Ethics and Legislation regarding Internet of Things & Data

Information Technology and Society

Frank Helgers

ANR: 620258

July 2017

Master of Information Management
Tilburg School of Economics and Management
Tilburg University

Master's Thesis supervisors:

Hans Weigand	Tilburg University
Hennie Daniels (co-reader)	Tilburg University
Ruud Kuil	Business & Decision

Management Summary

Internet of Things utilizations are nowadays abundantly present in our world. Our mobile phones, smart televisions and self-driving cars are all examples of such Internet of Things utilizations. All these ‘things’ sense information, process data and intercommunicate with other ‘things’ and people. In this processing a lot of data is handled. This could be plain and simple data, but also very detailed or essential data.

With the rise of Internet of Things and other developments, there can be seen a Big Data trend. To be short, the term ‘Big Data’ implies that the gathered and processed data becomes more extensive, in multiple ways. The collecting, storing, using and processing of all these data has implications for individuals and societies. The data can be used in a beneficial way, but could also have harmful consequences. These developments bring ethical concerns.

This thesis examines the ethical values which could come at stake when data is processed. The practical viewpoint is taken from Internet of Things utilizations, because that development is highly connected with the Big Data trend. In this study a practical framework is developed, in order to use it in practical IoT cases and to discuss the ethical side of data handling. Besides this, new legislation is coming; the General Data Protection Regulation will come into force in May 2018. Therefore this study focuses also on the possible connection between the ethical values and the main determinations of this new legislation.

The research is according the principles of design science in information systems. With the help of sub-questions is worked towards the answering of a main question. Academic literature, the legal text of the GDPR and consultation with experts contributed to the research and the development of a framework. To assess the situation in practice a case study with an interview is carried out. Furthermore, a fictional case is proposed to illustrate the working of the framework.

Preface

This is a Master's Thesis report for the completion of my Master Information Management at Tilburg University. Technical developments in this digital information era are wonderful. But advancement comes with consequences for individuals and society. In order to optimally benefit from all these new developments, we have to consider more than the sheer technical side. That is the domain where my interest is sparked.

The IT consultancy firm Business & Decision gave me the opportunity to support the writing of my thesis with their practical input. Besides writing my thesis, I learned a lot and gained a lot of experience in multiple ways. My supervisor at Business & Decision was Ruud Kuil. He assisted me in my journey as an intern. I am thankful for his support and advice.

Hans Weigand was my graduation supervisor at Tilburg University. He was really supporting and inspiring during my research process. His expertise helped me in times of stagnation. Therefore I am very grateful.

Furthermore, I would like to thank Tim Straatsma, Chris Otten and Alex Aalberts for their help and their expertise during my time at Business & Decision.

Lastly, I would like to thank my interviewee at Vodafone. The insights he gave me contributed a lot to this thesis.

Frank Helgers
July 2017

Table of Contents

Management Summary 0

Preface 2

Table of Contents 3

Chapter 1. Introduction 5

1.1 Problem Indication 5

1.2 Internship at Business & Decision 6

1.3 Problem Statement 6

1.4 Research Question 7

1.5 Research Design and Research Method 7

1.6 Structure 7

Chapter 2. Literature Review 9

2.1 Internet of Things 9

2.1.1 Terminology, definitions and visions 9

2.1.2 Internet of Things in practice 11

2.2 From Data to Big Data 12

2.2.1 Data 12

2.2.2 Metadata 12

2.2.3 Big Data 13

2.3 Internet of Things and Data 15

2.4 Ethics of IoT and Data 17

2.4.1 Why ethics? 17

2.4.2 Power 19

2.4.3 The ethical values 20

2.4.4 Privacy 20

2.4.5 Confidentiality 22

2.4.6 Security 23

2.4.7 Transparency 23

2.4.8 Trust 23

2.4.9 Equality 24

2.4.10 Identity & Free Choice 24

2.4.11 Fairness 26

2.4.12 Categorizing of ethical values 26

2.5 Legislation & Regulations 27

2.5.1 The Dutch data protection law: *Wet Bescherming Persoonsgegevens* 27
2.5.2 What is a data breach? 28
2.5.3 Current situation European Union and the road to GDPR 28
2.5.4 Practical implications and determinations of the GDPR 29
2.5.5 Linking ethical values to GDPR statements 31
Chapter 3. Methodology & Research Design 34
3.1 Research & Methodology 34
3.2 The Research Artifacts 37
3.3 Research Design 38
Chapter 4. Results & Findings 40
4.1 Framework evaluation with experts 40
4.2 Fictional IoT case 41
4.3 Ethics in practice 44
4.3.1 Case setting 44
4.3.2 The process 45
4.3.3 Analysis of ethical values in the Vodafone case 47
Chapter 5. Summary, Conclusions & Discussion 48
5.1 Summary & Conclusion 48
5.1.1 The main research question 50
5.2 Discussion & Limitations 50
5.3 Recommendations 51
References 53
Appendix 58

Chapter 1. Introduction

1.1 Problem Indication

In 2015 every five seconds, five billion gigabytes of data was created (Zwitter, 2014). This generation of data will only continue and increase in the future. Data is nowadays collected everywhere. Messages on social media, posting pictures, measurements of weather information, navigational routes, cell phone records, search history; the list is endlessly. Regarding to Richard and King (2014) "we are on the cusp of a Big Data Revolution" (p. 393). This information revolution influences our society and our daily lives.

Not only the rapid increase of data collection is remarkable, but also the way this data is collected. One of the factors herein is the phenomenon Internet of Things. Simply said, Internet of Things encloses the concept of interconnectedness of objects. Things interact with each other. With the rise of Internet of Things, digitalization and the web of interconnectivity in our modern world, the control and overview regarding the matters data collection, data storage and data use, is vague and unclear.

What about data collection of an individual's' health by an insurer? Or what about a future employer who could see all kind of personal information of a possible employer? Who is accountable for hacks or system failures of autonomous systems like self-driving cars?

Individuals, corporations, government institutions and 'things' collect all kinds of data. On societal level we see for example the advent of smart cities. Implementation of IoT technologies in the public space could be really beneficial for the quality of living, but what are the limits of IT developments and in what way will this be governed?

These matters have all kinds of ethical implications for the whole society; on an individual level but also on the group level. Internet of Things and the use of data can be used in a beneficial way and can enhance societies, but there is also a dark side. An example: data analytics could be used to serve people's needs, but it could also be used to track political opponents and suppress freedom of speech. Values like privacy, equality and fairness, for instance, come into play when working with, and using, data. The ethical questions are an important part.

Besides that, regulations and legislation are also an important factor in this field of play. The General Data Protection Regulation of the European Union will come into force from May 2018 onwards. What does this mean for citizens, governments and businesses?

1.2 Internship at Business & Decision

Business & Decision Nederland is a consulting firm which focuses on offering solutions and strategic advice regarding Business Intelligence, Business Process Management, Data Management and Data Driven Business.

The company is at the center of the matters surrounding the use of data. How could data and information be beneficial in managing a business and be a competitive advantage? For the clients they advise it is important to know the current state of affairs in the field of information technology. Knowledge regarding developments, ethics and legislation (GDPR) in this field could benefit the company in consulting their clients.

In an academic way this topic is interesting because the developments in IoT and Big Data have an increasing impact on society. The rise of Big Data is a socio-technical phenomenon (Boyd & Crawford, 2012). Gaining more understanding of this phenomenon is valuable and helpful for society as a whole.

1.3 Problem Statement

There is a lot of vagueness surrounding the topics of Internet of Things and the enormous accompanying data collection. What are the limitations of corporations and governments when collecting, storing and using this data? Which ethical issues rise in this new information society?
What about the legislation and governance of privacy sensitive information? How should companies behave when collecting data?

All these questions are society wide problems. Malicious use of information technology and data could lead to disasters. Possibilities to make abuse of Information Technology are numerous (McCarthy, Halawi & Aronson 2005). Technology goes often in front of ethics and legislation, but companies nowadays do not have a clear framework of handling the difficult questions which arise in this new era. By making use of IoT a lot of privacy issues arise, for example (Weber, 2010).

By analyzing the current state of affairs, one can build on with further knowledge to a clearer framework regarding ethics and legislation of the IT trends IoT and Big Data. By means of a report where the problems and solutions are analyzed, this problem could be addressed. The focus will be on the ethical side and on the regulatory side.

1.4 Research Question

The main question is as following:

What ethical issues and GDPR norms have to be taken into account when handling data in Internet of Things utilizations?

In order to answer this question the following sub-questions are handled:

- What does the concept Internet of Things mean?
- What is (Big) Data?
- What ethical issues arise when working with data in Internet of Things applications?
- What kind of GDPR determinations address the issues concerning IoT and data?
- How do organizations handle ethics and regulations concerning IoT and data?

1.5 Research Design and Research Method

The problem will mainly be addressed through qualitative research. The data collection will be performed by means of in-depth interviews with experts in the work field of IoT and data. With gaining knowledge about the current situation, it is possible to develop some kind of framework regarding the problem. The purpose of this thesis is two-sided. How do the specific discussed organizations handle ethics and regulations (GDPR) concerning IoT and data? Secondly, in what way can they use a certain framework in practice regarding these issues? There will also be an analysis of a fictional case to illustrate the proposed framework in practice. In chapter 3 there will be extra explanation about the research design and methodology.

1.6 Structure

In the previous sections the topic was introduced and it is shortly clarified how the research will be composed. The next chapter consists of the literature research regarding Internet of Things, (Big) Data ethics. Besides this, the legislation, with a focus on the GDPR, is discussed. Chapter 3 will further elaborate on the research design of this thesis. After this, chapter 4 encompasses the findings and results. In the closing chapter will be room for discussion and recommendations.

Chapter 2. Literature Review

2.1 Internet of Things

The following section of this thesis will introduce, and further elaborate on the phenomenon Internet of Things.

2.1.1 Terminology, definitions and visions

The term ‘Internet of Things’ is now widely used for a couple of years. Especially in the field of information technology and management it is a well-known buzzword. The term hums around in business plans and policy papers.

Yet there is no single and unique definition of Internet of Things. The term originates from around 20 years ago, when it was used to encompass the work of the Auto-ID Labs. This is a research group working, among other things, on radio-frequency identification (RFID) infrastructures (Atzori, Iera & Morabito, 2010). From that time the definition and vision surrounding Internet of Things was further broadened and developed.

In 2012 the International Telecommunication Union (ITU) defined the Internet of Things as “a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies” (ITU, 2012).

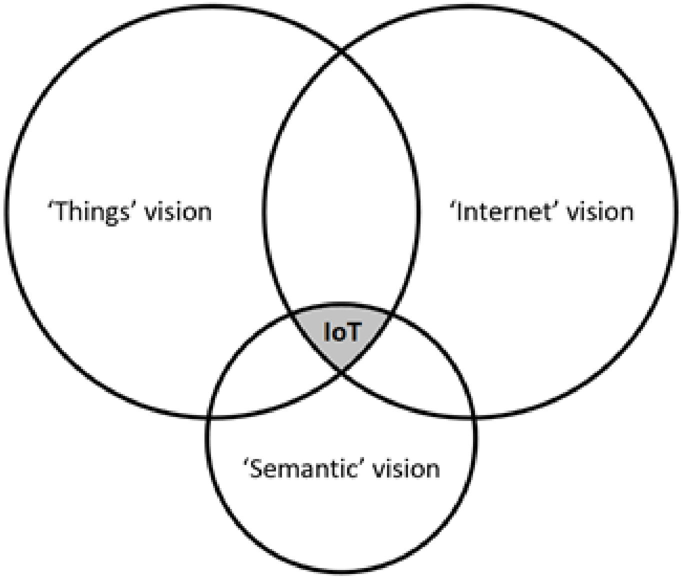


Figure 1. Internet of Things paradigm in academic literature

When using the term Internet of Things, one can differentiate between the ‘Things’ and the ‘Internet’. The first view emphasizes on the object itself which is connected. The second view focuses more on the networking technology such as the internet which enables the things to be connected. The combination of these two (the physical and the digital) provides the value which is assigned to this phenomenon.

As a third vision, the ‘Semantic oriented’ perspective comes into play. This is somewhat a bit of a side road. The main idea behind this vision is that there will be an extremely large number of items involved in the future internet. Issues concerning the representation, storing, interconnecting, searching and organizing information which is produced by Internet of Things practices will be very challenging (Atzori, Iera & Morabito, 2010).

The reasons for these different visions are the different perspectives stakeholders can take in the approach of Internet of Things. Hereby are the ‘Things’ approach and the ‘Internet’ approach the most common.

Other definitions of Internet of Things could be found in academic literature. Xia, Fang, Wang & Vinel (2012) refer to Internet of Things as “the networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence” (p. 1001). They further state that “IoT will increase the ubiquity of the internet by integrating every object for interaction via embedded systems, which leads to a highly distributed network of devices communicating with human beings as well as other devices” (Xia et al., 2012, p. 1001).

Furthermore, Giusto, Iera, Morabito & Atzori (2010) explain the concept behind Internet of Things as the presence of objects which are able to connect with each other, by means of unique addressing schemes. Those ‘things’ are capable of cooperating with other surrounding objects in order to reach common goals.

According to Chen, Mai and Liu (2014) the network architecture of IoT can be split into three layers. The sensing layer senses and collects the data by means of sensors. The network layer is in charge of the network functioning, information transmission and the connectedness between the IoT applications. Lastly, the application layer carries out the support of particular IoT applications.

2.1.2 Internet of Things in practice

The impact of Internet of Things is already highly noticeable in everyday society and will further increase to make its mark in everyday life. The US National Intelligence Council listed already in 2008 IoT as one of the six Disruptive Civil Technologies with great impact on the United States out to 2025 (National Intelligence Council, 2008). *Gartner, Inc.* forecasts that in 2020 there will be 20.4 billion connected 'things'.

The fields where IoT can be applied are abundant. IoT technology can be seen for instance in healthcare, agriculture, energy, logistics and transportation. In manufacturing you could see for example the term *Industry 4.0*. This refers to the smartness of the industrial processes whereby the implementation of Internet of Things is a major factor.

In urban development we know the term *Smart City*, where the concept Internet of Things could play a substantial role in several fields such as energy, traffic and security.

In our everyday lives we are surrounded by smartphones, computers and smart televisions. All of these objects are constantly connecting and interchanging information and tasks. Except from these yet ordinary utilizations, other smart applications such as energy control, lightning and smart washing machines will further appear in our households. In the future nearly every machine will be connected.

The impact of the concept Internet of Things is vast and will have a substantial place in future societies. The interconnectedness of objects generates and utilizes huge amounts of data. The next sections will expand on the vast amount of data which comes into play by the existence of Internet of Things.

2.2 From Data to Big Data

Every single day, 2.5 quintillion bytes of data is produced in our world. Remarkably, the last two years we created 90 percent of the total data out there in the world (IBM, n.d.). To illustrate, it is said that “every animate and inanimate object on earth will soon be generating data, including our homes, our cars, and yes, even our bodies” (Smolan & Erwitt, as cited in Richard & King, 2013, p. 41).

Data has been there always and it is everywhere. One could, for example, call the drawings from the Stone Age a form of data. Data in itself is a very broad term. In the light of this thesis, it is necessary to specify on the term data. Subsequently, the term ‘Big Data’ will be further explained.

2.2.1 Data

In a most simple way we can classify data as items that are the most elementary description of things, events, activities, and transactions that are “recorded, classified, and stored but are not organized to convey any specific meaning” (Maeder, Hädrich & Peinl, 2009, p. 4). By this explanation is not meant ‘elementary’ in a psychical way, referring to the natural sciences. Furthermore, one could categorize data into internal data or external data. Internal data refers to the data which is generated by the organization itself. When the data is generated by external parties, it becomes external data. Another way to classify data is the deviation between structured and unstructured data. In this way unstructured data refers to the data which can be found anywhere – such as the Stone Age drawings or nowadays text messages, videos and audio. Data gets structured when it is stored and organized in a database (E. Caron, personal communication, January 1, 2017).

Data items are the most elementary description of things, events, activities and transactions that are “recorded, classified, and stored but are not organized to convey any specific meaning” (Maeder et al., 2009, p. 4).

2.2.2 Metadata

A special kind of data is metadata. Simply said this is data about data. More expanded it is “data whose primary purpose is to describe, define and/or annotate other data that accompanies it” (Nadkarni, 2011, p. 1). How many times author ‘X’ is found in a library is for example metadata.

2.2.3 Big Data

Last decade the term ‘Big Data’ has come into play. The buzz word gained attention in business, media and the academic world. We have seen headlines like: “Big data is opening doors, but maybe too many” (Lohr, 2013). Richards and King (2014) speak about a ‘Big Data Revolution’ which is the latest stage in the Information Revolution. This Information Revolution started during World War II with the first stage being the power to compute, the second stage was the power to connect. In this third, and latest, stage it is about the power to predict. It is all about data. Richards and King (2014) state that “we have collectively built and are now living with a really big metadata computer” (p. 397).

In vernacular the term ‘Big Data’ is used all the time. Mostly it denotes the vague description of ‘very much data’. Academia as well as businesses all try to encompass the definition of Big Data, mostly from their own point of view. In order to elaborate further on this subject, it is needed to further discuss the term ‘Big Data’.

One of the first most cited definitions comes from a Meta –now Gartner- report dating from 2001. It speaks about ‘three Vs’, namely: Volume, Velocity and Variety. The report observes that the size of data increases, data gets produced in an increasing rate and the data varies more in terms of formats and representations. So there are at an increasing rate bigger data items with a greater variety in terms of data formats (Douglas, as cited in Ward & Barker, 2013).

After this, a fourth ‘V’ was included: Veracity. “Veracity includes questions of trust and uncertainty with regards to data and the outcome of analysis of that data (Ward & Barker, 2013). Veracity refers to the quality of the data. Businesses often add a fifth ‘V’: Value. This suggests that if you are going to put an effort in Big Data, it must have value (Anil, 2016).

In a survey of Big Data definitions Ward & Barker (2013) admit that there is a whole range of definitions, but there are some common denominators. Ward & Barker (2013) state that all of these definitions have at least one of the following assertions:

“**Size**: the volume of the datasets is a critical factor.
Complexity: the structure, behavior and permutations of the datasets is a critical factor.

Technologies: the tools and techniques which are used to process a sizable or complex dataset is a critical factor (Ward & Barker, 2013)."

In this Master thesis the term Big Data will be addressed by means of the five 'Vs', namely: Volume, Velocity, Variety, Veracity and Value.

2.3 Internet of Things and Data

With Internet of Things phenomena the world is encircled with a vast amount of sensors which are constantly collecting data. All these sensors generate daily a lot of data; one could refer here to Big Data. With the increase of Internet of Things utilizations, data collection will self-evidently increase as well.

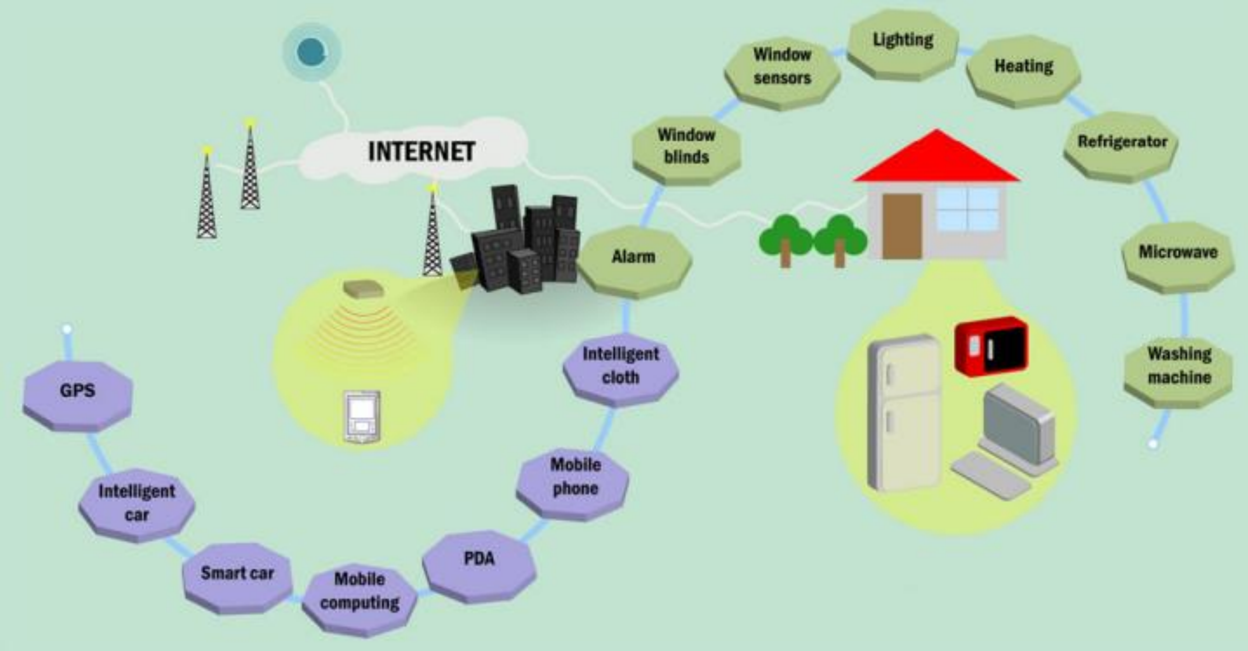


Figure 2. Illustration of data acquisition equipment in IoT. Reprinted from “Big Data: A Survey,” by M. Chen, S. Mai, Y. Liu, 2014, *Mobile Networks and Applications, 19(2),* p. 177. Copyright 2014 by Springer Science+Business Media.

Figure 2 (Chen et al., 2014, p. 177) illustrates some of these IoT utilizations which are abundantly present in our world. While the data collected by IoT devices is now still a fraction, the quantity of sensors in our lives will only increase. It is forecasted that by 2030 this quantity will reach a trillion. Consequently the IoT data will account for a much bigger fraction of the total Big Data collection (Chen et al., 2014).

Thus, it is clear that IoT devices and Big Data have an interdependency. Chen et al. (2014) articulate this as following:

> On one hand, the widespread deployment of IoT drives the high growth of data both in quantity and category, thus providing the opportunity for the application and development of big data; on

the other hand, the application of big data technology to IoT also accelerates the research advances and business models of IoT. (p. 177)

2.4 Ethics of IoT and Data

With the development of Internet of Things and the accompanying increasing existence of huge volumes of complex data, issues arise. Richards and King (2014) illustrate this as following: “We are building a new digital society, and the values we build or fail to build into our new digital structures will define us” (p. 395). When looking at these developments of IoT and (Big) Data it is important to notice the ethical values which come into play. Noting these values and eventually forming a new set of rules is important to control the societal costs of these developments without giving up on the huge possible benefits for society (Richard & King, 2014). What values are important? In this part the relevant ethical values will be discussed. Also the stakeholders in the field of play will be mentioned. First, ethics as a concept will be defined and the need for ethics in the context of IoT and data will be further articulated by means of some examples.

Ethics

Ethics can be described as the study of morality (Tavani, 2011). But was is this ‘morality’? Morality comes from the Latin word ‘mores’, which means something like manners or customs. Academic literature defines morality as “the systems of rules for guiding human conduct, and principles for evaluating those rules” (Tavani, 2011, p. 36). Gert (1999) offers another clarification on morality by stating that morality is “an informal public system applying to all rational persons, governing behavior that affects others, and includes what are commonly known as the moral rules, ideals, and virtues and has the lessening of evil or harm as its goal” (p. 58). Thus morality is sort of a set of guidelines for guiding human conduct. The policies or guidelines, belonging to morality, could be implemented in a formal or informal way. Laws could for example be imposed, but morality comes also with unwritten rules.

2.4.1 Why ethics?

In this section there will be some critical remarks on ethics regarding the handling of data and some questions will be raised.

One of the issues with Big Data is that it tends to accentuate correlation over causation (Zwitter, 2014). With enormous datasets it is easy to induce on data, but the possibility of wrong conclusions lingers. The next example illustrates this and rises the issues regarding propensity:

“What if Big Data analytics predict that a certain person (e.g. a single parent living in a certain neighborhood, with no job, a car, no stable relationship, etc.) has a likelihood of 95% to be involved in domestic violence?” (Zwitter, 2014, p. 4). Would it be ethically justified to send social workers to this person’s house?

Further, Hildebrandt (2013) addresses additionally the improper Big Data interpretation of people who advocate for the ‘N = all’ principle. This principle means that researchers or analyst interpret that the sample of a dataset is equal to the whole population. By stating this, red flags are raised nearly without thinking. The ones who advocate for this interpretation argue that the availability and use of huge amounts of data will make uncertainty in the predicted outcomes practically zero. But Hildebrandt (2013) denotes that the quest for the ‘why’ behind a certain situation or outcome is more and more dismissed. The causes behind the correlations seem to be less meaningful in the age of Big Data.

Along with the arrival of Big Data, other concerns rise in regard to de-identification of data. With the use of methods like anonymization, encryption and data sharding, data could not be coupled to real identities. But computer scientist have shown that it is in some cases even possible to re-identify this anonymized data and assign it to specific persons. The rise of Big Data and enhanced analyzing techniques support these developments (Tene & Polonetsky, 2011).

A typical example of an Internet of Things utilization case is the smart home care. Sensors in and around the house, as well as on persons, collect all kind of information like (body) temperature, blood pressure and humidity. The smart house regulates itself (like temperature and humidity) with the use of all this information. Assume an elderly person lives in this house. The house could ‘provide’ medicines for this elderly person if sensors and other indicators sense that the condition of this person is not optimal.

This case directly illustrates some issues and raises questions. To what extent will the autonomy of these IoT utilizations reach? Who is responsible for possible wrong medicament? What are the procedures when the systems in the house do not function properly anymore? In what way is all this data handled and secured?

All these examples denote some critical concerns regarding the handling of data in, for example, IoT applications.

The next section discusses the power paradox which comes with Big Data.

2.4.2 Power

‘Scientia potentia est’ is an old Latin proverb meaning ‘knowledge is power’. This saying can be extended to ‘information is power’. The use of (Big) Data can be very powerful in all kinds of utilizations and practices. But this brings some hazards. Those who are able to collect, to analyze and to make use of the knowledge have power over the ones who are not able to do so. The first group is able to set the rules and decides what questions are postulated.

Boyd and Crawford (2012) advocate that “the current ecosystem around Big Data creates a new kind of digital divide: the Big Data rich and the Big Data poor” (p. 674). The small group who is able to gather and use huge data sets has maybe disproportional power over others. Hildebrandt (2013) speaks about a knowledge asymmetry and questions if “we should accept the novel inequalities created by the knowledge asymmetries between data subjects and data controllers?” (p. 32).

Also Richards and King (2013) address this issue with the denomination ‘power paradox’; the arrival of Big Data generates winners and losers. An example of these issues can be seen in the occurring’s of the so-called Arab Spring. The usage of Facebook, Twitter and YouTube was used to track dissidents. These, possible harmful, uses of data can be seen in a lot of regimes but also in so-called liberal and democratic societies.

Certain questions can also be raised about the power of corporations like Google and Facebook. In what way do they use all the collected data and could this lead to disproportionate power distributions? Richards and King (2013) state the issues surrounding the use of data as following:

> Individuals succumb to denial while governments and corporations get away with what they can by default, until they are left reeling from scandal after shock of disclosure. The result is an uneasy, uncertain state of affairs that is not healthy for anyone and leaves individual rights eroded and our democracy diminished. (p. 45)

2.4.3 The ethical values

It is already said (and illustrated with the previous examples and cases) that Internet of Things and all the involved (Big) Data could lead to harmful consequences for individuals and society. The ethics of IoT and data study its system of morality, where evils and harms such as privacy invasion or manipulation rise. Therefore, it is needed to address some important ethical values concerning IoT and data in order to gain more knowledge about the issues in this field of play.

After reviewing some ethical values, an ethical framework could address the ethical concerns surrounding IoT and data and gradually give some handles to deal with these issues. Such a framework could be used in organizations to make ethical decisions in their business processes and to stay alert for moral concerns.

Essential to state is the notion that ethics per se are of a subjective nature. Opinions of what are 'the evils' differ from person to person. This thesis adopts a pragmatic approach, whereby the 'mainstream' ethical issues which are mentioned in academic literature, the media and jurisdiction will be discussed.

The following sections will discuss the ethical values.

2.4.4 Privacy

Privacy could be seen as of one of the key terms in the ethical debate surrounding data and IoT. But when looking at the term 'privacy' its definition plays a big role in the whole discussion. In common language we mean by privacy something like: information of me that is unknown to others. In *Privacy and Freedom* Westin (1967) described privacy as "the process of controlling the disclosure of information about an individual, group, or institution, to others" (Westin, as cited in Kwasny, Caine, Rogers & Fisk, 2008, p. 5).

Additionally, Parent (1983) defined privacy as "the condition of not having undocumented personal knowledge about one possessed by others" (p. 269). Important to notice in this definition of Parent is the word 'undocumented', where we will elaborate on later. The privacy of a person is thus lessened by the level of undocumented personal knowledge which is possessed by others, according to Parent (1983). Important hereby is the definition 'personal knowledge', which can be explained by the concept of 'personal information'. Parent (1983) stated this as following:

> Personal information consists of facts which most persons in a given society choose not to reveal about themselves (except to close friends, family, ...) or of facts about which a particular individual is acutely sensitive and which he therefore does not choose to reveal about himself, even though most people don't care if these same facts are widely known about themselves. (p. 270)

This definition of privacy (including the concept of personal knowledge) omits the knowledge of *documented* personal information. So there is a distinction between *undocumented* and *documented* personal information (Parent, 1983).

Parent (1983) has the following reasoning behind this: when a random person is looking in some old newspapers and sees the name of person X in a story about child prodigies who did not make it. This person X, a former child prodigy, is now an alcoholic and an obsessive gambler. Did this random person invade the privacy of person X? “What belongs to the public domain cannot without glaring paradox be called private; consequently it should not be incorporated within our concept of privacy” (Parent, 1983, p. 271).

Parent (1983) additionally stresses that it is important not to mistake documented facts with facts about individuals which are preserved on some kind of special file, used for special purposes. Think of health records in a hospital. What are these special purposes and what can be exactly called the public domain which Parent (1983) mentioned? It becomes clear that when excavating on the subject of privacy and personal information definitions are multi-interpretable and boundaries are vague.

Richards and King (2014) argue that it really depends on what we mean by the word ‘privacy’. Helen Nissenbaum (2009) argues that, with the word ‘privacy’, we actually address ‘the rules that govern the information flows’. The word ‘privacy’ has become sort of a buzzword to aim for something like ‘what are the information rules?’. Richards and King (2014) state that if we had to define and design things again the word ‘privacy’ would surely be exchanged by something other like ‘information rules’. Further, they argue that we should recognize that privacy is not just about keeping secrets from the world. Privacy is not a binary state, where information is either known to the world or is unknown. “Virtually all information exist in intermediate states between completely public and completely private” (Richards & King, 2014, p. 413). Keeping this in mind, it indicates the difficult fenced in framing of privacy Parent (1983) discussed.

For example: what is documented and what is undocumented information? What is the public domain and what is the private domain, especially in this digital world?

Therefore, this paper suggests that this digital age and the information revolution requires another outlook on privacy. Due to the vague and multi-interpretable definition of privacy it is useful to insert another value, namely confidentiality. The following section will further elaborate on this.

2.4.5 Confidentiality

When speaking about privacy it is maybe more applicable to talk about confidentiality. As argued before it is difficult to approach privacy in its purest form. A narrow understanding of privacy should be dismissed (Richards & King, 2014). In confidentiality can be found a sort of privacy founded by trust and reliance on promises in interactions (Richards & Solove, 2007). Confidentiality is all about relationships. It looks at the information you actually share with others, and in what way this is handled. When framing privacy in the form of confidentiality, it is much easier to handle the issues in this debate.

Richards and King (2014) argue that “shared private information can remain ‘confidential’” (p. 413). They reason that it is still possible to share private information in the digital world with all kind of parties we trust and to regulate this by laws of privacy. Privacy does not mean that no data can be shared, but it rather means that it can remain confidential. So we need to get rid of the notion that privacy is purely a state where nothing is shared with the outside world. That is where confidentiality comes into play. Private information could still be handled confidentially. In that way the benefits of data can be reaped, without the possible drawbacks. Because, in this digital era, we share much of our personal information willingly. Most of the time we keenly share our personal data for the sake of usability for instance. We want to use GPS to navigate and track our location, but we do not want this data to be used for unfavorable acts. It is difficult to balance on this thin line. Davis (2012) mentions accordingly that negative unintentional consequences, can quickly outweigh the possible benefits of Big Data developments. Confidentiality tolerates the benefits of sharing data and takes simultaneously privacy into account. It is confidentiality which offers some kind of trust to share information without handing in too much privacy (Richard & King, 2014).

2.4.6 Security

Accompanied with the values privacy and confidentiality rises another value; security. Working with personal data while establishing the privacy and confidentiality surrounding this data, comes together with security. Security measures are the means to ensure other values like privacy and confidentiality. Security as a value is also needed to cope with criminal activities like identity fraud and stolen information.

This thesis will not elaborate on the various technical ways like authentication and access controls to safeguard this security, but will merely address this important value of security. With the acknowledgement of this value, in for example an IoT utilization, specific security measures could be further refined.

2.4.7 Transparency

Transparency is a paradoxical concept in the ethical discussion surrounding data. Transparency is needed to build trust and confidence, but too much transparency (in the wrong places) can raise issues with privacy or confidentiality. “Transparency…fosters trust by being able to hold others accountable” (Richards & King, 2014, p. 419). There is always a thin line between secrecy and openness. Transparency can lead to positive actions, but it can also have a harmful effect when it is used in the wrong way.

An additional paradoxical aspect of transparency is the expressed potential of (Big) Data to make the world more transparent, but in the same way, the collection, use and analyzing of this data is mostly done in secrecy (Richards & King, 2013). Regarding this, it is necessary to critically address the balance between openness about the process of collection and handling (Big) Data and the secureness.

2.4.8 Trust

The value trust is also an interconnected value with transparency and confidentiality. We can define trust as “the level of confidence with which an entity can ensure to another entity or entities specific services tailored for given contexts and quality (fitness for purpose and reliability)” (Kounelis, Baldini, Neisse, Steri, Tallacchini & Pereira, 2014, p. 74).

This trust is for example fostered by transparency. If you are better informed on how things are organized in an organization, this could lead to a better outlook regarding the trustworthiness of that organization.

In this way, you as a consumer have confidence in the way things are handled in this organization. This trust can also be stimulated by imposing sufficient security measures.

2.4.9 Equality

In the study of morality the ethical value equality also plays a role. This value is in danger when for example an algorithmic bias appears. What if a recommendation system has built in biases and produces outcomes that are different for a range of people? The output is unequal. The recommender system acts like a black box. Only the output and some of the input is visible. What happens inside cannot be observed. Subsequently, the behavior of these people is manipulated. In such situations not only the value transparency is impaired, but ethical concerns about equality could be raised when this output is produced with a malicious agenda in mind (Paraschakis, 2017). What if some people are deliberately faced with other outputs or other results, which could negatively impact them?

Another example could be seen in A/B testing. This is a testing procedure where two or more groups are exposed to different algorithms, or are exposed to different content on a website, for instance. These tests result in more information about the interaction of people, or the consequences of different content. Facebook, for example, manipulated in 2012 the timelines and news feeds of more than 600,000 users in order to study the phenomenon of emotional contagion (Paraschakis, 2017).

In the previous examples the value equality is highly linked with the value transparency. The actions which could be seen with a recommender system and A/B testing lack a certain amount of transparency.

In a simpler example, the value equality plays a role when in the design of an IoT application English the only possible language is which can be chosen. People who do not master this language are less able to use and understand the functioning of a particular application.

2.4.10 Identity & Free Choice

The term ‘identity’ is used in a lot of ways. One definition of identity is as following: “the identity of a thing, including a person, is comprised of those properties or qualities which make it that thing” (Richard & King, 2014, p. 422). In this way you can say that when the specific properties or qualities are changed, this ‘thing’ has a new identity.

Famous psychologist Erik Erikson (1968) stated identity as "a process 'located' in the core of the individual and yet also in the core of his communal culture, a process which establishes, in fact, the identity of those two identities" (p. 22). Furthermore, Cohen (2012) argues that selfhood and social shaping are linked. This selfhood is the combined action of the autonomous selfhood and the reality social shaping.

Linked with identity is the right to choose who you are; the free choice to define yourself. I like this, I am that, I am supporter of this, I am against that, I buy this, and so on. Richard and King (2013) see the 'Identity paradox', whereby "big data seeks to identify, but it also threatens identity" (p. 43). 'Shaping' of identity is of all times. Hundred years ago your identity was also influenced by, for example, the newspapers you read. Identity is shaped all the time by interacting with the environment. But which role plays Big Data nowadays herein? Richard and King (2014) state that "as consumers, our identities are increasingly being shaped by big data inferences and the companies that control them" (p. 424). Companies are able to access or collect data about basic characteristics of people such as their search behavior on internet, 'likes' on Facebook and buying behavior. Combining this kind of information could lead to "you will like this", instead of "I like this" (Richard & King, 2013). When you execute a search in Google's search engine or browse through your timeline on Facebook, what you see is influenced by their algorithms.

Andrew Leonard (2013) writes for instance in his article about Netflix:

> The companies that figure out how to generate intelligence from that data will know more about us than we know ourselves, and will be able to craft techniques that push us toward where they want us to go, rather than where we would go by ourselves if left to our own devices. (para. 20)

Again, the influencing effect of the environment is not new, but in this age of Big Data, this game is stepped up and the precise impact is yet vaguely identified. Big data could be used in a very powerful way.

> If we lack the power to individually say who "I am," if filters and nudges and personalized recommendations undermine our intellectual choices, we will have become identified but lose our identities as we have defined and cherished them in the past. (Richard & King, 2013, p. 44)

2.4.11 Fairness

One of the most difficult ethical discussions is about fairness. Fairness is a thin conception. Some say that fairness is strictly in the eye of the beholder. One can define something as fair, what could be seen as unfair for the other. Society defines and constitutes fairness constantly; it is an ongoing process. The notion of fairness changes over time. Therefore this thesis will not dwell on the precise standard of fairness, but merely addresses the important considerations regarding fairness in IoT and (Big) Data practices. Society must and shall define what could be considered fair and what is not. In the development and utilization of IoT practices this value is something which is important to examine.

2.4.12 Categorizing of ethical values

The described ethical values could be categorized in groups of values. In this thesis we differentiate between social values and communicative values.

Communicative values	**Social values**
Privacy	Equality
Confidentiality	Identity
Security	Fairness
Transparency	
Trust	

Table 1. Categorizing of ethical values

Appendix

The appendix encloses an overview of all the ethical values with a short and concise definition per value.

2.5 Legislation & Regulations

In this section the regulations and legislation surrounding data will be discussed. The focus will be on the new General Data Protection Regulation of the European Union which will be enforced on the 25th of May, 2018. Apart from that, the current Dutch law concerning the protection of personal data ('Wet Bescherming Persoonsgegevens') will also shortly be discussed.

2.5.1 The Dutch data protection law: *Wet Bescherming Persoonsgegevens*

Currently, this law regulates all the matters concerning the handling of personal data and information (Autoriteit Persoonsgegevens, n.d.). This law dates from September 2001 and is based on the European directives of the protection of personal data. The law is all about the handling personal data in a legitimate way. The main determinations are:

- Personal data can only be handled according to the law and needs to be processed in a decent and careful way;
- Personal data can only be gathered under the guise of specific, prior explicitly defined, and justified objectives. Further processing is only justified when the objectives are compatible with this statement;
- The person involved (of whom the personal information is processed), has to be informed about the identity of the organization or person (the one who is responsible), who is processing the personal data. Also, the objective of this data processing has to be clear;
- The processing and handling of data has to be secured in a suitable way. Additional rules apply for special information like race, health condition and religious beliefs.

As of January 2016 the *Wet Bescherming Persoonsgegevens* is expanded with the report duty in the case of data breaches. Organizations (government and companies) have to report to the *Autoriteit Persoonsgegevens* (the Dutch authority concerning personal data) immediately, in the case of a serious data breach (Autoriteit Persoonsgegevens, n.d.)

2.5.2 What is a data breach?

In the case of a data breach it is about access, destruction or releasing of personal data in an organization, when this is not the intention of the organization. This is also true for illegitimate processing of personal information. There is a violation of the protection of personal data. Examples are the loss of an USB-stick, a stolen laptop or the access to data because of a hacker (Autoriteit Persoonsgegevens, n.d.).

The exact interpretation of these laws is up to jurisdiction.

2.5.3 Current situation European Union and the road to GDPR

In the existing situation every member of the European Union has its own regulations concerning data protection and the handling of personal information. In this sense, the rules and laws are fragmented across whole Europe. A Dutch company operating in France has to comply with the French law. This law could differ from the Dutch law. Remarkable for the digital world is the absence of boundaries as can be seen in the 'real' world. The internet does not stop at the border of a country. Kobrin (2001) touched this problem also in his research of territoriality and the governance of cyberspace. "Internet transactions are non-vectorial, they are difficult to locate in two-dimensional geographic space and thus render territorial jurisdiction problematic" (Kobrin, 2001, p. 690).

With the new General Data Protection Regulation (GDPR) the EU tries to simplify and rectify the regulations across the whole union. It is a step to "strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market" (European Commision, n.d., para. 2). The unification of regulations has to lead to less bureaucratic and administrative hassle. In December 2015 the policymakers agreed upon the new data protection rules. From May 2016 the regulations came into force, but from May 2018 onwards the rules have to be officially obliged by all EU members.

2.5.4 Practical implications and determinations of the GDPR

The following sections will go into more detail about the determinations and effects of the GDPR (Deloitte, n.d.; EUR-Lex, 2016; “[GDPR Key Changes],” n.d.; Regulation (EU) No 2016/679, 2016).

Scope of the legislation

The most important thing is that this legislation “applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company’s location” (“[GDPR Key Changes],” n.d., Increased Territorial Scope (extra-territorial applicability) section, para. 1). Thus for example, an American company working with personal data of people in the EU, does also have to oblige to these regulations.

Penalties

The GDPR can result in fines up to 4 percent of the annual turnover of an organization, with a maximum of 20 million euro. These maximum fines are meant for the most serious violations such as infringing on the core of Privacy by Design concepts.

Consent

Consents have to be more easily understandable. Long and complex terms and conditions are not done. Furthermore, the terms have to be easily accessible. The purpose of the data processing must be clear, explained in plain language.

Breach Notification

As seen in the current Dutch data laws, a breach notification is yet mandatory. With the GDPR this report duty will be required in all member states, when there is a risk for the individual’s rights or individual’s freedom. It is needed that the notification of the breach takes place within 72 hours after the awareness of the breach. Besides this, the data controllers need to notify their customers when becoming aware of a data breach.

Privacy by Design

The concept Privacy by Design is already known in business and academic literature. With the GDPR it gets more and more important, as it becomes a legal necessity. The concept Privacy by Design needs to be encompassed and implemented in the beginning of the total design of a system, application or data warehouse. Data minimization should, for instance, be default.

Right to Access

In order to enhance transparency, data subjects have the right to be informed about the processing of possible personal data and for what purpose. If personal data of a data subject is handled within an organization, is has to be possible to get a copy of this personal data. In that way it is clear for EU citizens which personal data is used.

Right to be Forgotten

The Right to be Forgotten is another determination to strengthen the individual rights of EU citizens. The data subject has a right to demand erasure of his or her personal data. The exact elaboration of this right is outlined in Article 17 of the GDPR. This is also known as the 'right to erasure'. When one of the six conditions apply (as stated in Article 17), the data controller is obliged to erase the personal data of the data subject. One of these conditions is as following: "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed" (Regulation (EU) No 2016/679, 2016, Article 17).

Right to Rectification

The data subject has a Right to Rectification if the personal data is inaccurate. This is also in line with the Right to Access and gain insight in your personal data as a data subject.

Data Portability

This right to Data Portability is also in line with the previous rights such as the Right to access, the Right to be Forgotten and the Right to Rectification. All these rights give the individual EU citizens more power over their 'own' personal data. The data portability right entails the right to transfer your personal data from one data controller to the other. The data controller has to cooperate in this process.

Data Protection Officers (DPO)

In section 4 in the new regulations the data protection officer is discussed. In some cases the appointment of a data protection officer is compulsory. A data protection officer is needed when:

(a) The processing of data is "carried out by a public authority or body, except for courts acting in their judicial capacity" (Regulation (EU) No 2016/679, 2016, Article 37).

(b) “the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale” (Regulation (EU) No 2016/679, 2016, Article 37).

(c) “the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10” (Regulation (EU) No 2016/679, 2016, Article 37).

Within the designation, position and task of the data protection officer there are some other conditions. For example, a data protection must not carry out other tasks that could lead in a conflict of interest. The exact conditions of this data protection officer are outlined in articles 37, 38 and 39, and in the referred articles of the GDPR.

One Stop Shop

One of the important reasons for the introduction of the GDPR is the harmonization across all member states of the EU. With these regulations it is tried to imply a ‘one stop shop’ model. Organizations will be supervised and regulated by the data authority of the country where their main establishment is. Thus, they have to deal with just one regulator.

2.5.5 Linking ethical values to GDPR statements

Legislation happens not out of the blue. The rules have a purpose to serve some fundamental values and rights of citizens in the EU. The above stated determinations could be linked to some of the previous stated values. The question here is: which values support the peculiar determinations in the GDPR? Surely, the values could not be linked one-to-one, but the values do say something about the motives to establish these rules. By analyzing this, there can be found some overlap within the ethical values and the determinations of the GDPR. This is illustrated in figure 3 and figure 4. For some determinations it is pretty clear which value is supported (Transparency & Consent), for others this is more vague (Data Protection Officer).

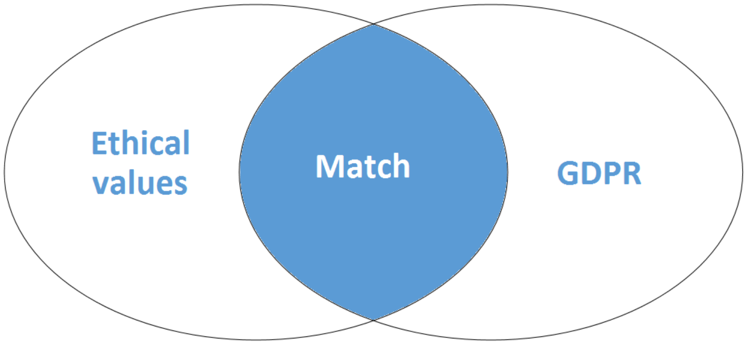


Figure 3. Matching values with the GDPR determinations

The matrix in figure 4 connects the particular ethical values with the GDPR determinations.

Privacy			🟦		🟦			
Identity					🟦	🟦		🟦
Transparency	🟦	🟦		🟦				
Confidentiality	🟦		🟦					
Security		🟦	🟦					
Trust	🟦			🟦				
Equality	🟦							
Fairness						🟦		
	Consent	Breach Notification	Privacy by Design	Right to Access	Right to be Forgotten	Right to Rectification	Data Protection Officer	Data Portability

Figure 4. Matrix with matches between ethical values and GDPR determinations

In matching the values with the GDPR determinations, the most evident and clear combinations are stated only. Surely, in some sense almost all values could be coupled to some of the GDPR determinations, but in the deliberation is only chosen for the most distinct matches.

The value privacy can be connected with the Privacy by Design determination and the Right to be Forgotten. Both determinations promote the ideas behind the value privacy. The value identity can be seen in the Right to be Forgotten, Right to Rectification and Data Portability determinations. These are all rights to give the individual extra control and authority over ‘their’ data. Transparency can be identified in the need for a well-formulated consent, the Breach Notification determination and the Right to Access. These three determinations all try to enhance a certain level of transparency. Confidentiality is matched with Consent and Privacy by Design. The determinations in a consent have a purpose to nurture the confidentiality in a relationship. The statements are agreements between the two parties. Privacy by Design is also a way to enhance the level of confidentiality in the relationship. The value security can also be seen in the Privacy by Design determination. In an early phase developers have to take into account the privacy and security measures of a utilization. Also, within the need for a Breach Notification, security motives are seen. If such a breach occurs, fast and secure notification to the right persons and organizations could help in a quick recovery, or could prevent further harm. The value trust is nurtured with the establishment of a well-formulated consent. Statements in a consent could prosper the trust between parties. Additionally, the Right to Access, could prosper the trust. If customers are allowed to get access to 'their' data, this functions as a kind of reassurance in the relationship. Equality is seen in the Consent determination. The purpose of this determination was to establish a consent which was written in clear language and better understandable for 'normal' people. This fosters the equality because a wider range of people is able to get a good grasp of the terms and agreements which are discussed in a consent. Lastly, fairness is a value which can be identified in the Right to Rectification. Such a determination is intuitively in line with the value fairness. If false information of yours is used and processed, it is fair to say that you have a right to rectify this.

The matrix shows also that the Data Protection Officer norm, a determination is which is not specifically matched with values. The Data Protection Officer norm can be seen as a secondary determination which supports other norms and values indirectly. The DPO is, for instance, responsible for the procedure surrounding a data breach in an organization.

Chapter 3. Methodology & Research Design

This chapter elaborates on the qualitative research design of this Master thesis. The research started with an introduction of the subjects and the accompanying research question which are investigated. Then, the academic literature in this field was reviewed. After this, an initial version of a framework regarding ethics and the General Data Protection Regulation will be developed. This framework will be propounded in practice. Hereafter the proposed recommendations and feedback will be incorporated in the framework and the response will be described. Furthermore, chapter 5 shall consist out of the answering of the sub questions and conclusions.

3.1 Research & Methodology

Literature review

The literature review of chapter 2 served as the explorative part. In this part the existing literature was discussed in order to gain an understanding of the issues in the field. Topics in this section were Internet of Things, (Big) Data, Ethics and Legislation.

Framework

The framework is founded upon two main parts:

- The academic literature regarding IoT, data and ethics;
- The documentation of the General Data Protection Regulation and other secondary sources.

Feedback of experts

Beside the literature, consultation took place with experts in the work field of IT and Data Management. Their job roles are Product Manager Data Management and Portfolio Manager. These experts offered feedback to refine the initial framework. This took place in the first stages of the development of the framework. During three iterative and interactive discussions of approximately one hour each, the progress of the framework was evaluated.

Case study interview & Fictional Case

By means of an analysis of a case and an interview with an expert in the field, the issues surrounding the handling of data will be further investigated. The purpose of this interview is two folded. Firstly, how do organizations handle ethics and regulations concerning IoT and data? Secondly, is the framework useful in practice? The interviewee is an Access Network and Innovation architect at VodafoneZiggo who is highly involved with Internet of Things and Big Data developments. Besides that there will be an analysis of a fictional IoT case in the medical sector. The framework shall be applied and examined.

End Framework

After the examination of the response to the framework in practice, the knowledge in literature and the experiences in practice can be combined to develop a framework which addresses and informs about the issues that should be taken into account when working with data in practice.

This research design is illustrated in figure 5 below.

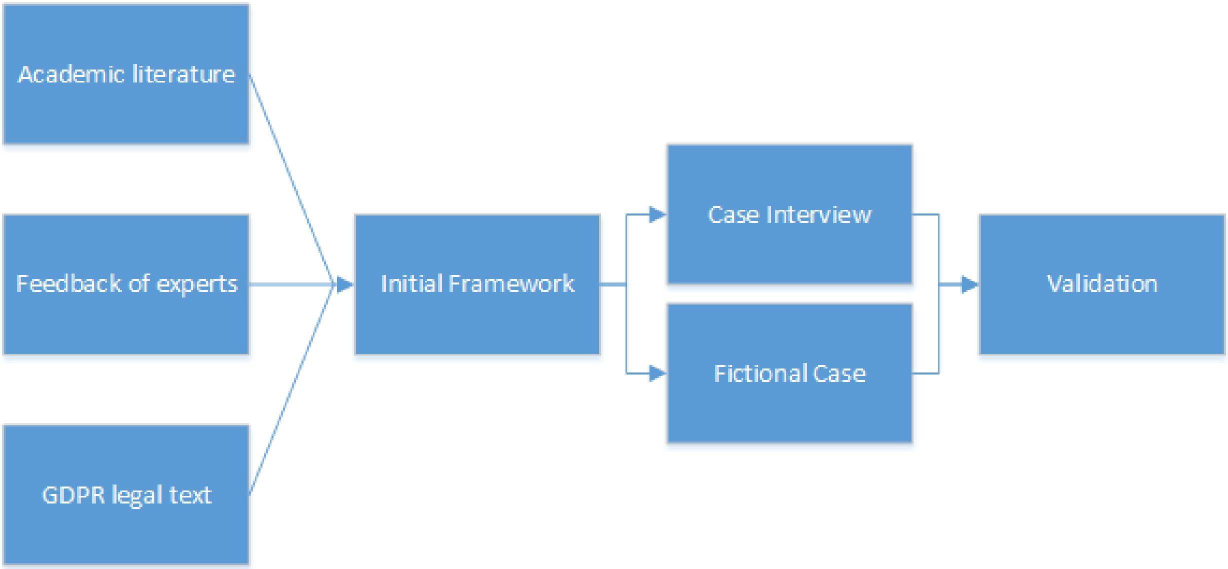
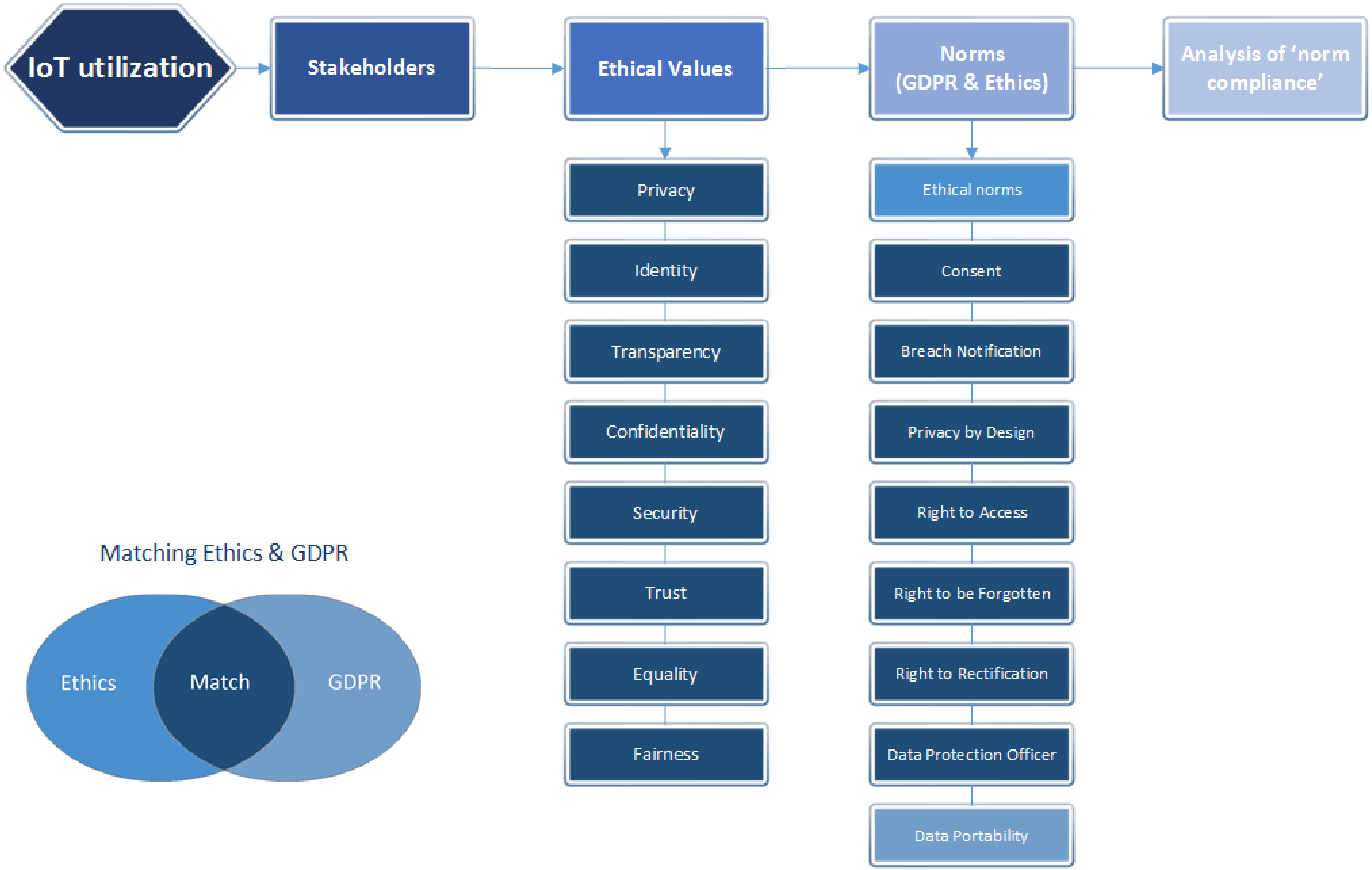


Figure 5. Research Design

The next page shows the proposed framework to handle ethical issues with regard to data in Internet of Things utilizations.

Framework for IoT utilizations



3.2 The Research Artifacts

The framework

The starting point of the framework is the IoT utilization. What kind of utilization is this? How does it work? What are the goals of the utilization? After identifying and describing the IoT utilization, the involved stakeholders are considered. In order to incorporate the perspectives and consequences of all different entities which could be affected, it is needed to address the stakeholders within the development and use of an IoT utilization. Every stakeholder has peculiar interests. Different IoT utilization have different consequences for people and society. In figure 6 an example of a stakeholder overview can be seen. In this case the firm is stated in the center, surrounded by other stakeholders.

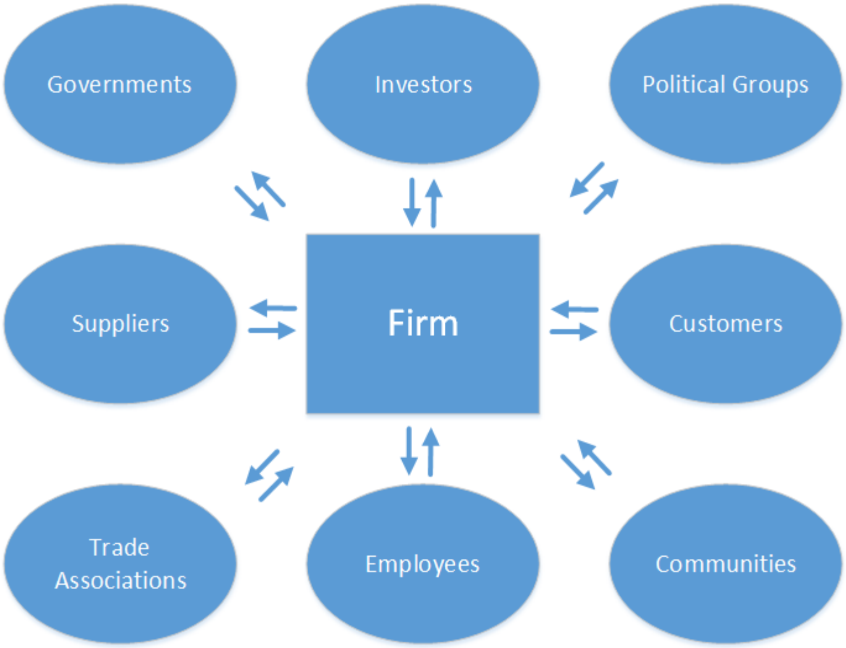


Figure 6. Contrasting Models of the Corporation: The Stakeholder Model. Adapted from "The stakeholder theory of the corporation: Concepts, evidence, and implications," by T. Donaldson, L. E. Preston, 1995, *Academy of management Review, (20)1*, p. 69. Copyright 1995 by Academy of Management Review.

After the stakeholders, the various values are discussed. The values are privacy, identity, transparency, confidentiality, security, trust, equality and fairness. These values are extensively reviewed in chapter 2. Subsequently, norms regarding the values could be distinguished. Norms which unite with societal norms about certain values and what the organization thinks is needed. Besides that, the GDPR norms are postulated. These norms refer to the main determinations from the legal text of the General Data Protection Regulation.

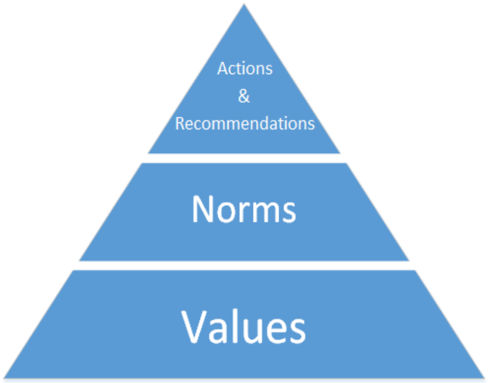


Figure 7. From values to actions

These legal norms are Consent, Breach Notification, Privacy by Design, Right to Access, Right to be Forgotten, Right to Rectification, Data Protections Officer and Data Portability. The clarification of these determinations is stated in section 2.5.4. After recognizing these norms, they can be gradually analyzed in the company. The main question is then: are we compliant with the posed norms?

The purpose of the framework is to acknowledge the ethical values as the foundation of the conduct of business. In figure 7 this is illustrated; values account as the foundation, whereupon consecutive norms and actions could be formulated. By using the matrix in figure 4 the matches between ethical values and the GDPR norms could be identified.

3.3 Research Design

The research design of this thesis is according to the seven guidelines for design science in information systems research of Hevner, March, Park and Ram (2004). This section describes the adoption of these seven guidelines:

(1) Design as an Artifact
(2) Problem Relevance
(3) Design Evaluation
(4) Research Contributions
(5) Research Rigor
(6) Design as a Search Process
(7) Communication of Design

The research of this thesis is aimed to create an artefact such as the framework which is discussed in section 3.1 (1). The relevance of the topic is discussed earlier; the handling and use of data (within IoT applications) could have beneficial consequences, but also harmful consequences. This is a society wide issue, on the individual level and the group level (2). The design evaluation is carried out by means of observational and descriptive methods (3). The design of the artifact should contribute to the research in this area (4). The initial framework is formed with academic literature and the legal texts as foundation. Besides this, experts offered their view on the artefact. The artefact is hereafter evaluated by conducting interviews in the work field (5). As typical in design science, the modeling of the artifact is an iterative and interactive process. The generation of frameworks is followed by testing and assessing. After this the cycle restarts (6). When the response to the framework in the work field is gathered, this will be described and communicated extensively (7).

Chapter 4. Results & Findings

This chapter covers the results and findings of the research. The first section elaborates on the findings of the first phase discussions about the construction of a framework to use in practice. The second section describes the fictional IoT case in the medical sector. Lastly, the findings after interviews and examination in practice will be discussed.

4.1 Framework evaluation with experts

In this section the modelling process of the initial framework is discussed.

The first version of the framework consisted actually out of two frameworks. One was regarded to ethical values specifically, the other covered the main GDPR determinations. These frameworks where derived from academic literature, legislative texts and other sources.

But this twofoldness of the frameworks was a problem. The intention of a framework was to discuss the ethical issues and the GDPR norms simultaneously. The overlap between the determinations and ethical concerns regarding the handling of data had to be explored. The experts stated in their feedback that the frameworks had to be combined in order to properly discuss the ethical concerns, and not only the GDPR determinations. The notion was that businesses in practice wanted to see concrete implications. Without some connection to the GDPR, the ethical values might be overlooked.

The matches between the ethical values, which could serve as the foundation for some GDPR determinations could also be seen in the matrix where the ethical values and GDPR determinations are combined. The idea of such a matrix was discussed during the consultation with experts.

Besides this, the idea of some sort of a statements survey was suggested for the next phase. During the discussions it became clear that this maybe would oppress the open conversation about ethics. Because of the abstract nature of ethical discussions such a narrow-minded discussion about privacy or other ethical values would not be constructive.

Thus, the consultation with experts resulted in a framework which combined the ethical values and the GDPR determinations. With such a framework it would be interesting to discuss the overlap between the ethical values and the GDPR. Additionally, the stand-alone issues of the GDPR and the ethical values could be spotted.

4.2 Fictional IoT case

The upcoming part exhibits a fictional IoT case in the medical sector. According to the framework, which is proposed in chapter 3, the stages will be discussed gradually. Only some main ethical issues with regard to IoT and especially the data processing will be covered. Furthermore, this analysis is not entirely comprehensive; it functions mainly as a showcase to illustrate the framework.

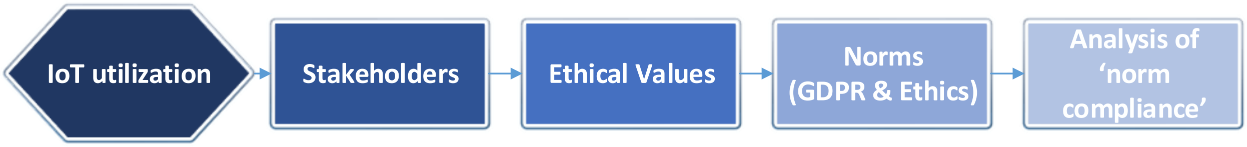


Figure 8. The stages of the framework

The IoT utilization

This Internet of Things utilization is a band which you can put on your arm to monitor your heart rate. The band is interconnected with an application on your phone. The application displays the real-time heart rate and shows statistics and the development of your heart rate during past times. Besides the interconnectedness with an application on your phone, the data gets transferred to a doctor. In this way, the medical staff can monitor you and interfere if needed.

The stakeholders

For the sake of brevity, this section highlights only the four most important stakeholders. The patient or 'customer' is the main stakeholder. Besides this the medical staff which is involved in the treatment of this patient is also part of the equation. The institution, such as the hospital which facilitates the treatment, is a stakeholder. The company which facilitates the technical part of the band, such as the device itself and the software (to interconnect, software for the medical staff and the application) is also a stakeholder.

When the stakeholders are identified, this knowledge can serve as an illustrative guideline to assess the accompanying ethical issues which could arise and need to be discussed.

The ethical values

Privacy and especially the confidentiality of the monitored data is very important in this case. For example, it could be harmful for the patient if information about some episodes of bad heart functioning got unwillingly known to the public or to some people specifically. Therefore, the confidential processing of this information is crucial. Combined with this is the value security. To ensure the confidential handling and protect the privacy of a person, security is needed. The technical part of the IoT utilization has to guarantee that the utilization functions properly, without data breaches or malicious attacks from outside. In the light of this it is also crucial that the intercommunication of data is processed securely.

Additionally, the patient has a bond of trust with his doctors, with the hospital and with the creator of the IoT utilization. The patient needs to have a certain level of confidence in this relationship. This trust is fostered by a certain level of security but also by another value, namely transparency. The relation is a bond of trust where good communication plays a vital role. With communication the value transparency can be supported. The patient needs to know how the utilization works, what the procedures are and what happens with the processed data for instance. If this is clarified it could improve the bond of trust. All the stakeholder are herein involved, albeit from other perspectives. The facilitating organization, such as a hospital, enters a strong relationship with the producing company. The medical staff needs to rely on the hospital and so forth. In this chain of trust the patient is the end user.

The value identity and the accompanying right to choose who you are, to a certain extent, or what you decide to show to the outside world, play also a role in this case. Once more, this value is highly linked with the other values. For example, in order to define yourself to some extent, you need to be able to govern the display of your heart rate data to the outside world. Well-constructed privacy and security measures are essential to facilitate and support the right to define yourself.

Next is the value equality. One could think in this context about the importance of an equal treatment and handling of the medical data. The technical set-up of the utilization has to be carried out with care. The statistics in the application with regard to the data have to be presented in an understandable manner for a wide range of people. Elderly people, for example, need to get a proper chance to (surely within boundaries) make use of this technical utility. The usability of the application also needs to give these elderly people the opportunity to apply this technical device in a fairly equal manner to their lives. In the development process of the band all the four main stakeholders have a saying in this.

Likewise, the value fairness can be discussed in this context. Because of the subjective notion of fairness it is difficult to assess this value. That being said, it does not mean that the value fairness should be dismissed in ethical discussions. In the context of this case, one could argue what exactly fair is in the dedication for equality. How far should the manufacturer of the band go in order to guarantee the usability for everyone?

Norms

The next stage examines the accompanying norms. Two kind of norms are distinguished in this part; the ethical norms and the GDPR norms.

When working according to the stages of the framework for all the above ethical issues, different views and conceptions about the values can be chosen. Consequently, these standpoints are translated into norms. A certain norm to support the issue regarding identity could be as following: “within the context of this utilization the patient/customer may self-decide up to what level of detail his/her heart rate data is shared and showed”.

Besides the ethical norms, GDPR norms are postulated. These come into force in May 2018. One norm, which is associated with the previous stated ‘identity norm’, is the Right to be Forgotten. Shortly, this determination implies that the data subject (in this case the patient), has the right to demand erasure of his or her personal data. With this example, the overlap between the ethical values (and the accompanied norms), can be recognized. The GDPR norm supports the identity value. Both the ethical norm and the GDPR norm strengthen the individual right to define yourself.

For all the ethical values certain norms can be formulated. This is an iterative and ongoing process. The GDPR norms with regard to the data processing in this IoT utilization are already decreed. After the stage of norm postulating the analysis can commence. Procedures and actions are attached to these formulated norms. The crucial question hereby is: are the procedures in the organization and in the development of the IoT utilization sufficient to meet these norms?

To return to the example norms of this case:

- “Within the context of this utilization the patient/customer may self-decide up to what level of detail his/her heart rate data is shared and showed”

- “The data subject has the right to demand erasure of his or her personal data”

To assess the compliance with these norms, certain questions can be put forward. What are the procedures in the organization regarding these norms? In what way does the organization make sure that the personal data of the patient can be erased? How is the data subject empowered and able to self-arrange which data he wants to show?

In this way all the norms can be examined and the level of compliance can be determined. Moreover, the matches between the GDPR norms and ethics can be seen.

4.3 Ethics in practice

This section describes the research part with the interview in practice and the propoundment of the framework. In the first part the setting of the interview and the discussed IoT case will be clarified. Then, the outcomes of the interview will be described.

4.3.1 Case setting

Mobile phones are one of the most ubiquitous Internet of Things devices. The ‘things’ intercommunicate with other phones, with other devices, with radio masts et cetera, by means of a network. In the Netherlands about 86 percent of the people above the age of 12 own a smartphone (Wijkman van Aalst, 2016). Most of the time people actually keep their phones with them, 24 hours a day. By knowing this, it is clear that such devices generate a lot of useful information. The investigated case consists out of a large telecom provider, Vodafone, and a company which specializes in mobility cases by using (Big) Data. The point of view is from Vodafone.

Vodafone has as of January 2017 more than 5 million mobile telephone connections in the Netherlands (VodafoneZiggo, 2017). This is about one third of the total market share in mobile telecom. KPN, T-Mobile and Tele2 are their main competitors in the Netherlands (NU.nl, 2016). Across whole of the Netherlands thousands of radio masts are located which communicate with the mobile phones of the 5 million clients of Vodafone. Vodafone can identify how much mobile phones communicate with the radio masts distributed across the Netherlands. This is done in three ways. Firstly, the text messages are tracked. Secondly, the phone calls are tracked. Lastly, a data session could be seen. If a mobile phone communicates with the Vodafone network via the radio masts, a Cold Detail Record (CDR) will be made. This CDR contains information about the time and the location of that mobile device. Vodafone can divide the Netherlands in about fifteen thousand little cells. In densely populated areas such as cities these cells are smaller, and thus more precise, than in rural areas.

The information of these CDRs can be used, for example, to count how much people are in a certain area and to track the migration of huge crowds. The other party in this case, besides Vodafone, specializes in facilitating and analyzing such figures. Information about crowds can be used by the municipality of Amsterdam in the case of huge manifestations like Kings Day. Questions about the amount of visitors on that day, where they come from and how they move can be answered with this data. Subsequently, the data could be used for safety measures or to control the traffic flows accompanied with large gatherings.

4.3.2 The process

When Vodafone got the proposal to work together with a third party, a team of people from Vodafone got into consideration whether they should do this. Firstly, the applicable legislation got revised, such as the Dutch *Wet Bescherming Persoonsgegevens* and the *Telecommunicatiewet*. Besides this, the ethics side was discovered. The point of view of Vodafone was more aimed at reputation. Questions were asked. *Even if this is allowable in a legislative way, is such a cooperation and sharing of our data desirable for our clients?*

Primarily, matters were looked from a legislative point of view. Due to the subjectivity of ethics, one could say: ethical standings are formed in society. From this arises some ethical consensus. Thus, the ethical standings are wrapped up in the political and legislative decisions. They thought: if we obey the laws, the ethical side is also covered to a large extent. The primary objective of Vodafone is not external data sharing for commercial benefit. So, by sharing these data, some additional laws count. If Vodafone wanted to proceed this venture the CDR data had to be made anonymous or the clients had to be asked for permission to share their data. The last condition would be rather precarious and tedious. Most of the people would not agree with some seemingly random data sharing without explicit benefits for them. Thus, Vodafone chose for the first option: the anonymization of the radio masts data. But hereby they encountered some challenges. In section 2.5.1 it is already noticed that there is a problem with re-identifying anonymized data (Tene & Polonetsky, 2011). Even if data is anonymized, in some cases it could be assigned to specific individuals with the help of other data and extensive analyses. Vodafone encountered this problem also. The mobile phone numbers from the CDRs could be made anonymous but when this data would be combined with other data, a random person X could still be identified.

To solve this issue Vodafone made sure that the data could only be accessed from outside. They built a sort of black box with the data inside; the external party was only able to do counts from that black box. Beside this, the minimum count of mobile devices (and thus people) was fifteen; the data got aggregated. By doing this they could make sure that the anonymity was guaranteed. This number of fifteen devices in one area had to be enough to prevent specific people from being traceable. So the external party was only able to get an outside view of the black box and only counts of fifteen people or more in one area were showed.

By establishing these measures Vodafone made sure the legal side was well-covered. But the ethical questions still remained. For a commercial business like Vodafone the question was especially reputation driven; what do our customers think of this data sharing, albeit anonymous, safe and within the legal restrictions?

Ethics

Internally huge discussions took place up to the level of the board of directors about this to-be cooperation. Although the argumentation was that if Vodafone complied with the laws, apparently they satisfied the ethical norms of society. This is a viewpoint based on the presumption that discussions about ethics in society lead to sufficient legislation which serve as the guidelines of the human conduct. According to the people working on this projects maybe this was not totally true. Between legislation and ethics is still a grey area. Therefore, the consensus was that despite of the fact that the venture was legally permitted, proper communication in the direction of their customers was really important. The upcoming data sharing and cooperation was announced on their website and beside this their customers got the opportunity to opt-out from the anonymous data sharing with the external party. About 25.000 people from the 5 million customers opted-out over the course of the cooperation.

To extra ensure and assess the procedures and course of events, Vodafone approached TNO to carry out a privacy risk assessment. The advice of this nonprofit knowledge organization led to some minor additional adjustments in the procedures.

The above measures were Vodafone's way of Privacy by Design, which is also a legal requirement in the upcoming GDPR. By doing things this way Vodafone believed it made sure that the ethical side was, among other things, covered by the current laws and the grey area by the choice to opt-out.

There was no special framework for these kind of issues. A framework as initiated in this thesis could be helpful in an illustrative way, but ethical values are not gradually discussed within Vodafone.

4.3.3 Analysis of ethical values in the Vodafone case

In the Vodafone case some ethical concerns emerged. The primary objective of Vodafone as a telecom provider is to offer services to customers regarding telecom solutions. With this new venture they blazed a trail. They had to make some well-thought decisions; not only legal, but also ethical concerns rose. What if the data was traceable to a unique individual and this would have been used to do harm? The following section will highlight some ethical values which could have been at stake within this new venture.

The privacy of their customers had to be guaranteed. If the data was not anonymized enough this value could come at stake. Confidentiality is highly linked with the quest for privacy. As earlier mentioned, an exact interpretation of privacy is difficult. It is a very abstract concept. Therefore confidentiality is more appropriate as an addition. Customers had to trust Vodafone in the confidential handling of their personal information. By stating this, another value is introduced; trust. Vodafone had to emanate and prove trust by handling this new venture in an integer way. This trust could be reinforced by proper security measures concerning their data and by a good level of transparency in their communication. With the possibility to opt-out from this data sharing venture Vodafone offered their customers the opportunity to withdraw and to let them decide for themselves. This gets along with the identity value and the possibility of free choice.

By installing measures Vodafone tried to ensure that this new venture could proceed within the frame of what was right or wrong in the context of a commercial company. The data was made anonymous and secured, the external party only could do outside counts, there was transparent communication towards their customers, they offered an opt-out option and a risk assessment by TNO was carried out.

Chapter 5. Summary, Conclusions & Discussion

This chapter leads to the end of this research. In the following sections the research will be summarized, some conclusions will be presented and there is room for discussion.

5.1 Summary & Conclusion

In order to answer the main question which is stated in the first chapter, the sub-questions will be discussed step by step.

What does the concept Internet of Things mean?

Internet of Things is a major trend in Information Technology and is nowadays a constant factor in our everyday lives. Simply said there is the combination of 'Things' and the 'Internet'. The things can be everyday objects like mobile phones, smart televisions and smart thermostats. The internet part represents the networked interconnection of these smart objects. In IoT there can be identified a sensing layer, a network layer and an application layer. These interconnected things or objects form a network of communicating things.

What is (Big) Data?

Firstly, data can be described as descriptions of things, events, activities, and transactions that are "recorded, classified, and stored but are not organized to bring specific meaning" (Maeder et al., 2009, p. 4).

In the last years, Big Data is on its rise. This refers to the notion of very much data. Particularly Big Data is denoted by the five Vs: Volume, Velocity, Variety, Veracity and Value. The volume and size of data increases. The 'production' of data is rapidly increasing. All these data items show an increase in variety in terms of formats and representations. The last two Vs are later added and say something about the truthfulness, the quality and the value of the data.

What ethical issues arise when working with data in Internet of Things applications?

Internet of Things devices process a lot of data. Sensing layers collect data, data gets stored, there is transmission of the data through the intercommunicating objects and the data gets used for all kinds of pursuits. In all these proceedings ethical issues could arise. In chapter 2 a set of ethical values is discussed which could play a role in data processing. There can be identified social values like equality, identity and fairness. Additionally, there are communicative values like privacy, confidentiality, security, transparency and trust. Some of these values overlap, strengthen or even contradict each other.

When developing IoT utilizations it could be helpful to incorporate the ethical deliberations of the particular ethical values, addressed in this thesis.

What kind of GDPR determinations address the issues concerning IoT and data?

From May 2018 onwards new data regulations will commence. This legislation holds some main determinations, noticed in practice. Most importantly, the new data legislation will apply to all EU members. The purpose of the GDPR is especially to strengthen the citizens' rights in the intense playfield of data processing.

Next, the outline of the main determinations will be discussed. Penalties up to 4 percent of the annual turnover are introduced. Consents have to be better understandable and accessible. A breach notification will be mandatory in some circumstances. Privacy by Design is yet a well-known concept, but with the new legislation this will become a legal necessity. Furthermore there are certain rights, namely the Right to Access, the Right to be Forgotten, the Right to Rectification and the Right of Data Portability. These are all determinations which give the 'normal' citizens more rights and ownership over 'their' data. Beyond this, there needs to be a Data Protection Officer (DPO) in some cases. This DPO has to meet some conditions.

How do organizations handle ethics and regulations concerning IoT and data in practice?

In chapter 3 the Vodafone case is discussed. The perspective of this commercial company was in the first place, legal. Their reasoning presumed that the existing laws were formed upon the wide-spread consensus about what was ethically right or wrong.

In the first place they cared about covering the legal requirements, hereafter the grey area of ethics was discussed. They found that proper communication and the possibility to opt-out from the data sharing was the right way to ensure this grey area was covered.

Also, it is expected in Vodafone that everyone has in some way an 'ethical compass' about what is right or wrong. There is no particular ethics board within Vodafone. Using an ethical framework with specified values to handle data processing, as is introduced in this thesis, is not within the normal procedures. Yet, there is a department within Vodafone which focuses on image and reputation. They consider in which projects Vodafone should be involved, for example.

5.1.1 The main research question

> What ethical issues and GDPR norms have to be taken into account when handling data in Internet of Things utilizations?

The discussed sub-questions provide the answering of the main question. The proposed framework which displays the ethical values and the main GDPR norms, can perform as a useful resource to assess the important ethical values and GDPR norms which play a role in the data processing with regard to the development and organization of an IoT utilization.

Also, the matrix which shows the most distinct overlaps between the GDPR norms and the accompanied pursued ethical values, can be helpful in the discussion and layout of a proper conduct of business.

The Vodafone case offers valuable insights about the process of handling ethical issues and legal norms in practical IoT cases. Moreover, the fictional case gained some illustrative insight in the possible functioning of the proposed framework.

5.2 Discussion & Limitations

On account of the enforcement of the General Data Protection Regulation just in May 2018, less academic literature is written with respect to this particular topic. Therefore, limited information is available about the implications and effects of the GDPR. The exact implementation and interpretation has yet to come.

The Vodafone case offers useful insights about the deliberations in a specific IoT case. There are no standard or structured procedures regarding ethics specifically. In the talking's with experts within Business & Decision it was acknowledged that these proceedings could be seen in the whole commercial

world. The point of view in the Vodafone case is from a commercial business. This may be limiting for the bigger picture of how others organizations might handle issues in data processing.
When developing the framework it was important not to impose too complex schemes or models. Also, the level of detail and specific steps could not be too profound. This appeared after consultation with experts in this field. If a framework had to be suggested in practice, matters should not be too intricate in order to keep the discussion open and forward. Ethics are intrinsically subjective and can be addressed in a very abstract way. Besides that, every IoT case is different. A framework had to be applicable to all kinds of cases. In one way this makes the proposed framework very accessible, but the framework can lack profundity when applied in more mature cases. So, for the first discussions about ethics and deliberations about Privacy by Design, for instance, the framework could be useful as a guideline, but in later phases it may lack profundity.

5.3 Recommendations

When the GDPR is fully enforced and the exact consequences become clear, further research can be initiated. The possible pitfalls or positive aspects can be analyzed for example. Also, an extra, and more extensive, study to the practical implications regarding ethics and the GDPR can be executed. Besides this, it may be interesting to look at the cultural differences between countries with regard to the ethical issues in data processing. For instance, people living in Portugal have for sure different conceptions about what is right or wrong in the discussions about the use of personal information. This is yet more interesting because the GDPR determinations will apply to all EU member states.

Further research could also direct more attention to other practical IoT cases. Vodafone is a commercial company in the telecom branch. The ways to handle and process data can differ in the public sector or in other branches which are occupied with IoT utilizations.

The primary focus in, especially commercial, organizations occupied with IoT utilizations and data handling, is not on ethical concerns. This is understandable. But in this digital age of information it could be good to keep in mind that a well-formed approach for the handling and management of data is vital. Harmful events, albeit often unintended, could occur suddenly and can have thorough consequences for the viability of an organization. Although, there may be less attention for ethical concerns, the Vodafone case proved that a grey area was acknowledged. They looked beyond the legal aspects only. But, for these deliberations were no clear procedures. This may give the space and the proof of a need for a more profound framework to handle ethics, regarding data within the context of IoT utilizations. With this in mind, the research in this field could be extended.

Furthermore, the fictional case about the band to monitor your heart rate, shows that having a proper idea of your ethical standpoints, can serve as a foundation for external imposed legislation such as the GDPR. In this way, ethics and legislation can support each other. In an ideal situation, well thought-out considerations about ethical values can yet cover up a substantial part of the legislation. The practical implementation of the GDPR norms, for example, could occur a lot smoother in this manner.

Therefore, it is interesting to try to discover the overlap between the organizations own postulated ethical norms and the GDPR norms. The framework and the matrix, as proposed in this thesis could assist hereby. The matching could help to not only see the GDPR as 'some rules imposed from above', but it could uncover the intrinsic ideas and motives behind the legislation, which are pursued in your organization. When this happens the GDPR becomes a lot more interesting and the involvement of your workforce rises.

References

Anil, J. (2016, September 17). The 5 Vs of Big Data [Blog post]. Retrieved from https://www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Autoriteit Persoonsgegevens. (n.d.). *Wet bescherming persoonsgegevens*. Retrieved 2017, May 3, from https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens

Autoriteit Persoonsgegevens. (n.d.). *Meldplicht datalekken*. Retrieved 2017, May 3, from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, *15*(5), 662-679.

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, *19*(2), 171-209.

Cohen, J. E. (2012). What privacy is for. *Harv. L. Rev.*, *126*, 1904.

Davis, K. (2012). *Ethics of Big Data: Balancing risk and innovation*. "O'Reilly Media, Inc.".

Deloitte. (n.d.), *The General Data Protection Regulation*. Retrieved from https://www2.deloitte.com/nl/nl/pages/risk/articles/the-general-data-protection-regulation.html

Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. *Academy of management Review*, *20*(1), 65-91.

Erikson, E. H. (1968). *Identity: Youth and crisis*. New York: Norton.

EUR-Lex. (2016). Protection of personal data (from 2018). Retrieved from http://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX:32016R0679

European Commision. (n.d.). *Reform of EU data protection rules*. Retrieved 2017, May 8, from http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Gartner. (2017, February 7). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* [Press release]. Retrieved from http://www.gartner.com/newsroom/id/3598917

[GDPR Key Changes]. (n.d.). Retrieved 2017, May 8 from http://www.eugdpr.org/key-changes.html

Gert, B. (1999). Common morality and computing. *Ethics and Information Technology*, *1*(1), 53-60.

Giusto, D. (2010). A. Iera, G. Morabito, l. Atzori (Eds.) The Internet of Things.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, *28*(1), 75-105.

Hildebrandt, M. (2013). Slaves to big data. Or are we?. *Idp. Revista De Internet, Derecho y Política*, *16*(forthcoming).

IBM. (n.d.) *What is big data?*. Retrieved 2017, May 8, from https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

ITU. (2012). New ITU standards define the internet of things and provide the blueprints for its development. Retrieved from http://www.itu.int/ITU-T/newslog/New+ITU+Standards+Define+The+Internet+Of+Things+And+Provide+The+Blueprints+For+Its+Development.aspx

Kobrin, S. J. (2001). Territoriality and the Governance of Cyberspace. *Journal of International Business Studies*, *32*(4), 687-704.

Kounelis, I., Baldini, G., Neisse, R., Steri, G., Tallacchini, M., & Pereira, A. G. (2014). Building trust in the human? internet of things relationship. *IEEE Technology and Society Magazine*, *33*(4), 73-80.

Kwasny, M., Caine, K., Rogers, W. A., & Fisk, A. D. (2008, April). Privacy and technology: folk definitions and perspectives. In *CHI'08 Extended Abstracts on Human Factors in Computing Systems* (pp. 3291-3296). ACM.

Leonard, A. (2013, February 1). How Netflix is turning viewers into puppets [Blog post]. Retrieved from http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets/

Lohr, S. (2013, March 23). Big Data Is Opening Doors, but Maybe Too Many. *The New York Times.* Retrieved from http://www.nytimes.com/

Maeder, M., Hädrich, T., & Peinl, R. (2009). *Enterprise knowledge infrastructures*. Springer Science & Business Media.

McCarthy, R. V., Halawi, L., & Aronson, J. E. (2005). Information technology ethics: a research framework. *Issues in Information Systems*, *6*(2), 64-69.

Nadkarni, P. M. (2011). What Is Metadata?. In *Metadata-driven Software Systems in Biomedicine* (pp. 1-16). Springer London.

National Intelligence Council. (2008). *Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests Out to 2025* (CR 2008-07). Retrieved from https://www.dni.gov/files/documents/2008%20Conference%20Report_Disruptive%20Civil%20Technologies.pdf

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

NU.nl (2016). KPN groeit op mobiele markt ten koste van Vodafone en T-Mobile [News article]. Retrieved From http://www.nu.nl/mobiel/4358903/kpn-groeit-mobiele-markt-koste-van-vodafone-en-t-mobile.html

Paraschakis, D. (2017). Towards an Ethical Recommendation Framework. *978-1-5090-5476-3/17/$31.00 2017 IEEE.*

Parent, W. A. (1983). Privacy, morality, and the law. *Philosophy & Public Affairs*, 269-288.

Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Richards, N. M., & Solove, D. J. (2007). Privacy's other path: recovering the law of confidentiality. *Geo. LJ*, *96*, 123.

Richards, N. M., & King, J. H. (2013). Three paradoxes of big data. *Stan. L. Rev. Online*, *66*, 41.

Richards, N. M., & King, J. H. (2014). Big data ethics.

Tavani, H. T. (2011). *Ethics and technology: Controversies, questions, and strategies for ethical computing*. John Wiley & Sons.

Tene, O., & Polonetsky, J. (2011). Privacy in the age of big data: a time for big decisions. *Stan. L. Rev. Online*, *64*, 63.

VodafoneZiggo. (2017). *Wie we zijn*. Retrieved from https://www.vodafone.nl/over-vodafone-ziggo/wie-we-zijn/index.html

Ward, J. S., & Barker, A. (2013). Undefined by data: a survey of big data definitions. *arXiv preprint arXiv:1309.5821*.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, *26*(1), 23-30.

Wijkman van Aalst, T. (2016, June, 26). 86 procent van de Nederlanders bezit een smartphone [Blog post]. Retrieved from http://www.gsmhelpdesk.nl/nieuws/12857/86-procent-nederlanders-bezit-een-smartphone

Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering*, *57*(3), 221-224.

Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems*, *25*(9), 1101.

Zwitter, A. (2014). Big data ethics. *Big Data & Society*, *1*(2), 2053951714559253.Nadkarni, P. M. (2011).

Appendix 1. Definitions per value

Value	**Definition**
Privacy	“The process of controlling the disclosure of information about an individual, group, or institution, to others” (Westin, as cited in Kwasny et al., 2008, p. 5).
Confidentiality	A kind of privacy founded by trust and reliance on promises in interactions (Richards & Solove, 2007).
Security	Freedom from danger or risk. The protection of information, data or other IT assets from danger in information technology.
Transparency	A certain state of openness, the capability of seeing through.
Trust	“The level of confidence with which an entity can ensure to another entity or entities specific services tailored for given contexts and quality (fitness for purpose and reliability)” (Kounelis et al., 2014, p. 74).
Equality	The state of being equal.
Identity	“The identity of a thing, including a person, is comprised of those properties or qualities which make it that thing” (Richard & King, 2014, p. 422). The state of being an individual or object.
Fairness	The state of (something) being fair.