Nissenbaum, *Privacy in Context,* 144.

[41] Ibidem, 141.

[42] Ibidem, 182.

In this research I will use much of this heuristic in assessing the way in which the GDPR affects the contexts in the next three chapters. The contextual integrity decision heuristic exists of 9 steps:

1. Describing the new practice in terms of information flows. Much of the describing of the new practice has already been done in the previous chapter, so I will not give extensive attention to this in the chapters to come. I will describe some context specific informational flows, which leads to the next step;
2. Identify the prevailing context. The contexts used in this research are 'health care', 'education' and 'business'. I will describe these contexts and give examples of other contexts nested within them;
3. Identify information subjects, senders, and recipients;
4. Identify transmission principles. The GDPR can be seen as a new transmission principle. It is a new constraint on how information flows and gives conditions under what circumstances information can be transferred. It is comparing this new transmission principles given by the law to the transmission principles already existing before the GDPR, explicitly or implicitly, that will give us an answer to how well the GDPR protects privacy;
5. Locate applicable entrenched informational norms and identify significant points of departure;
6. The first assessment of whether and how a system or practice defies entrenched norms. In the next chapters I will skip this step and continue with the heuristic until a complete assessment has been done and a conclusion can be given;
7. Consider the moral and political factors affected by the practice in question.
8. Ask how the system or practice directly impinge on values, goals, and ends of the context. The values of the contexts will be given in step 2 when identifying the contexts. Given the nature of the practice in question in this research – a new law governing informational norms – it is unlikely that it will have much effect on the goals in a context;
9. The above steps will lead to a conclusion on whether the practice or systems can be recommended by the framework of contextual integrity. The answers provided by this step in the next three chapters will eventually lead to the answer to my research question: does the General Data Protection Regulation succeed in protecting contextual integrity in different contexts?

In the following three chapters I will use this heuristic to define the effect of the GDPR on the contexts of healthcare, education and business. Since contexts vary across times and places, I will

need to specify here that the contexts described in the next chapters are all set in The Netherlands in contemporary times.

Chapter 3: the context of healthcare

This chapter will discuss how the GDPR does or does not respect contextual integrity in the context of healthcare. As already stated in the introduction, healthcare is an example which Nissenbaum also frequently calls upon in her book. Likely because of the sensitivity of health information and the need of protection this creates. It isn't surprising then that there are already many privacy regulations concerning healthcare. First and foremost there is the Hippocratic Oath with which medical specialists vow to uphold patient confidentiality, among other ethical vows and considerations. But there are also other, more contemporary laws, rules and codes of conduct that protect privacy in a healthcare context.

The context

First I will give a description of the context of healthcare, the value of it, the activities in it, the information flows in it and the sub contexts nested in it.

The value of healthcare is health. People value being healthy. When they are sick, they desire to recover and when they are recovered or heathy, they desire not to become sick. Being sick is obviously unpleasant for the individual that is sick, but it is also bad for society at large. A sick person costs money to nurse and is economically unproductive or less productive than a healthy individual. So the end goal of the context of healthcare is to make as much people as possible healthy.

To do so, people who are sick visit healthcare professionals to get cured. A pretty standard activity in the healthcare context would be a sick person making an appointment with his or her General Practitioner, describing his symptoms to this doctor and the doctor giving a diagnosis. After providing the diagnosis the doctor will likely proscribe some form or treatment or medicine or send the patient on to a specialist healthcare provider, at whose office a similar activity will take place.

There are many contexts nested in the context of healthcare: the general practitioners context, specialist care context (with its many specialties as sub-contexts), home care context, and the context of a teaching hospital to name a few. Somewhat loosely connected there is also the context of healthcare insurance.

In most of these contexts the information will flow from patient to doctor and sometimes from the doctor onward to other doctors or healthcare professionals. The personal information that is flowing obviously contains information about the patient's health, but also other information necessary to

identify or contact the patient, such as his name, birth date, address, phone number, citizen service number, and more.

To make it possible that the health insurance company pays for the health care costs made by the patient, they need to know various types of information about the patient. Information to identify the patient like name, date of birth and perhaps address; information about the health procedure and/or medication the patient received and would like to get payed for or refunded; and information to make the payment if necessary, so financial information like bank account numbers.

Another context loosely connected as a sub-context to healthcare is the context of prevention. Some healthy individuals will visit a healthcare professional even though they are not sick, but because they want to monitor their health and prevent becoming sick. In this sub-context a person visits a doctor or some other kind of healthcare professional, providing not their symptoms but information about their general health, like blood pressure, heartrate, diet, physical fitness, and other kinds of measurements. An example of this is people visiting a dietician. They may not be sick just yet, but by being over- or underweight run a higher risk for certain diseases. The individual visits the dietitian, gives personal information about their diet and possibly their overall fitness and the dietician will help them follow a healthier eating and exercising regimen.

Information subjects, senders, and recipients

This section describes the actors in a healthcare context.

The information subject in a healthcare context is usually the patient seeking care, which also in most cases is the sender of the information. The recipient would be the doctor, or multiple doctors, and sometimes nurses or any other kind of healthcare professional. A regular instance of information flowing from sender to recipient would be a sick person coming to the doctors office or the specialist clinic in the hospital, describing his symptoms, the doctor taking note of these symptoms in a (digital) file. The doctor will then give his diagnosis. But since the diagnosis, and following that the prescription of medication or treatment doesn't involve personal data, it is not relevant here. The information flow is one sided. It is just the patient giving the doctor information about his health, the doctor is not expected to also share his own health information with the patient.

Patient to doctor is not the only flow of personal information in the healthcare context. There are other flows with other actors involved. A General Practitioner might further health information of a patient to other doctors and nurses who will take part in the care and recovery of the patient. The doctor now being the sender of personal information and the other doctors and nurses the recipients, while the patient is still the data subject. Another flow is one from the doctor to the

health insurance company. In this case the doctor is again the sender of information and the health insurance company is the receiver of information. In both of these cases the patient, or data subject, is not part of the data transmission as either sender or receiver.

Transmission principles and entrenched informational norms

One most basic informational norm in the healthcare context is doctor-patient confidentiality, as is already named in at the start of this chapter. This means that a consult at the doctors office will take place in a secluded room, with just the patient and doctor present. If there are to be any other people present, like medical students or a friend or family member of the patient, it is always with consent from the patient. Unless the patient is a child, in which case a parent or legal guardian may accompany him or her.

The patient shares information about his or her health, without expecting the doctor to do the same. It is even quite inappropriate if the doctor does so. The sharing of information is voluntary and individuals can rarely be forced to visit a doctor. Forced admission in a hospital is only possible when the individual is a danger to themselves or everyone around them, which is the case with some mental diseases.

The information shared between patient and doctor is confidential, unless the patient gives permission to share the information or the sharing of information is needed for treatment.

Moral and political factors affected and impingement on context goals

The above sketches the healthcare context, the actors in it and the way information is expected to flow. This serves as a departing point from which we will examine the effect of the GDPR upon this context. In this paragraph I shall discuss what might be the harms and threats to political and moral factors such as autonomy, freedom, the implications for justice, fairness and democracy.

In my opinion there is no threat from that the GDPR imposes on the above values in the context of healthcare. The freedom or autonomy of the individual is not touched upon, they can still seek health care as they see fit. As for justice, fairness and democracy, the regulation does not change the way wealth or democratic power is being distributed among individuals in society. Therefore, it is not a threat to these factors. It will not change the access people have to proper healthcare, which would be one of the main concerns in a healthcare context.

As for the goals of the context: does the GDPR help to reach the goal of health for the individual or population? To this I would have to answer no. The GDPR doesn't make reaching health easier or more efficient. It does endorse the main informational norm governing the healthcare context, namely confidentiality. It provides more rules or transmission principles to uphold the privacy of the

patient in healthcare context. Since health information is a special category of personal information under GDPR law, it is harder for (healthcare) companies to collect this kind of information, putting an extra constraint on the information flow from doctor to third parties. It may also put a constraint on the information flow from patient to other organisations. Even if the patient decides to share healthcare information freely with another organisation, this organisation may be restricted from saving or using that data in any form, or actively seeking out this data.

Contextual integrity

In this paragraph I will give a verdict on whether the framework of contextual integrity would recommend the new practice as is dictated by the GDPR.

The GDPR endorses existing norms and transmission principles in a healthcare context. Especially the distinction between normal and special categories of personal data is important here. When thinking about the information flow in a healthcare context there is the assumption of patient-doctor confidentiality. However, this transmission principle doesn't exists for all kinds of information the doctor collects. A medical file may hold information about ones symptoms and physical condition, but also ones name or phone number. The appropriate flow for a name or phone number is very different from the appropriate flow of information about a patients symptoms. One would expect a higher rate of confidentiality with the latter. GDPR endorses this by its distinction between the two categories of personal information and the restrictions it puts upon the collection and processing of the special categories of information, to which health information belongs.

So while the GDPR doesn't help to reach the goals within a healthcare context, it does help by endorsing and formalising existing transmission principles in the context. In doing so, it doesn't pose a threat to other moral or political factors. This leads to the conclusion that the contextual integrity of the healthcare context is not breached by the new practice of the GDPR and the GDPR succeeds in protecting the citizens privacy in a healthcare context.

Chapter 4: the context of education

After describing the context of healthcare, this chapter will discuss whether the GDPR does or does not respect contextual integrity in the context of education.

The context

In this paragraph I will give a description of the context of education, the value of it, the activities in it, the information flows in it and the sub contexts nested in it; in a similar way like I did with healthcare in the previous chapter.

The value of education is for people to learn. This can be an individual value, people can find intrinsic value in learning new things or learn things that help them in achieving goals and values in their daily life, but it can also be a collective value. Society at large benefits from educating their people, and most of all their young. It helps people become well-functioning and productive members of society. Education for the individual can be about two things: learning new knowledge and skills and learning how to us them, and character building and personal growth that comes along with being educated. So the end goal of education is to help people reach their learning goals according to their capacities and helping them to become good citizens.

There are many different ways in which people learn, for instance some are autodidact, but a canonical activity in the education context would be a teacher passing on knowledge and skill to students, most likely in a classroom and sometimes one-on-one environment. This is the way education looks in the sub-contexts of primary education, secondary education, applied sciences and university. I will use this kind of context as the context of education as is under evaluation here, and leave contexts such as professionals taking courses to stay op to date in their work field, autodidacts learning new skills by themselves out of account. The education context described here is aimed at children or young adults, largely government funded, and mostly mandatory.

Although there is much information flowing from the teacher to the students, this is not the kind of information under scrutiny here. Our focus lies with personal information. What personal information flows in a education context? First of all there is the information needed to enrol students in schools and classes. Information such as a name, address, birthdate, public service number, and previous education are obvious information types needed for enrolment. But also some health information may be necessary: some schools won't allow unvaccinated children or children whose health will be a danger to other students in other ways. After enrolment, the school continues to collect information about its students by monitoring their grades and academic progress.

Especially with children, in both primary and secondary education, the behaviour of the child is also monitored and reported on. Teachers and other education professionals may also play a part in diagnosing learning disabilities, hereby gathering more health information.

Information subjects, senders, and recipients

The information subject in an education context is almost always the student, but it can also be the parents of a student. Another subject we can identify in the education context is the teacher who may be getting monitored to keep track of his or her teaching abilities. The sender of the information can be the student or the parents of the student and the recipient is the teacher, or the school as an institution.

There are cases in which the school is the sender, for instance when they talk to the parents about the child and his behaviour or academical accomplishments, or when they further information about the student to a healthcare professional that's treating the child, or when they report on the child's presence in class to an authority tasked with the the duty to check if compulsory education law is being upheld. In these cases the parents, healthcare professional, and education authority are respectively the recipient of the information.

Transmission principles and entrenched informational norms

Since in the education context we deal with a law that obligates children to follow at least primary and secondary education until a certain age, much of the information that needs to be shared is not shared voluntary. Since registration at a school is compulsory and some personal information is needed for this registration, students or parents are obligated to share this information with a school.

Just like the healthcare context, the sharing of information is not reciprocal: the school, teacher, or administrators are not expected to share their personal information with the students who register or enrol. The information is mostly not strictly confidential, but it isn't expected to be used for any other goal than registration or the monitoring of the student's progress in school.

Moral and political factors affected and impingement on context goals

Just like in chapter 3 I will use this paragraph to discuss what might be the harms and threats to political and moral factors such as autonomy, freedom, and the implications for justice, fairness and democracy when the GDPR is implemented in a education context. And just like with the context of healthcare, there doesn't seem to be a reason to think the GDPR will affect or harm these factors.

The GDPR doesn't have an affect on the freedom or autonomy: it doesn't change the amount of freedom that is already taken away by the compulsory education law. It may make it easier to switch schools due to the new right on data portability, although changing schools and transferring data between them wasn't very difficult before the implementation of the GDPR.

While there is a lot to say about the justice and fairness inherent in the school system, the GDPR does little to nothing to address any of that. In fact the GDPR does little to further the goals of education. It doesn't help students learn or teachers teach. It doesn't restrict the information flow of the knowledge being shared in classrooms. It will have more effect on the school administrators than on the teachers and students themselves, who are – or should be – the main focus in an educational context.

Contextual integrity

Since the GDPR doesn't have a strong impact on the goals of education or other political and moral factors possibly connected to it, the end result of the contextual integrity decision heuristic would likely be that the framework of contextual integrity favours the implication of this new practice. The expected information flows between student, school, parents, and some third parties like the education law authority or a physician, can be maintained under GDPR law.

One informational flow that may be altered is the flow of personal information about the student to the parents. When the students comes of age at sixteen, the parents are to be taken out of the loop. Report cards and attendance data can not be send to the parents without the students consent. One can wonder whether this alteration in the information flow is a bad one. It is uncertain if this change benefits or disadvantages a students educational progress. A rebellious student might use this lack of external control for skipping classes and less achievements, while a motivated student flourishes with this new-found autonomy. Besides, the way the student deals with this new self-ownership, can also help them grow on a personal level. Personal growth and character development are also an important value in the context of education.

My final verdict in this case would be that the GDPR respects the contextual integrity in the educational context, because of the limited effects it has on its core values and information flows.

Chapter 5: the context of business

The final context I will discuss is the context of business. This chapter will evaluate whether the GDPR respects contextual integrity in a business context.

The context

I take business to be very broad, containing both private companies and governmental organisations. This makes the context quite diffuse, because public and private organisations have vastly different values. This broad take does make describing the context somewhat difficult. So I will divide this description up in two where necessary.

The goal of business for a private company is to make as much money as possible for the owners and the shareholders. They usually do this by providing goods and services that are wanted by people in society and selling these goods and services with a profit. In governmental organisations the situations is a little different. The goods and services offered by governments are usually those that are needed by people, but can't be sold on a private basis since they are common goods or are deemed too important to privatise. Making money from it isn't a main objective, but may come as a side effect or a necessity to cover the costs.

A common private business situation can be: a costumer is in need of some goods, she then visits a store, either offline or online, to buy the goods. Whether this transaction takes place online or offline makes a lot of differences on the amount of data being shared. When the customer buys the good in a physical store, very little of her data is flowing to the business. Only in cases that the goods need to be registered or need to be delivered, the customer will have to share name and address and possibly a phone number. In some cases, like when buying alcohol or tobacco, the customer will be asked for a date of birth, which usually isn't registered. When this transaction happens online, the goods have to be delivered, so the customer will have to provide personal information like an address to finalize the transaction. Also, many web shops require you to make an account when ordering and will ask for more personal data during the process of creating this account.

A relatively new form in which information flows from customer to business, and from business to business, is companies offering free services but selling personal information of their customers to advertisers, who then can advertise a select and relevant group. The company then doesn't make money by selling goods or services themselves, but by selling advertising space. Advertisements paying for free goods is not a new practice – think of free newspapers that were being handed out at train stations that were more advertising space than news – but the collecting and selling of personal

data to make these advertisements more relevant is new. Never before was gathering personal information so easy; people freely give it up on social networking sites, websites can place cookies and trackers to find out exactly where a potential costumer surfs and how often he does so. The gathering, buying, and selling of personal customer data has become a way of creating profit for a company.

Usually the customer is free to find another seller if he doesn't like one business or doesn't want to give his information to this one business, sometimes however, businesses have a monopoly on goods. In that case, the customer is forced to deal with this company if he wishes to receive the goods. The information flow then changes from being optional to being compulsory. In government business this is always the case. There are several goods and services that the government has a monopoly on – and rightfully so. The only way to get a driver's license or a passport is through the government. In order to be able to deliver these and many other goods, the government does need personal information from its citizens.

It's hard to describe a canonical activity for the government context. Not all goods the government provides are directly asked for by citizens. Getting a passport or a drivers licence takes place in a similar way like buying goods at a store, the citizen is quite literally a customer in this case. But receiving goods like public streetlights or infrastructure, is not a direct response to a customer requesting and buying this good. It is provided by the government to the benefit of the people, the costs of which are not payed for by the ones using it, but by everyone through taxes and it requires little to no personal information. However, gathering those taxes necessary to fund these goods, does require a lot of personal information about citizens. It requires all the financial data concerning one person and other personal information used for identification. The information flows to and from the government are therefore very different, varying from case to case.

Information subjects, senders, and recipients

The information subject in a business context is the costumer in private business and the citizen in a governmental context. In private business the information flows from customer to business and from there on sometimes from business to business. For instance, when a web shop outsources its payment or shipping, the personal data of the customer is forwarded to the payment or shipping company.

In transactions with the government the information subject is the citizen and he or she is usually also the sender of the information, unless there is a lawful guardian or endorsee taking care of the subject. The recipient is almost always the government agency. A interesting deviation from this flow is the allocation of a citizen service number. The first time this a piece of information flows it is from

government to the citizen (or more realistically: its parents or guardian), as this piece of information is 'made up' by the government and allocated to the individual.

Transmission principles and entrenched informational norms

In many business contexts people expect to provide their personal data to the company that's providing them goods. If something needs to be delivered, and address is needed to complete the transaction or if a bill needs to be made, a name and some payment details are necessary. Most people have no problem with sharing these information attributes. It is expected in this context. The further use of this information isn't always expected by the customer. Some advertising by the company with which the transaction took place is to be expected, but most consumers don't expect their data to be forwarded or sold to other companies for advertising purposes.

Companies are also required to protect customer data to a certain degree. Especially data that when leaked can lead to the customers detriment, like when it increases the chances of (identity) theft, or creates a risk to the customers safety.

The government is also expected to gather some personal information. Since this information is often needed to provide the citizen with the goods and services it needs and wants. From the child benefits to the collective retirement benefits, the government will need and is expected to need certain information about an individual, such as but not restricted to: names, dates of birth, addresses, citizen service numbers, financial information, etc. People tend to get wary about the government collecting data about religious beliefs, political affiliation, sexual preferences and the like. So when the government proposes changes to the intelligence law, mandating intelligence services to monitor more people, gathering more data about them, and saving this data for a prolonged time – practices that may lead governments to collect data about the aforementioned attributes – people show some resistance. They do not expect this information to flow to the government.

Moral and political factors affected and impingement on context goals

Since buying and selling personal data is a way to make profit for some companies, the GDPR restricting this practice, is a direct impingement on the goal of a business context. However, this impingement is directly mitigated by the reduction of risks to autonomy and safety that the buying and selling of data creates for individuals. In the case of the Facebook scandal in the introduction, even democratic practice was harmed by this gathering of personal information for profit. It is likely that the contextual integrity decision heuristic would condemn the buying and selling of data for a profit. However, this is not the practise at stake here. Since the GDPR mitigates the risks to several

moral and political factors harmed by this business practice it is unlikely to do much harm to them itself in a business context.

In the case of government, there is also a chance that restricting the data flow may impinge on the end goals of this context. Sharing citizens data between different government layers, will make some government services easier, and perhaps less bureaucratic for the citizen. Luckily, under the GDPR the processing of data isn't only dependent on the consent of the citizen. When there is a lawful necessity to share or process the data, consent from the data subject is not needed. Thus the GDPR doesn't impinge on this government value.

Contextual integrity

So, does the contextual integrity decision heuristic judge in favour of the GDPR in a business context? I would argue that it mostly does. It restores the contextual integrity that was breached by companies using personal data for their own gain, without regard for the customer. While at the same time, it doesn't impinge on many government goals since is allows organisations to collect and process without the individual consent when there is a law based mandate.

Conclusion

In this conclusion I will give a brief recap of my research and I will give an answer to my research question.

Since laws protecting our core values from new technological advances are rarely tested, I set out to do just that. In this thesis I tested the General Data Protection Regulation – in effect as of 25th may 2018 - as a means to protect our privacy. To test this law, I used the framework of contextual integrity as developed by Helen Nissenbaum as a measuring stick. This framework was specifically designed to deal with new socio-technological practices and therefore suitable for this research.

The General Data Protection Regulation is a new data protection law by the European Union, aiming to protect the privacy of over half a billion people. It is based on its predecessor the Data Protection Directive and grounded in the Fundamental Rights of the European Union. It gives the EU-citizen several rights to govern their data and protect it from data hungry corporations trying to make money with this personal data, like Facebook.

According by the framework of contextual integrity, privacy is not protected when people have more control over their information, but when there is an appropriate flow of information. This appropriate flow is dependent on the context in which the information flows and governed by context relative informational norms.

When reading about the GDPR, it doesn't seem to concern itself with different contexts at all. The new rights that are given to EU citizens are all about more control on their personal information. From the right to access to the right to be forgotten, all are about the citizen controlling their information. However, when using the Contextual Integrity Decision Heuristic in assessing the contextual integrity in the different contexts in this research, it seems that the law does succeed in maintaining the contextual integrity. This leads me to the conclusion that while the law wasn't set up with the right focus – as it focusses on control of information instead of on context appropriate information flows – it does a pretty good job in keeping the information flows context appropriate and thereby respecting contextual integrity. Since contextual integrity is used as a benchmark for privacy, we can conclude that the GDPR succeeds in protecting the privacy of European Union citizens.

The fact that the focus of the law lies more on control of information instead of on appropriate information flows, may be explained by how difficult it would be to draft a general privacy law dealing with appropriate flows. The many different contexts existing, and the many different

appropriate flows in these context can hardly be governed correctly by one law, it would require too much detail. So perhaps privacy should be protected by a multitude of smaller laws, each focussing on specific contexts and the appropriate informational flows within them.

For now however, we may feel that our privacy as contextual integrity is sufficiently respected by the General Data Protection Regulation.

References

Books and articles

Jančiūté, L., (2016) 'EU Data Protection and 'Treaty-base Games', in: *Data Protection and Privacy*, R. Leenes, R. van Brakel, S. Gutwirth and P.de Hert (ed), 1-31.

Moor, J. H., (2005) 'Why we need better ethics for emerging technologies' *Ethics and Information Technology,* 7(3). 111-119.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119–157.

Nissenbaum, H., (2009). *Privacy in Context. Technology, Policy, and the Integrity of Social Life.*

Rys, L. and Grest, L, (2016) 'A New Era in Data Protection' *Computer fraud and security* Vol. 3, 18-20.

Sobolewski, M., Mazur, J. & Paliński, M. (2017) 'GDPR: A Step Towards a User-centric Internet?' *Intereconomics* vol. 52, 207-213.

Solove, D. J. (2008). *Understanding Privacy.*

Tankard, C. (2016). 'What the GDPR means for businesses' *Network Security* No. 6, 5-8.

Westin, A. F. (1970). *Privacy and Freedom.*

Zerlang, J. (2017) GDPR: a milestone in convergence for cyber-security and compliance' *Network Security* No. 6, 8-11.

Webpages

Autoriteit persoonsgegevens, https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens

Lex.europa.eu, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Handvest van de grondrechten van de Europese Unie, http://www.europarl.europa.eu/charter/pdf/text_nl.pdf

NYU: https://steinhardt.nyu.edu/site/ataglance/2012/02/inside-nyu-steinhardt-helen-nissenbaum-on-the-white-house-bill-to-protect-consumers-online.html

Wikipedia: General Data Protection Regulation, https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

GDPR info, https://gdpr-info.eu/