Privacy : constitutional rights and the internet of things
a technical, legal and ethical perspective

Baar, R.Y.

Award date:
2013

Eindhoven, September 2013

Privacy: Constitutional Rights and the Internet of Things

A technical, legal and ethical perspective

by Rhesa Baar

identity number 0613313

in partial fulfilment of the requirements for the degree of

Master of Science
in Innovation Sciences

Supervisors:
prof.mr.dr. J.M. (Jan) Smits
dr. A. (Andreas) Spahn

Privacy: Constitutional Rights and the Internet of Things

A technical, legal, and ethical perspective

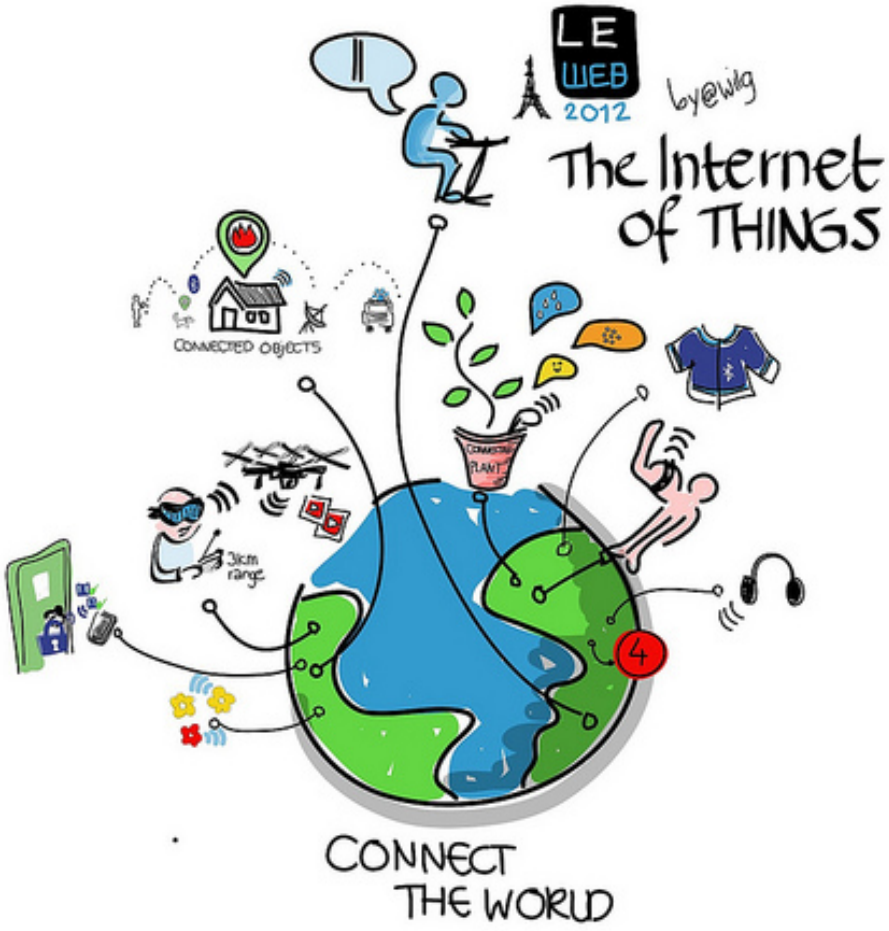


Figure 1: The vision of the IoT. **Picture made by Esther Gons, printed with permission source: (Gons, 2012)**

Keywords: internet of things, RFID, sensors, privacy, constitutional rights, data flow, ethics, law, data protection

Preface and Acknowledgements

During my bachelor, I have gained an interest in the prevention of identity theft and conducted my bachelor thesis about this. I looked at the impact of security measurements that were taken to prevent identity theft and concluded that these measurements make the group of people who can commit identity theft smaller; however, those who pass the security barriers become more difficult to catch. Therefore, we feel unrightfully safe by all these security measurements like biometric passports. I started to realize that much information is collected without a real necessity. Since then my interest in privacy grew and I was already sure from the beginning of my master that I wanted to do research in that area. The challenge of privacy is to find a formal ground on which privacy threats can be objectively analyzed. This is not easy since privacy is very subjective in its nature. I have always been very interested in new information technologies and their possibilities. This has led me to do research on privacy in a new technological area, namely privacy in the internet of things. Before this project I hardly knew anything about privacy rights or the internet of things, so looking back I can say that I learned much during this last stadium of my study. Since the hard work is done, it is finally my time to say thanks after seven years of study.

I have been very lucky that I found a professor with whom I could share my compassion for privacy, Jan Smits. He first became my mentor and later my first supervisor. We had many interesting discussions and shared many thoughts about privacy. Privacy is a huge topic that has many elements but despite our broad discussions, he has pushed me to focus, to save me from drowning in a large topic. This was not always easy since I can be so enthusiastic about something that it is hard to redirect me. In the end, I think I can be proud of the result. I really want to thank Jan for guiding me throughout the master process and enabling me to do research in a field where I am really interested in. He has truly helped me in becoming a more independent person, were I am especially thankful for. I would also like to thank my second supervisor Andreas Spahn. He has really helped me with his new perspective, his structure, his thorough feedback and his enthusiasm.

I would also like to thank Edward Snowden for showing the world the existence of the program called PRISM, since this news came out people have been more interested in my research. He really sacrificed himself in favor for a more privacy friendly world. It fuelled the privacy discussion again and I truly hope his sacrifice will not be in vain.

Of course, I would like to thank my friends, who have been there to give pleasant distractions from my work and who were kind enough to listen to my theories on privacy, but especially for making my seven years of study such an awesome time. Study Association Intermate has been my second home during my studies. I will really miss all the nice activities and random conversations on the couch. I would like to thank Tanja for being my office roommate, since social pressure and coffee are always good motivators. I would like to thank Bas for his love and support during my master thesis. Last, but not least I would like to thank my family, my parents in particular, who have been there for me during my entire studies. Without their support, this thesis would never have been written. Mom and Dad, I would like to dedicate this thesis to you.

Rhesa Baar, Eindhoven 2013

Executive Summary

Introduction
Each day more things are connected to internet, this is a concept coined the Internet of Things (IoT). Regular static things from daily life are being enhanced with Radio Frequency Identity (RFID) and sensor technologies, thereby becoming dynamic objects since they become able to sense the world around them and react on that. An example of this is the smart fridge that knows exactly what products are in there since all products are embedded with an RFID tag. The fridge would even be able to automatically re-order the items that are almost out of stock. All these things generate lots of new data and this data could contain personal related information. Therefore, the IoT might be threatening to violate our privacy, and the main objective of this research is to assess whether this is the case. Privacy is assessed from the constitutional rights perspective.

The main research question:
Are the constitutional privacy rights threatened to be violated by the internet of things?

To answer this question a technical, legal and ethical perspective is taken. This research has mainly been carried out by analyzing, interpreting and reflecting on documents. This research is best described as an explorative normative analysis.

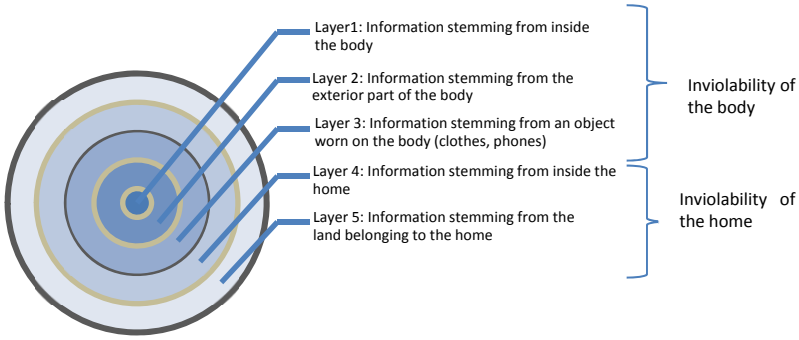
Basic concepts of the IoT
The IoT consist out of two main technology groups, namely RFID and sensor technologies. RFID is mainly used for the identification of objects; this can be done unobtrusively without having the object in sight. Sensor technologies are used to assess a status of the surrounding, for instance the temperature of the room or the heartbeat of patient. Several communication technologies for the sensors exist. Each has its own feature trade-off, in topology, energy usage, data range and data rate. The real vision of the IoT would come true if all things are accessible directly through the IoT. This is not feasible with IPv4, since there are not enough unique numbers, IPv6 does have enough numbers however. The IoT has many benefits, for example it can make lives more efficient and sustainable, since it has the capability of automatically reacting to certain events.

Privacy Rights
Privacy is a very subjective meaning. Depending on the research discipline the meaning of privacy may vary. Law can therefore serve as an objective basis, since it applies to all of us. It is chosen to assess privacy from the constitutional rights perspective. In the Dutch constitution, four privacy related rights can be found. The first one is article 10, the general right to privacy, which also protects personal data in databases. The second one is article 11, the inviolability of the body, which protects bodily integrity. The third one is article 12, the inviolability of the home. The last one is article 13, the privacy of communications. These articles where passed at a time when information technologies did not exist yet, therefore the articles are reinterpreted in this research, to fit the digital age. It is argued that the rights to inviolability of the home and body should not only be protected against physical interference, but that they should also be protected against informational interference. To determine whether a violation of a privacy right has been taken place, court ruling often makes use of the term “reasonable expectation of privacy”. This basically means that no

privacy claims can be made if privacy could not have been expected in that instance. One cannot expect not to be overheard telling a personal story in a crowded train for instance. Privacy legislation varies around the world which makes the protection of privacy rights complicated, since the flow of information in the IoT is not limited by a physical border.

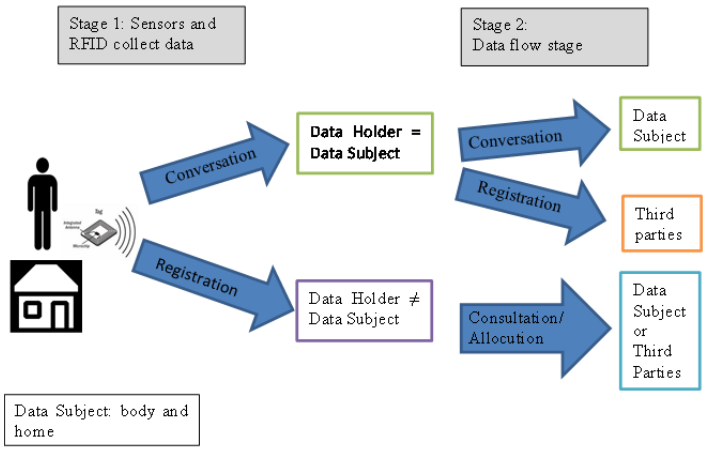
The internet of things compared to the internet

Much research has been carried out on privacy on the internet. In this chapter it is concluded that the IoT will amplify the existing threats of violations of the general right to privacy and the right of privacy of communications. There are reasons to suspect however that the IoT will threaten to violate the right of inviolability of the body and the right to inviolability of the home in new ways that were not possible before the IoT. Therefore it is chosen to zoom into these two rights. A privacy model taking the human body as a starting point is presented, the model is given below.



Data flow model

Data transmitted through information technology consists of two elements, traffic data and information content. Traffic data is data needed to deliver the message, like the address on an envelope. Two models of data flows are discussed. These models are combined into one model. The combined model can especially be used to assess violations of inviolability of either the home or the body. The model, given below, separates two stages namely the stage of information collection, which is done by sensors and RFID technologies, and the stage of data flow where information is communicated further.



Threats of violations

Several threats of violations of inviolability of the home and the body can be identified. In case the information collection was done by the data subject itself, for instance on a mobile device in the private network in the home, then there is a chance that there is someone eavesdropping on the communication, thereby revealing a lot of personal information. Even if the information content is encrypted, the traffic data can still reveal private information. More threats can be identified in case information is registered by an external data holder. The threat of violations by the IoT services is that information collection can be done directly at the data source and that this can happen unobtrusively. RFID tags can be so small that they are also unobtrusively embedded in our things; therefore people do not realize that information about them might be collected. This information can reveal information about the body or the home that could previously only have been collected by a body or home search. If the real vision of the IoT comes true and each thing is accessible through the internet then privacy violations could be committed from anytime anywhere in the world. Companies and governments are using algorithms to derive relevant information from all the information availability. Information stemming from the body and the home could add a new group of very relevant information that could make these algorithms even more accurate. These algorithms could derive information where you have never given your consent for. All this information availability could also lead to actual physical interference with the body or the home.

Ethical reflection

It has become clear that IoT technologies are capable of violation constitutional rights. If things are left the way they are there will be a lot of regulation issues since the law and technical possibilities do not comply with each other. There are two extreme ways of overcoming this problem. The first one is to adapt our values of privacy in favor of the new technologies. If one would argue from the utilitarian perspective than it could indeed be ethical justified that privacy rights are violated since the IoT can be very beneficial for other values like economic growth, sustainability, healthcare and national security. Privacy can be seen as a purely intrinsic value but also as an instrumental value for other values like freedom and autonomy. Therefore, the other option is to adapt the technologies to the existing law, so that the technology is value sensitive designed. There are some solutions to some threats available but they will still need improvements of their effectiveness and not all threats of violations can be solved without giving up some of the benefits of the IoT. Contextual integrity is very important and since the IoT is capable of sensing its environment, this capability could be used to establish contextual integrity with the technology. A third middle option gives the control of what could be disclosed to each person themselves. To achieve this, some technical changes are needed and there should still be a legal basis to make sure that control can actually be giving.

Conclusion

Although the IoT has many benefits, it is also threatening our constitutional privacy rights in multiple ways. Each threat by itself might not be perceived as severe. But if all the risks are taking together than it can be concluded that the IoT is a big threat to our privacy rights especially towards the rights of inviolability of the body and the home, since these rights are threatened in new ways that were not possible before. It is recommended that legislation is updated to the new technical possibilities brought by the IoT and that engineers will

develop new privacy enhancing technologies by taking privacy into the design. If things are just left the way they are, then we are at risk of creating big brother or even the brave new world with the IoT.

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Explanation
AI	Ambient Intelligence
CBP	College Bescherming Persoonsgegevens (Data Protection Authority)
CBS	Centraal Bureau voor de Statistiek (Central statistics bureau)
DC	Dutch Constitution
ECHR	European Convention on Human Rights
ED	Event Detection
EPC	Electronic Product Code
EU	European Union
FTC	Federal Trade Commission
ID	Identification
IECR	Internet of Things European Research Cluster
IoT	The internet of things
ITU	Internet Telecommunications Unit
MAC	Media Access Control
NFC	Near Field Communication
ONS	Object Naming Service
P2P	Peer to Peer
PIA	Privacy Impact Assessment
RFID	Radio Frequency Identification
SPE	Spatial Process Estimation
UHF	Ultra High Frequency
WBP	Wet Bescherming Persoonsgegevens (Data Protection Act)
WSN	Wireless Sensor Networks
WSAN	Wireless Sensor Actuator Networks

1 Introduction

It is only about 30 years ago that computers made their first entrance into the homes in western society. Some years later, a few households signed up for a dial-up internet connection. Nowadays it is very hard to imagine what the world would look like without the internet. Not just computers connect us to the web anymore. Anno 2013, many of us have smartphones, which enable us to access the internet wherever we go. Statistics from the CBS show that in 2011, about 93% of Dutch society had an internet connection and about 43% used a mobile internet connection (CBS, 2011). The internet is very useful since it allows us to find information from all over the world. For instance, if you have to visit a new place, you can use the navigation on your smartphone to find your way. You could even virtually walk the entire route beforehand with Google maps street view; see for instance Figure 2 where a part of the TU/e campus is shown as seen on Google street view.

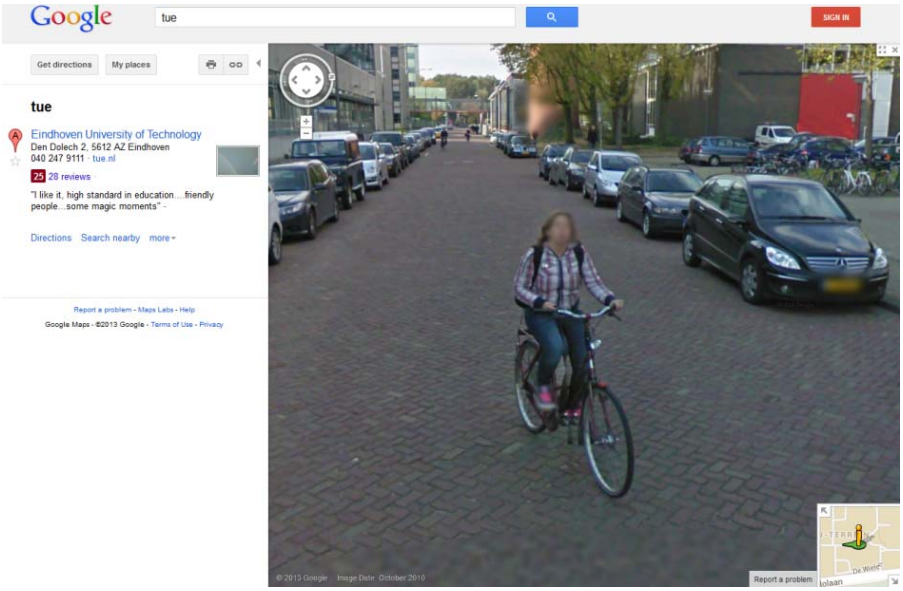


Figure 2: Rhesa seen on Google Maps Street View on the TU/e campus

The internet also makes it possible to communicate with others and to stay in touch with friends and relatives from all over the world, without much effort. The amount of services on the internet grows fast; more and more things are done online. Journalist Paul Miller disconnected, as an experiment, from the internet for one year. He felt left out and in the end of his project he even felt very isolated (Ringelestijn, 2013). From his experiences, it can be learned that the internet is more embedded in our (social) lives than we might feel or even dare to admit.

Nowadays internet is mostly used as a source of information and as a mean to communicate with other people. But what if not only our computer, laptops and smartphones but also our daily physical objects are connected to the web? In 1991 Weiser, back then a scientist at Xerox Parc, envisioned a world in which all objects are unobtrusively embedded with some sort of computer that contains information and which could communicate with the rest of the world. Weiser called this phenomenon *ubiquitous computing* (Weiser, 1991). Currently the internet really is connecting more and more objects, or things. Sensors and tags attached to these things share data about these things automatically through the internet; this concept is now coined *The Internet of Things* (IoT). This term, IoT, was first introduced

by Ashton in 1999 (Ashton, 2009). The IoT can be seen as a new internet infrastructure that can make other things possible. For instance, it can help businesses to better track and trace their products. Another example that can be realized with the IoT is *Ambient Intelligence* (AI). AI is the concept where people are surrounded by smart objects that react and respond to the presence of individuals (Hoepman, 2011). A basic example of this is that the lights turn automatically on when you enter a room.

The IoT can support human lives to make them more efficient and more sustainable. If, for instance, your refrigerator would be able to know what products are in there, it can tell you what you can cook with those ingredients or which products are overdue or missing. In addition, if you connect your refrigerator with albert.nl (the online web shop of the grocery store Albert Heijn) it would even be able to reorder certain products for you if you run out of them. In addition, if you leave the home to go to work but you forgot to turn off the heater, the heater can do this automatically for you since it got the signal from the GPS in your car that you are at least 5 km away from home. For some people this might still sound like science fiction, but the move towards the IoT is already happening. Samsung for instance showed their smart fridges on the CES 2013, the consumer electronics show, which will be sold at the end of this year (Smith, 2013).

The European Union is of the opinion that the possibilities of the IoT are capable of helping to solve prominent societal problems like the rising costs of healthcare in our ageing society. It could help to make better work environments and could give Europe a competitiveness boost, thereby stimulating economic growth. The EU sees the IoT not as merely a new stage of the internet but even as a paradigm shift. To help develop the IoT the EU has adopted an action plan for the IoT. In this action plan, 14 critical areas have been identified where attention needs to go to in order to make the IoT successful (Commission of the European Communities, 2009). One of these areas is privacy in relation to the IoT, because privacy is an important element for the acceptance of the IoT by its users. This research lies in that area; it is about the IoT in relation to privacy rights.

Although the IoT can help us to live our lives and run our businesses more efficiently, it might also be violating our privacy rights since it has the potential of processing lots of personal related information, like the information about the contents of your refrigerator. The availability of this information can be very interesting for different parties. For instance, the government can be interested in this information in the context of criminal investigations and companies for advertisement reasons. Sometimes you could also just want some privacy from the people you have personal relationships with. The IoT is still in its developing stage, so solutions for privacy issues could still be taken into the design, this is also called value sensitive design. However, the privacy issues should first be identified and analyzed. Also for legislators, it is important to be aware of the threats so they could already anticipate on the new developments. It is therefore very useful to know if and how the IoT is posing threats towards privacy. An ethical reflection is needed to assess whether these threats might be ethical justified.

Privacy is a word that is used in many disciplines, like psychological, technical, social, ethical and legal sciences. In this research it is chosen to approach privacy from a legal perspective, constitutional rights in particular, since it can be assumed that law is a reflection of our

societal values, and it can serve as an objective basis which is needed to assess privacy threats. This does not mean however that other elements or perspectives of privacy are not important.

1.1 Research objective

The development of new internet technologies and services goes fast. It is difficult for legislators to keep up with this speed of change. Engelfriet wrote a book about law, Dutch law in particular, on the internet and he stretched that laws that are applicable offline should also be applicable online. Nevertheless, sometimes it is difficult to make this translation since some possibilities with new technologies are hardly comparable with the offline world (Engelfriet, 2013). The IoT is a new infrastructure with new possibilities but nevertheless the existing laws and rights should still apply. Constitutional rights, as well as universal human rights should, in principle, also be protected equally under new technology related circumstances despite its new possibilities. In the Dutch constitution, four privacy rights can be found. While reading many papers and books about privacy, as a preparation for this research, there were reasons to suspect that the IoT might be threatening to violate our constitutional rights. One of the problems that cause this is that engineers design the technology without taking privacy consequences into consideration and that legislators do not know what the capabilities of the technology are.

The main objective of this research is to assess whether the IoT might be threatening to violate constitutional rights by combining technical, legal and ethical perspectives. A clear overview of the tensions between law and technical possibilities can provide opportunities for improvements, both for law and technology. To deal with the tension between technology and law an ethical perspective will be taken. In the ethical part it will be discussed whether technology should be designed in line with the values that are present in law or if it is a possibility that we change our values in favor of the new technology.

1.2 Research questions

The main research question of this research follows directly from the research objective and is:

Are the constitutional privacy rights threatened to be violated by the internet of things?

In order to answer this question the following sub questions need to be answered:

1. What are the basic concepts and technologies of the internet of things?
2. What are the constitutional privacy rights and how should these be interpreted?
3. What makes the threats posed by the IoT different from the threats already posed by the internet?
4. How does data flow from one person to another person?

After these four questions are answered the main research question can be answered. After the main research question is answered an ethical reflection will take place in which two more questions will be answered.

5. From an ethical perspective; could the deprivation of privacy rights be ethical justified?
6. Are there solutions to reduce the threats towards constitutional privacy rights?

1.3 Relevance of the research

Research should be justified by its relevance. The scientific and societal relevance are described below.

1.3.1 Scientific relevance

This research is a combination of technical, legal and philosophical perspectives. This research is done as a master thesis for the study of Innovation Sciences. One of the most important elements of Innovation Sciences is to approach new technologies from a socio-technical perspective, thereby integrating different disciplines. This has been done in this research.

There is literature available about the IoT and there is a rich body of literature available about privacy. Only some literature has been written about privacy in the IoT however, most of which were written from just one perspective or just focusing on one technology. For instance Weber & Weber have written about privacy in the internet of things but they have focused mainly on RFID technology and on privacy of businesses and did not take consumer privacy into consideration (Weber & Weber, 2010) (Weber R. H., 2009). New insights might be found if privacy issues in the IoT are assessed from multiple perspectives. This research will aid in creating an overview of the technologies in the IoT, which could be used in other research. Furthermore, this research will translate constitutional rights into the informational age, which can be of aid to other privacy researchers. This research will also present new models that will give insight in how far the internet of things might threaten our constitutional rights. The models presented in this research can be used in future research on privacy.

1.3.2 Societal relevance

This research is highly societal relevant. Constitutional and human rights are applicable to all of us. During this research, privacy has been a hot topic in the news especially when Edward Snowden told the world about the highly privacy intrusive program used by the US government called PRISM. From all these news articles, it can be concluded that privacy is very important and valued by many people. The IoT is still in its developing stage but is already seen as very promising, the IoT is therefore being implemented at a fast pace. The effects of new technologies cannot be known beforehand, but the IoT has the potential to change our way of living just as the internet already did. If internet is embedded in all our daily objects we cannot choose not to participate. We will probably all become users of the IoT and if this research could help by creating awareness, even if it is just a tiny bit, that this new technology infrastructure could limit our privacy, privacy could still be taken into account in its design.

1.4 Methodology

This research can best be described as an explorative normative analysis. Explorative research is very common with new technologies because you cannot know beforehand what the relevant technical, social and normative aspects are. This research has been carried out by analyzing, interpreting and reflecting on documents, this has been an iterative process. These documents include scientific literature but also legislative documents and newspapers. During this research, unstructured interviews have been held with technology experts from the Universities of Nijmegen and law experts from the University of Tilburg to get a better understanding of the matters discussed. Consultations with others, both

university and non-university related, have helped to gain more insights about different thoughts on privacy. This research started out with a descriptive approach of constitutional privacy rights and IoT technologies, which is necessary to gain insights in the current situation. This was done by giving structure to the fragmented information availability. After this stadium, a normative approach was taken. Besides normative elements this research also has design element since models are designed that can be used to conceptually analyze privacy threats.

1.5 Research structure

In this section a short explanation of each chapter will be giving. The chapters are closely related to the research questions.

Chapter 2, the basic concepts of the IoT, will describe the main technologies of the IoT and their features.

Chapter 3, privacy and constitutional rights, will approach privacy from the constitutional rights perspective and the protection of these rights.

Chapter 4, the internet of things compared to the internet, explains why privacy threats in the IoT are different from “regular” internet.

Chapter 5, data flow, will compare two theories about data flows and will combine these two theories into a new model.

Chapter 6, threats of violations of constitutional privacy rights posed by the internet of things, will give an answer to the main question of this research.

Chapter 7, ethical reflection, will give an ethical reflection on the findings of the previous chapter. It will also give some possible solutions for the threats of violations of constitutional privacy rights posed by the internet of things.

Chapter 8, conclusions and discussions, will summarize the main findings and some discussion points in relation with this research are raised.

2 The basic concepts and technologies of the internet of things

This chapter will explain the basic concepts and technologies of the Internet of Things (IoT). The IoT does not consist out of one technology or one system; the IoT can be seen as a vision in which many technologies and applications may find their place. The vision of the IoT is about connecting objects from our daily life with the internet, by enhancing them with communication and/or computing techniques (Chaouchi, 2010). This means that things that are not connected at the current time will be connected in the future through the IoT. The International Telecommunication Unit (ITU) described it as the move towards an *"any time, any place, and any thing connection"*, which can be seen in Figure 3. Some researchers expect that by 2025 already 1 trillion devices will be connected to the internet (Karimi & Atkinson, 2012).

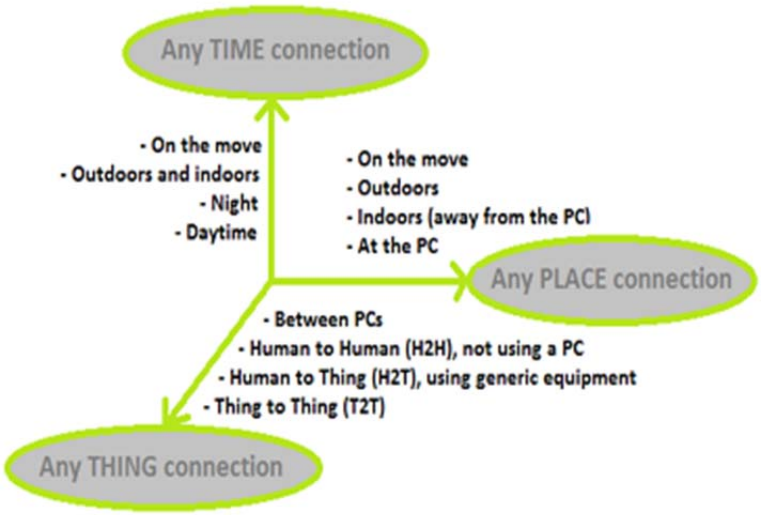


Figure 3: Anytime, anyplace, anything connection. Source (ITU, 2005)

The core of the IoT is to make our world intelligent by changing the static objects into dynamic objects, thereby creating new possibilities for products and services. To make this happen each object should be unobtrusively identified and should be able to know the physical status of its environment (ITU, 2005). Two major technology groups can be recognized that enable this change from static towards dynamic objects. These are *Radio Frequency Identification* (RFID) technologies and sensor technologies. Both are using wireless communications since most things are moveable and therefore it is not convenient to connect them by wire. Other advances in technology like nanotechnology, which enables smaller things to be connected, are also important for the IoT (Chaouchi, 2010). For this research, the focus will be on the two largest technology groups, both of them will be explained below.

2.1 Radio Frequency Identification (RFID)

As can already be deduced from the term, RFID is a technology meant for identification, objects in particular. The basis of RFID is a tag that contains a unique number that can be "scanned" with the use of radio waves. It can be compared to the traditional barcodes that have to be physically scanned. The big advantage of RFID is that it becomes possible to identify objects from a distance without having the objects in sight. Another advantage is

that more unique IDs can be assigned (Want, 2006). Therefore, with the use of RFID a complete shopping cart can be instantly scanned at the grocery store without the need to first unload the cart and then scan each item separately. This can save the consumer some time, and the grocery stores some employees.

An RFID-system consists out of three components, namely the RFID tag, an RFID reader and RFID middleware (Chaouchi, 2010). The purpose of an RFID reader is to obtain the identification data stored in the tags. It has one or more antennas to send and receive radio waves, thereby communicating with the tag. The RFID tag is attached to the object it is identifying. With the use of nanotechnology the tags are becoming smaller and smaller. The most commonly used RFID tag is just 1 by 1 by 0.18 mm. Even smaller tags are being developed, researchers have developed tags with the size of only 0.05 by 0.05 by 0.005 mm, this is also called RFID powder (Hornyak, 2008). Very small objects and even single particles can be tagged with this powder.

Each tag consists of an antenna and an integrated circuit, where the ID data can be stored. In Figure 4 an overview of a tag can be seen. A tag can be *active, semi-passive* or *passive*. A passive tag does not have a power supply; the tag uses the energy from a received radio wave to send a wave back to the reader. An active tag does have a battery, and is therefore capable of sending a signal on its own and is therefore better suitable for tracking purposes (Gubb, Buyya, Marusic, & Palaniswam, 2012). An active tag can also communicate with other tags or sensors because of this capability (Chaouchi, 2010). A semi-passive tag has a battery but only uses this power for its internal circuit. Batteries cause the tag to be more expensive and larger, therefore passive tags are most commonly use. By example, The *OV-Chipkaart,* a payment card used in Dutch public transport, is embedded with a passive RFID tag. A passive tag can be purchased from 5 US dollar cents and upwards whereas an active tag comes with the price of 25 US dollars and upwards, the actual price depends on the quantity bought (RFID journal, 2013). RFID tags can be classified according to its capabilities in six classes as can be seen in Table 1. Each class inherits the capabilities of the previous class.

Tag class	Passive/active	Capabilities
Class 0	Passive	This is a read only tag. It is the most basic tag with is used mostly to store an ID-number.
Class 1		This is a read/write once tag. Once data has put on the tag, it cannot be changed anymore.
Class 2		This is a read/write tag. The data of this tag can be changed. This tag is also capable of including basic cryptography.
Class 3	Semi-passive	Same capabilities of class 2 and can include sensor capabilities in addition due to the extra power. The power can also be used to increase the range.
Class 4	Active	This tag can also communicate with other active tags
Class 5		This tag can communicate with all other tags, hence it is a bit a reader itself.

Table 1: Tag classes source: (Chaouchi, 2010, p. 133)

As can be seen, tags from class 2 and up can be encrypted; therefore, in principle not everyone with a reader can read the content of those tags. However, it has been shown that even encrypted tags can be decrypted. For instance some researchers have cracked the encryption on the RFID tag used in the OV-Chipkaart (Garcia, et al., 2008).

A very important element of RFID readers and tags is the frequency used by the antennas for the radio waves. In principle, the higher the frequency, the higher the read range and the data transfer rate will be. A read range is the maximum distance at which a reader can still exchange data with a tag. The data transfer rate, is the speed with which data is send between tag and reader. RFID tags can therefore also be categorized according to their frequencies in four groups, but RFID is still in development and therefore new groups are found in some literature. Nevertheless, the four groups of RFID that are currently used the most are listed in Table 2.

Category	Frequency band	Read Range	Remarks
Low frequency (LF)	124 kHz - 135 kHz	Up to 0.5 meter	Slowest data rate but works well around metal and water
High Frequency (HF)	13,56 MHz	Up to 1 meter	Low costs
Ultra High Frequency (UHF)	860 MHz- 960 MHz	Up to 3 meters	Does not work well around water and metal
Microwave Frequency	2,45 GHz or 5,8 GHz	Up to 1 meter	Fastest data rate, but has a lower range than UHF

Table 2: RFID frequency groups deducted from: (Juels, 2005) (Scansource, 2013) (Chaouchi, 2010)

As you can see, the read range is in principle not that high, but the power unit that is available on the active RFID tags can also be used to power an extra antenna. This can add an extra read range of about 300 meters (Ni, Liu, Lau, & Patil, 2004).

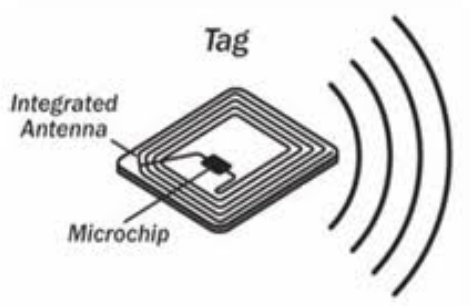


Figure 4: RFID tag Source: (barcodesinc, 2013)

The last part of the RFID system is the RFID middleware. The middleware is the part of the system that adds a meaning to the data captured by the RFID reader. The middleware makes sure that the data can be processed further. It can link the data from the reader with data from a database. For instance, when you scan your OV-Chipkaart at a card reader the middleware makes sure that the card reader replies with information about whether you are checking in or out and the status of your account balance. This information was not stored in the card reader itself, but instead the middleware made sure that it linked your number to the database thereby getting the information applicable for you on the screen of

the card reader. A graphical overview of a whole RFID system, with a passive RFID tag can be seen in Figure 5.

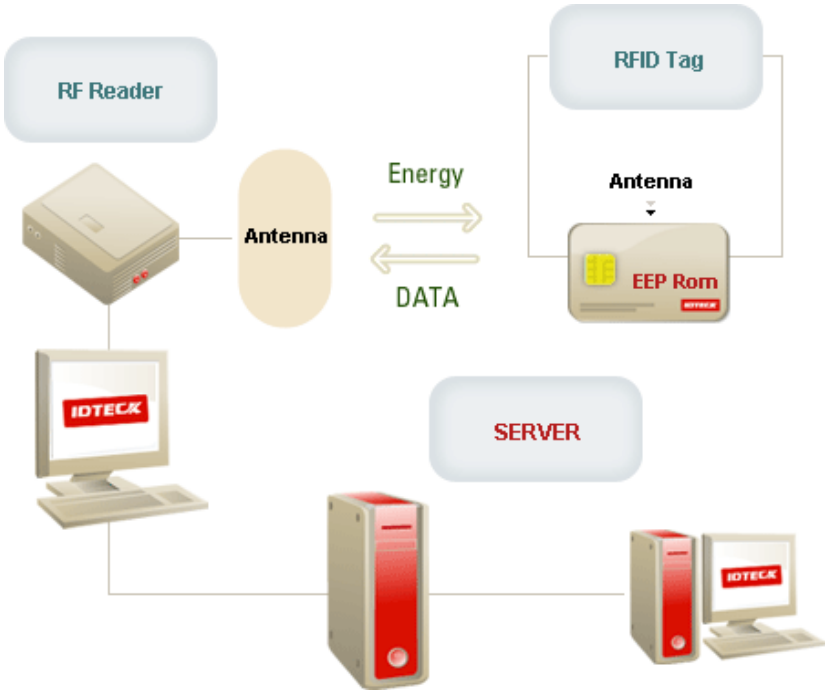


Figure 5: RFID system with a passive RFID tag source: (IDTECK, 2009)

2.1.1 Electronic Product Code

RFID systems often make use of the *Electronic Product Code* (EPC) system of EPCglobal. An EPC code can be seen as a classification system for ID-numbers stored in the tags. The code contains a certain number of bits (these can either be 0 or 1) depending on the type of EPC code. The basic of an EPC code is that the first few bits are a header, which states which version number of EPC is used. The next few bits state the domain manager; this is for instance a certain retailer "owning" that domain number. Then there is the object class that specifies the type of object. The last bits are for the serial number, which gives each product of the same object class a unique number (Brock, 2002) (Engels, 2003). In Table 3 an example of a structure of a code is giving with the corresponding possible unique numbers. As can be seen there are many unique numbers that can be allocated. Therefore, even if there are loads of copies of the same item, each copy could still get its own unique number. To make sure that each company uses a different domain number there is a system called *Object Naming Service* (ONS) that works very similar to the DNS system, which points website addresses, URLs, to the corresponding IP-addresses.

	Number of bits	Possible unique numbers
Header	8	(header denotes which type EPC is used)
Domain Manager	128	2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456
Object Class	56	2^{56}= 72.057.594.037.927.936
Serial Number	64	2^{64}= 18.446.744.073.709.551.616

Table 3: Example of a 256-EPC Type 3 code numbers calculated from source (Engels, 2003)

The newer code standards of EPCglobal, currently the latest version is the one of May 2013, also have some bits for user memory data and are not only able to identify the object but also the part of the object, but the basic idea remains the same. EPC codes are also compatible with other global identifiers like the global document type identifier and the GS1 barcodes (EPCglobal, 2013). The GS1 is an international non-profit association that is working on standardization of the supply chain, the GS1 barcodes are such standardization. Almost all products in the supermarket have a GS1 barcode. A quick test proved that if you type in the barcode of a random product, Google finds the corresponding product. There are also apps available that let you scan the product with the camera of your phone and it will find the product for you. Since the end of last year the clothing industry, including the smaller stores, also implemented GS1 codes (GS1 Nederland, 2012).

2.2 Sensor technologies

The other major group of technologies in the IoT is sensor technologies. Where RFID tags are mainly used for identification of the object it is attached to, sensors are meant to also communicate something about the state of the object or the surrounding of the object or change the environment by activating actuators. A (semi-)active RFID tag can be extended with a sensor, and can therefore be seen as a low-end sensor. A basic example of a sensor is a temperature sensor, which communicates the temperature of the room. In the IoT, these sensors can be connected through a network to be able to communicate wireless with each other and the rest of the world, this is also called Wireless Sensor Networks (WSN). The use of sensors has become more popular since they have become both smaller and cheaper through the use of micro-electrical mechanical systems. A sensor, also called a sensor node, consists out of one or more sensors, a processor, a memory, a power supply, and a radio to communicate. If a sensor also contains an actuator, which can change the environment, then it is also called a smart sensor (Yick, Mukherjee, & Ghosal, 2008). Sometimes a sensor node is also embedded with GPS to include location information (Matin & Islam, 2012). A sensor node creates data and sends this data to a sink, which can be described as a monitor. This sink can use the data itself to monitor or to activate actuators or the data can be sent through a gateway forward to another network, like the internet, as can be seen in Figure 6. If you look at the type of data the sensor is collecting, then the type of sensors can be divided in two categories, namely *event detection* (ED) and *spatial process estimation* (SPE) (Buratti, Conti, Dardari, & Verdone, 2009). ED is the easiest process since the sensors only have to compare their value with a certain threshold and once that threshold is reached, they sent out a signal. An example of this is a smoke detector that beeps when there is a certain level of smoke. In an ED WSN, multiple sensors can for example measure the presence of fire in a forest. If multiple sensors send a fire signal to the sink, the sink can then

communicate with the gateway that alarms the fire station. SPE are sensors that have the purpose of estimating the exact value of a certain phenomenon, like the humidity of a room.

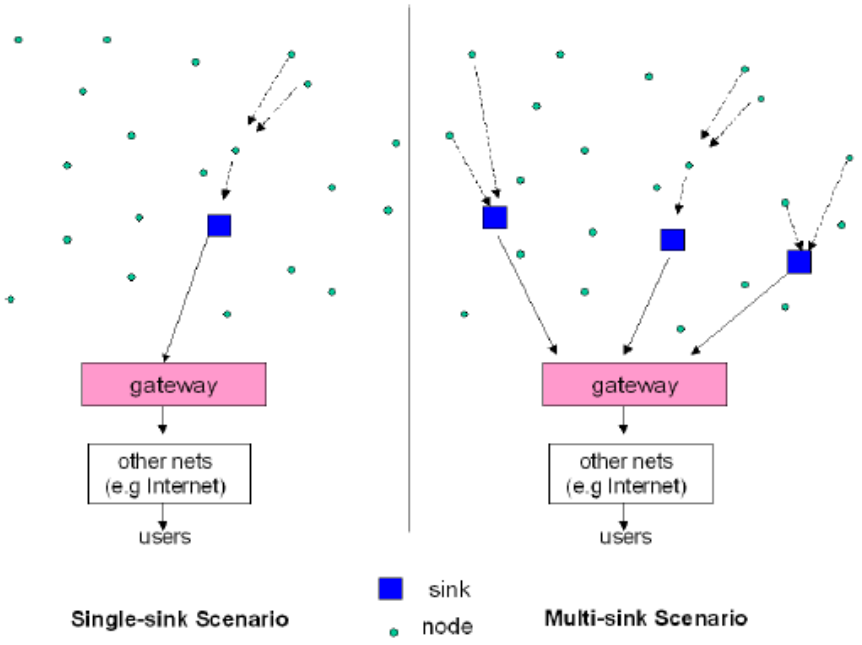


Figure 6: From sensor data to the internet through sinks and gateways Source: (Buratti, Conti, Dardari, & Verdone, 2009)

2.2.1 Communication technologies

There are many elements to a sensor technology, like how the sensing is processed or internally stored in the sensor node. The most important element for this research is how the sensor data is communicated between the sensor nodes and the sink. There does not exist a dominant technology for this communication (yet). Each communication technology has different feature trade-offs. These features are topology, power, data rate, range and costs. Each of these features will be explained below.

1. Topology: There are different ways of how nodes communicate with each other and the sink. The different types that are relevant for WSN are:
    - Star: The sink can sent and receive information from the different nodes, but there is no communication between the nodes (Matin & Islam, 2012). (See Figure 7)
    - Mesh: The nodes can also communicate with each other; this can also be done by multiple hops. Since all nodes are able to communicate with each other, the system is not really energy efficient (Matin & Islam, 2012). (See Figure 8)
    - Hybrid Star-Mesh: In this network topology, not all nodes are able to forward messages; this is left to the high-energy nodes (Matin & Islam, 2012). (See Figure 9)
    - P2P (Peer-to-Peer): Two nodes exchange information when they are brought very close to each other (Ok, Coskun, Aydin, & Ozdenizci, 2010).
    - Scatternet: This can be seen as multiple star networks that are connected with each other (Zacharisas & Newe, 2010).
    - Tree: This is a hierarchy based routing system.

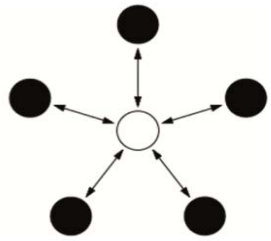


Figure 7: Star Topology Source: (Matin & Islam, 2012, p. 7)

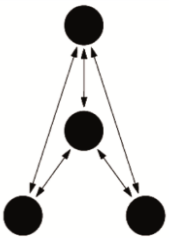


Figure 8: Mesh Topology Source: (Matin & Islam, 2012, p. 8)

Figure 9: Hybrid Star-Mesh Topology Source: (Matin & Islam, 2012, p. 9)

The topology has an effect on how the network can be secured. In order to break into an entire star network you need to break into the sink, which can have link-layer security. You can also break into a single node, but then you can only access that node. In a Mesh network however, you can gain knowledge about all nodes by breaking into one node since each node can forward information of other nodes (Neptune Technology Group Inc., 2010). Karlof & Wagner showed that each topology of sensor networks is still currently insecure. They argued that this is because the technology was not designed to be secure; it was designed to be able to connect. Thoughts about security measures only came at a later stadium (Karlof & Wagner, 2003).

2. Power: The amount of power that is needed for the communication is important. This is very relevant since this determines what kind of battery supply is needed for the sensor node. Therefore, the power also has a relevant effect on the size of the sensor node.
3. Data rate: This is the speed with which data can be exchanged between nodes and sinks.
4. Range: Data exchange can still happen between nodes and sinks in this area.
5. Costs: This is the cost of the technology compared to the other technologies.

In Table 4 an overview of the most promising communication technologies for sensors communications are given.

Technology	Topology	Power	Data rate	Range	Costs
NFC	P2P	Very low	400 KB/s	<10 cm	Low
Bluetooth (IEEE 802.15.1)	Scatternet	Low	1 MB/s-3 MB/s	<30 m	Low
Bluetooth LE (low energy, also called WiBree)	Star	Very low	1 MB/s	5-10 m	Low
WIFI (IEEE 802.11)	Star	Low- High	11-100 MB/s	2-20 m	Medium
ANT	P2P/Star/ Mesh/ Tree	Very Low	1 MB/s	1-30 m	Low
Z-Wave	Mesh	Very Low	40 KB/s	30 m	Medium
IEEE 802.15.4 (also called ZigBee)	Hybrid Star-Mesh	Low	250 KB/s	30-50 m	Medium
Wireless HART	Star / Mesh	Very Low	250 KB/s	200 m	Medium
KNX	Star/Mesh/Tree	Very Low	12 KB/s	800 m	Low
WiMAX	Mesh	High	11-100 MB/s	50 km	High
2.5-3.5 G	Mesh	High	1.9-7.2 MB/s	Phone range	High

Table 4: An overview of the most promising sensor communication technologies. Information from (Chaouchi, 2010) (Buratti, Conti, Dardari, & Verdone, 2009) (Karimi & Atkinson, 2012) (Zacharisas & Newe, 2010)

A short explanation of each of the technologies:

- NFC (Near Field Communication): Is very similar to RFID but with a smaller range. It is used to exchange information between two devices when they touch each other. There is research being carried out on to deploy NFC as an electronic wallet (Want, Near Field Communication, 2011).
- Bluetooth: Bluetooth was originally designed by Ericson to replace cables for communications between phones and computers (Zacharisas & Newe, 2010). Many devices that are connected with a computer use Bluetooth. Like wireless keyboards and headphones.
- Bluetooth LE: This is designed for sources that have low energy resources but still need a Bluetooth connection (Zacharisas & Newe, 2010).
- WI-FI: This technology is widely spread. Many people use this already in their home to wirelessly connect their home devices like a laptop to the internet. This technology is capable of transferring a vast amount of data per second but uses lots of power and because of that and therefore is not suitable for each sensor (Zacharisas & Newe, 2010).
- ANT: ANT is a low power low costs solution that can be implemented in all kinds of typologies and is therefore very flexible in its use (Dynastream Innovations Inc, 2013). ANT is being used particularly in sports and fitness equipment.
- Z-Wave: This technology is mainly used for monitoring and controlling home applications like automatically controlling lights or curtains (Z-Wave Alliance, 2012).

- IEEE 802.15.4 (ZigBee): ZigBee is most suitable to connect with simple devices that use minimal power; the data rate is low compared to Bluetooth for instance. ZigBee is a standard that is especially designed to work with sensors (Lee, Su, & Shen, 2007).
- Wireless HART: This technology is used the most in the industrial sector to monitor everything in the production process (HART, 2013).
- KNX: This is a communication standard mostly used for building automation like heat and lighting control (KNX, 2013).
- WiMAX: This technology can be seen as a successor of Wi-Fi, with not only a very high data rate but also a very large range. It is envisioned that WiMAX will be placed on top of cellular towers so that there is a fast internet connection everywhere (Sidhu, Singh, & Chhabra, 2007).
- 2.5-3.5 G: As mobile phones already have some sensors build in like a camera and a microphone, the cellular network could also be used to transmit sensor data (Kansal, Goraczko, & Zhao, 2007). A recent example of this is the experiment by the organization iSpex. In this experiment, 5000 volunteers from the Netherlands measured particulate matter with a special sensor attached to their smart phones. The measurements were sent to a central database (RIVM, 2013).

2.3 RFID and Sensors and the human body

Although the IoT only seems to be related to objects, it can also be related with RFID and sensors embedded in human bodies. RFID can, for instance, be used during surgeries to aid the surgeon; an RFID tag is then temporally placed in the body (Rogers, Jones, & Oleyniko, 2007). UHF RFID cannot be used inside the body since it does not work well around water, the most relevant substance of a human body, but the other frequencies RFID tags can be used in or near the human body. There is also a chip called the VeriChip, which is legally approved, by the U.S. Food and Drugs administration since 2004, to be implanted permanently inside the human body. This chip is about the size of a grain of rice (Foster & Jaeger, 2007). In the Netherlands, this VeriChip was implanted in VIPs in a nightclub in Rotterdam to be able to pay for their drinks with their arms (Dossier X, 2008). Although this chip is not widely implanted in humans (yet), it is already widely implanted in animals since 1970, for instance to be able to find the owner of a lost dog (Rieback, Crispo, & Tanenbaum, 2006). Some researchers are also exploring the idea of making edible RFID tags that could measure the food intake of people (ZDNet, 2011).

Sensors can also be used to measure physiological statuses of the human body, like heart rate, muscle activity, brain activity and such. These sensors can be placed on the human body but can also be implanted inside the body, depending on the aimed measurement (Jovanov, Milenkovic, Otto, & de Groen, 2005). There is, by example, already a Bluetooth sensor available that connects to a smartphone that warns a doctor when someone gets a heart attack (techzine, 2013). Another example is an implantable sensor that can detect the growth of cancer inside the body (scientias.nl, 2013).

2.4 IPv6

The real vision of the ITU about the IoT would only come true if in principle all things would be accessible through the internet, that you can for instance access their statuses from anywhere in the world. This means that all things would need their own IP address and therefore IPv4 is not suitable since it “only” has 4.3 billion addresses and, as stated at the

beginning of this chapter, the expectations are that by 2025 already 1 trillion devices are connected. With IPv6, there are 3.4×10^{38} that are 340 trillion, different addresses. This would give the opportunity for more things to be connected to the internet. IPv6 would make it possible that not only the gateway of a WSN is accessible but also all the separate nodes. There is already a taskforce that is working on the integration of the IEEE 802.15.4 (Zigbee) with IPv6, this technology is also called 6LoWpan (IPv6 over Low Power Wireless Personal Area Networks) (Bandyopadhyay & Sen, 2011). This IPv6 connection can also be made with RFID tags, and in principle, each item can carry both a sensor and an RFID tag. The RFID reader should be connected to a virtual Media Access Control (MAC) generator, also called a Home Agent in some literature (Dominikus & Schmidt, 2001). The reader sends the ID numbers of the RFID tag forward to the virtual MAC generator who stores the ID and assigns a virtual MAC address to the tag. This address is send towards the DHPC server that in return gives the IP address for the RFID tag back to generator. The item can then be accessed from everywhere in the world since it has its own IP address (Tsirbas, Giokas, & Koutsouris, 2010). An overview of this is given in Figure 10.

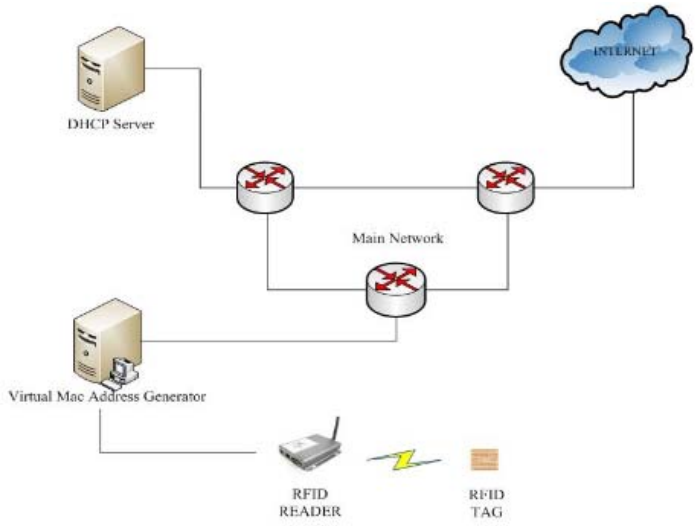


Figure 10: IPv6 and RFID source: (Tsirbas, Giokas, & Koutsouris, 2010, p. 810)

2.5 Benefits of the IoT

The IoT is seen as a very promising infrastructure. It can make our business but also our personal lives more efficient due to the automatic tracking, sensing and actuating capabilities of the IoT. The list of (business) opportunities with the IoT is endless. As you can see in Figure 29 of the appendix there are many businesses working on the IoT in different areas. Since the concept of the IoT is still relatively new and abstract to some, more sample applications are given below to gain a better feeling of what the IoT can establish. The examples are a small selection of the list of 50 most promising applications according to (IERC, 2012).

Smart grids

Smart grids are systems where energy is distributed more efficiently, the demand and availability of power are matched with each other. Devices, like washing machines, are connected in the smart grids and thereby the system can assign which home appliance is allowed to use energy, depending on the availability of energy. Home appliances from different households have to be connected with each other and an energy company to be

able to establish this, smart grids are therefore a very good example of an application of the IoT.

Supply chain control
With the use of the IoT the supply chain could be super-efficient. Each arriving box with items does not need to be scanned by hand anymore; everything can be scanned automatically. In addition, depending on which type of RFID tag is used it is easy to store extra information on the tag in each part of the chain, so that you get better overview of what happens in the total supply chain. This could for instance be used to get more insights in food waste.

Intelligent road systems
If all cars and roads would have sensors and actuators then they could react on each other in such a way that accidents and traffics jams could be limited.

Patient Surveillance
RFID and sensors could be used in hospitals to monitor the health status of the patients, thereby increasing their chance of survival. This could also help in reducing the costs of health care since patients can be controlled with a fewer amount of staff members.

2.6 Main points of this chapter

Main points of the chapter basic concepts of the internet of things

- With the use of RFID each item can be uniquely identified
- Sensors can basically measure anything
- RFID tags and sensors can also be implanted inside the human body
- The real vision of the IoT only comes true with all things have an IPv6 connection, since IPv4 does not have a sufficient amount of unique numbers
- The IoT can contribute to many things like efficiency, sustainability and healthcare

3 Privacy and constitutional rights

In the previous chapter, the technological possibilities of the IoT were described. The IoT will in principle be able to track all objects, but also humans, in the world and "know" everything about them. E. A. Blair, better known under his pseudonym George Orwell already warned the world against privacy invasion in 1948 with his novel "Nineteen Eighty-Four" where the character Big Brother knows everything about the citizens of Oceania mainly with the use of telescreens (Yeo, 2010) (Orwell, 1948). Furthermore, Huxley has warned the world against a society in which everything is controlled by technology from birth until death in his book "A brave new world". In the brave new world people are made artificially happy in such a way that there is no need for either individuality or personal freedom (Huxley, 1932). Are we by implementing the IoT actually implementing the Big Brother or even the brave new world?

In this chapter, the privacy rights will be analyzed. First, the notion of privacy is discussed. Then an argument is made why it is wise to look at privacy from the constitutional rights perspective. Then privacy rights in the Dutch constitution will be analyzed. These privacy rights were passed when information technology did not yet exist; therefore, the constitutional rights have to be put in the context of the digital age. Indicators for when there is a possibility that privacy rights are violated will be created. Then these Dutch rights will be placed in the broader European perspective. Finally, the protection of these rights will be discussed.

3.1 What is privacy?

The study of privacy is not new; many researchers have written papers and books about it. Around sixty thousands articles on privacy can be found on ScienceDirect for example. However, there is not one clear definition of privacy. Therefore, in many papers about privacy the authors first give their own definition of privacy. One famous definition is the one used by Warren and Brandeis whose definition of privacy is the "right to be let alone" (Warren & Brandeis, 1890). Warren and Brandeis are seen as the founders of the right to privacy since they were the first to argue that privacy should be seen as an independent right (de Graaf F. , 1977), that cannot be reduced to other constitutional rights. They developed their arguments in the context of privacy invasions brought about by technologies that were new back then, like photography and the printing press.

Another definition comes from Westin, he gave the definition that privacy is the control over what to disclose to others (Westin, 2003). The element of context is very important. In some situations, you do like to share information while you would not want this information to be shared in other situations. For instance, you would like to tell your friends that you were at a great concert but you do not want your boss to find out that this was the reason why you called in sick. And although you might want to share the pictures of your children playing in a bathtub with your family and close friends, but you would probably not want to share them with anyone else. Some researchers like Nissenbaum find the concept of context of such importance that contextual integrity is the essential element of privacy for them (Nissenbaum, 2004).

Privacy as defined by Westin is sometimes referred to as informational privacy (Fischer, 2010). Some researchers divide privacy into four categories namely body, territorial, informational and communicational privacy (Beresford & Stajano, 2003). Since this research

is aimed at how the IoT, which consist out of Information Technology, has an effect on privacy rights the focus is on informational privacy. This categorization is, however, not very strict since different categorizations can be found in literature as well, for instance in (Clarke, 1999), where behavioral privacy is also seen as a separate category.

Yet another definition comes from Gutwirth who discusses the meaning of privacy in his book “Privacyvrijheid!” (the freedom of privacy). He sees privacy as the protection of personal freedom. For Gutwirth the essential part of personal freedom is that it is undefinable, because its meaning varies from person to person and per context. Many elements of privacy are associated with personal freedom, for instance the free choice of relations and the integrity of body and spirit (Gutwirth, 1998). Since each person might give their own interpretation of what freedom means to them, consequently each person also has his/her own interpretation of privacy. Since the interpretation privacy is subjective, the perceived threats of privacy violations are also subjective. Some might see cameras in a public area as a threat to their privacy while others do not think this is a privacy invasion since they are of the opinion that you cannot have privacy in a public area. Based on the arguments of Gutwirth we do keep in mind that the interpretation of the concept of privacy may vary from person to person, but also from time to time, which might even be the most essential aspect of privacy.

Newell already noted in 1995 that perspectives on privacy are diverse across the different scientific disciplines (Newell, 1995), and that is still true today. It is clear that there is not a workable definition of privacy that has been accepted by all researchers. The only thing that most researchers agree on is that privacy is important and therefore important to protect. During this research, many conversations were held about privacy and from these it can be concluded that privacy is indeed a very subjective concept since almost everyone expressed their own definition. Since there is not a straightforward definition of privacy, another approach could be useful. For now, based on the above-mentioned different definitions of privacy, we will say that privacy has something to do with the protection of your personal life, and the control to whom and when you want to (not) disclose certain personal related information.

Since the Dutch Constitution (DC) can be assumed to be formed and adapted by means of a democratic process, the DC should reflect on the basic values shared among the majority of the Dutch citizens. Therefore, it is useful to look at the constitutional rights that are there to protect your personal life. The constitution is the supreme law of the Netherlands so all laws should also comply with constitutional rights (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013). By assessing privacy from the perspective of the constitutional rights, we have a legal basis that reflects the basic values of privacy. No matter what the personal subjective meanings of privacy of people might be, the constitution is applicable to all Dutch citizens, therefore the constitutional rights form an objective basis.

3.2 Privacy and constitutional rights

The DC stems from 1814 but has had some adaptions since. The DC is mainly based on the constitution of 1798 of the Bataafse Republiek (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013). In legal documents like the DC, many terms are used as synonyms for privacy like the terms “private life” and “personal sphere”, so all privacy related terms must be searched within the DC (Gutwirth, 1993, p. 623), to make sure that you capture all the privacy related rights. The rights in the first chapter of the constitution are also referred to as fundamental or human rights, so they are the basic rights that all citizens should have at the very least.

According to Bert-Jaap Koops et al., there are four articles in the DC that deal with privacy. These articles are article 10, 11, 12 and 13 of the DC (Koops, van Schooten, & Prinsen, 2004, p. 13). The original Dutch texts of the articles are cited below as well as the English translation given by the Dutch government on the website under the maintenance of the Documentation Center of the University of Leiden. Each of the articles will be discussed shortly and then an indicator for each article will be given which indicates that an information technology might violate privacy rights. If this indicator is met by a certain information technology, then this means that this article is threatened to be violated, this does not mean however that this threat or actual violation cannot be justified in some cases. In fact, each article can be lawfully limited under certain circumstances; this is arranged in designated laws.

3.2.1 Article 10: Privacy

Text from (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013).

Dutch literal text[1]:

> *1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.*
> *2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.*
> *3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.*

[1] Text copied from: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbl6ah4zz

English text translated commissioned by the Dutch government[23]:

> *1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament.*
> *2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.*
> *3. Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.*

This constitutional right is the broadest one of the privacy constitutional rights. Article 11, 12 and 13 can also be seen as subparts of this article. Paragraph 1 of this article says that all Dutch citizens have the right of respect of his personal life. This however again is very broad so it is hard to really test information technologies on this paragraph. But it can be interpreted as the right to not share everything of your personal life with others, and that others have to respect this, which makes sense looking at the next paragraphs. Paragraphs 2 and 3 refer to the collecting and storage of data, namely that this can only be done according to laws and these laws also establish how citizens can view and adapt data collected about them. This law is the *Wet Bescherming Persoonsgevens (WBP)* (the Data Protection Act) which is in accordance with Directive 95/46/EG of the European Union. A directive can be seen a mandatory guideline set by the EU where national law needs to comply to, in order to harmonize the European laws. The WBP basically states that data can only be collected (Logius, 2013):

- with the full consent of the person concerned
- if it is necessary for a clearly communicated purpose
- if the data is only used for this clearly communicated purpose
- if not more data than necessary is collected
- if the organization collecting the data takes (technical) measurements to protect the data
- if the data is not stored longer than necessary for the purpose

On top of this, the WBP also has a special paragraph regarding *sensitive* data, which has stricter rules. This is data about a person such as religion, political beliefs, health status, race or sexual orientation. In principle it is not allowed to collect this kind of data but if an organization has good reasons to store this information that it can be done, but stricter rules have to be followed (Logius, 2013). There is a specific authority responsible for making sure that everyone complies with the WBP, this is “het College Bescherming Persoonsgegevens” (CBP) (Data Protection Authority). Under certain circumstances, an organization also has to inform the CBP that it is collecting personal data (College Bescherming Persoonsgegevens, 2013). Something that is worth mentioning with respect to

[2] Text copied from: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbl6ah4zz

[3] It is interesting to note that the English translation could be interpreted slightly different than the Dutch text. This is the case for all the four articles. One could say that just by making a translation a small reinterpretation is inevitable.

this article is that currently the Secretary of Security and Justice, Fred Teeven, is trying to pass a law that requires a notification in case of a data breach. This means that each data holder has to inform the concerned persons and the CBP in case of a data breach (Rijksoverheid, 2013). This is already required in some other European countries, for instance, this is mandatory in Germany since 2009 (Hunton & Williams LLP, 2011).

To analyze whether the IoT might threaten to violate article 10 we need an indicator. Since this article is mostly about the collecting and availability of data, the following indicator is suggested:

There is a possibility that the right of privacy (article 10) is violated if data related to your personal life is collected.

The violation might be justified if the collecting of data is done in compliance with the rules of the WBP and CBP, but the threat of unlawful usage is still there once people start collecting data.

A discussion about the definition of data related to personal life can be held. In this research, the definition of the European Directive 95/46/EC for personal data will be used. This definition is: "*any information relating to an identified or identifiable natural person"* (EURLex, 2013). Engelfriet described this as follows; if information can lead towards an individual person, it must be personal information (Engelfriet, 2013). Since a photo can lead towards an individual, a photo is also considered as personal information. The picture on page 2 is therefore a violation of this privacy right since for some people it is very recognizable, despite the face blur, who is photographed in the picture and no permission has been asked. Personal information can also include data about which products are in your fridge if your fridge number is registered under your name. If your fridge for instance would actually be linked to albert.nl to make sure it would re-order certain items for you, your fridge must be also linked with you personally, otherwise albert.nl would not be able to deliver the items to your home or bill the right person. The working party of EU Directive 95/46/EG also gives opinions in relation with data protection that the member countries can use as guidelines when it is not clear if something is personal data or not. This was for instance the case with location-based data, which are also available in the IoT. It was not clear for organizations like the CBP how to deal with location-based data. The working party is of the opinion that location data is always personal data since the unique MAC address is needed in order to calculate the exact location, thereby it can be linked back towards to device and thus towards the person. The party also expressed their opinion that location data can be so privacy invasive that the individual really needs to explicitly express their consent for location data being used, this cannot be done with a general agreement (Data Protection Working Party, 2011). Interesting to note here is that in case you call an emergency number like 112, telecom providers have the obligation to share your location data with the emergency organization. The reason behind this obligation is that this could help people in life threatening situations since they might be unable to state where they are (Knol & Zwenne, 2009, p. 340). In this case, a value hierarchy can be identified since the value of life is seen as more important than the value of privacy.

3.2.2 Article 11: De onaantastbaarheid van het lichaam (the right to inviolability of the body)

Text from (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013).

Dutch literal text[4]:

> *Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam.*

English text translated commissioned by the Dutch government[5]:

> *Everyone shall have the right to inviolability of his person, without prejudice to restrictions laid down by or pursuant to Act of Parliament.*

This right can be seen as the right of integrity of your own body; you can decide what happens with it. This right came into the DC relatively late compared to the other rights, namely only in the adaption of 1983 (Koops & Prinsen, 2005). Article 11 seems to be mostly aimed at physical interference with the body. However, Koops & Prinsen, specialists in technology law, argue that information related to your body also belong to this right. In Canada and Germany court law has already suggested that not only the body itself but also data related to the human body should be protected under inviolability of the human body (Koops, Leenes, & de Hert, 2007). This right was included in the constitutional rights of the Netherlands through a motion of Kappeyne van de Copello and she added a nota in which she stated example acts that could be seen as violations of this right. One of them was radio graphical examinations (Mendelts, 2002). Because she included this violation, it can also be argued that information from the body gathered by other means can also be seen as violations to this right in the DC, since there is also no physical contact with radio graphically examinations. Just recall for instance the privacy discussion about the use of the full body scanners in Schiphol Airport that replaced the body searches by humans, many people felt threatened since the scanners could “see” right through their clothing (Mironenko, 2011). Therefore the indicator that this right might be violated is:

There is a possibility that the right of inviolability of the body (article 11) is violated if information about a person’s body is available to others.

Note that this can also include information about the clothes that you are wearing since it can give away details of your body. This indicator is actually a stricter indicator than the one for article 10, which makes sense since article 11 can be seen as a detailed element of article 10. Although the indicator is currently aimed at informational privacy, an actual physical interference with the body caused by the IoT will of course also be seen as a violation. The laws that state circumstance under which this right might be limited can for instance be found in the Police Act (Politiewet) of 1993 and article 56 of the Criminal Procedure Code (Wetboek van Strafvordering). From these laws it can be learned that it makes a difference if the body is externally or internally examined. A police officer can do external examination on the body if there is a good reason to do so. And in principle, this examination needs to be

[4] Text copied from: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnblu821m2
[5] Text copied from: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnblu821m2

done by someone from the same sex. If there are valid grounds to carry out an internal examination a doctor should be involved (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013) (Wetboek Online, 2013). Therefore, internal examination of the body can be seen as great violation of the right.

3.2.3 Article 12: Het huisrecht (the right to inviolability of the home)

Text from (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013).

Dutch literal text[6]:

> *1. Het binnentreden in een woning zonder toestemming van de bewoner is alleen geoorloofd in de gevallen bij of krachtens de wet bepaald, door hen die daartoe bij of krachtens de wet zijn aangewezen.*
> *2. Voor het binnentreden overeenkomstig het eerste lid zijn voorafgaande legitimatie en mededeling van het doel van het binnentreden vereist, behoudens bij de wet gestelde uitzonderingen.*
> *3. Aan de bewoner wordt zo spoedig mogelijk een schriftelijk verslag van het binnentreden verstrekt. Indien het binnentreden in het belang van de nationale veiligheid of dat van de strafvordering heeft plaatsgevonden, kan volgens bij de wet te stellen regels de verstrekking van het verslag worden uitgesteld. In de bij de wet te bepalen gevallen kan de verstrekking achterwege worden gelaten, indien het belang van de nationale veiligheid zich tegen verstrekking blijvend verzet.*

English text translated commissioned by the Dutch government[7]:

> *1. Entry into a home against the will of the occupant shall be permitted only in the cases laid down by or pursuant to Act of Parliament, by those designated for the purpose by or pursuant to Act of Parliament.*
> *2. Prior Identification and notice of purpose shall be required in order to enter a home under the preceding paragraph, subject to exceptions prescribed by Act of Parliament.*
> *3. A written report of the entry shall be issued to the occupant.*

This right is one of the oldest constitutional rights. It was in all the different constitutions that the Netherlands had, except for one year in 1814. Many researchers find this constitutional right the most important one. As de Vries, back then an important politician, put it in 1864;

"No freedom is possible if not everyone can find a safe harbor in his house and has the right to control whom to grant access to his home (Tak, 1973, p. 3)*".*

Note that the home does not necessarily need to be an actual house. In determining whether a location should be considered as a home, the use of the location is taking into consideration (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013). The general law to enter (in Dutch: "Algemene wet op het binnentreden") specifies

[6] Text copied from: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbm9pegm3
[7] Text copied from: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbm9pegm3

circumstances under which an officer of justice can commence a grant to enter a home and thereby limiting the right of a citizen (overheid.nl, 2013). Violating this right is seen as a very serious violation, so this general law has to be followed strictly. This right only limits itself to the actual home, so the garden is not included as can be read in the script of the Municipal of Vlissingen of how to practically apply the general law to enter (gemeente Vlissingen, 2004).

When article 11 was discussed in the previous section, it was questionable if physical interference was needed to violate the article. The same question goes for this article since it sounds like a real physical entrance in the home is needed for someone to violate this right. Koops & Prinsen also struggled with this question and they argued that the right should be interpreted such that a violation of it is already made if others gain knowledge about what is going on in the home (Koops & Prinsen, 2005). They also point to a report of the House of Representatives about eavesdropping of communications from outside the home, where it is stated that this can be seen as equal as actually entering the home to be able to deploy eavesdropping techniques (Tweede Kamer, 1997). Therefore, it can also be argued that the gathering of other information coming from the home can be seen as violations of this constitutional right. Therefore the indicator for this article is:

There is a possibility that the right of inviolability of the home (article 12) is violated if information about what is going on inside a home is available to others.

This can also be related to the resistance towards Google street view, since Google was sometimes literally taking pictures from inside the home that could be viewed online. In Japan for instance the Google cameras had to be lowered 40 centimeters since they were directly looking into the homes before (van 't Hof, van Est, & Daemen, 2010, p. 185).

3.2.4 Article 13: Het brief-, telegraaf- en telefoongeheim (The letter, telegraph and telephone privacy)

Text from (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013).

Dutch literal text[8]:

> *1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.*
> *2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.*

English text translated commissioned by the Dutch government[9]

> *1. The privacy of correspondence shall not be violated except in the cases laid down by Act of Parliament, by order of the courts.*
> *2. The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament.*

[8] Text copied from: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbn1m96qm
[9] Text copied from: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbn1m96qm

This article is about the right to have private conversations with others by other means than face-to-face communication. However, this right is explicitly stating letter, telephone and telegraph communications. Therefore, it is not clear if communication through the IoT would also fall under this right. Moreover, it is not clear if a communication originating from a thing could also be considered as communication. For instance if your fridge really sends an order to albert.nl, albert.nl would send the items together with an invoice. You could argue that no communications between humans have taken place. On the other hand, there are currently also lots of automated letters and they do fall under the protection of paragraph one so these automatically generated messages should be protected as well. In October 2012, a constitutional reform of article 13 was proposed. Since changing constitutional rights is not an easy process, the amendment is still not implemented. At his moment the amendment is in the phase where the ministers already agreed to it and it has to go through the House of Representatives and the Senate of the Netherlands (in the Netherlands known as the Second and First chamber). The text of the new proposed article 13 is[10]:

1. *Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim.*
2. *Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, met machtiging van een of meer bij de wet aangewezen ministers.*
3. *De wet stelt regels ter bescherming van het brief- en telecommunicatiegeheim.*

Unfortunately, there is no official translation available. Since giving a translation might lead towards a new interpretation, it is chosen to only discuss this new article. The protection of the letter is still stated explicitly but instead of just mentioning telephone and telegraph, all communication with telecommunications is included. It is interesting to note that the second paragraph is explicitly mentioning that this right might be limited in the interest of national security. The accompanied report with this new proposed article also mentions what they mean with communication. Three criteria must be met to be protected under this article according to this report.

The first one is that a communication tool is used, which would be the case in the IoT. The second one is that a third party is responsible for the transport of this communication; Google is for instance such a third party in case a mail is send through Gmail. Communications that are done over a private network do in principle not fall under this protection. Restrictions on gaining knowledge about communications in a private communications can be arranged in other rules or policies, for instance in the working conditions. In a reaction from the CBP to this report, it can be read that the CBP advises to also include private communications networks (CBP, 2013).

The last criteria mentioned in the report, needed to be considered communication, is that the communication is directed to an entity (this can be a person but also an organization for example). They explain that automated messages also fall under this right as long as it is directed. They also mention the differences between the information that is needed to deliver the message, which is also called traffic data, and the actual content of the message.

[10] Text copied from (Overheid.nl, 2012)

The traffic data is protected under article 10 and the message itself under this article 13 (Overheid.nl, 2012). Where traffic data stops and where the actual message begins is still a huge debate as can be read in the PhD thesis of (Fischer, 2010). But for now, an indicator is needed to determine if technologies or applications of the IoT might be a threat to article 13. For this research, the newly proposed article 13 will be taken into consideration, since this is a technical independent article and the chance is high that it will be implemented, since it already passed some crucial stages. Since the traffic data is already protected under article 10, the indicator should only be about the content message. There is a violation of this constitutional right if another party unrightfully takes note of the message. Therefore the indicator will be:

There is a possibility that the right to letter and telecom privacy (article 13) is violated if there is a possibility that another party takes note of the information content of a directed communication through (tele-)communications, operated by a third party.

Rightful violations of this article are mentioned in the Police Act and the Telecom Act (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013).

3.2.5 Summary of the indicators

Indicators are established for all four articles related to privacy in the constitutional rights in the DC. The indicators reveal when there is a possibility that a certain application or service in the IoT will actual violate a privacy right. These indicators are:

- There is a possibility that the right of privacy, article 10, is violated if data related to your personal life is collected.
- There is a possibility that the right of inviolability of the body (article 11) is violated if information about a person's body is available to others.
- There is a possibility that the right of inviolability of the home (article 12) is violated if information about what is going on inside a home is available to others.
- There is a possibility that the right to letter and telecom privacy (article 13) is violated if there is a possibility that another party takes note of the information content of a directed communication through (tele-)communications, operated by a third party.

3.2.6 Reasonable expectation of privacy

Indicators have been giving for each privacy related constitutional right, which can indicate that an information technology is violating these rights. This does not mean that an actual violation of a right has been made. In EU and US court ruling dealing with privacy, the term "Reasonable expectation of privacy" is used to assess whether an actual privacy violation has been taken place. This term basically means that you cannot claim privacy rights if there are reasons to not expect privacy. An example is that you cannot expect to not be overheard if you are telling a private story in a crowded train. Two principles are relevant, the voluntary and the mischance principle. The first one is if you voluntary share information with the rest of the world you cannot expect privacy protection anymore. The mischance principle refers to information that can be obtained by others without putting real efforts in this. For instance if someone walks by a home and the curtains are open the person could just look through the windows without any efforts. The person inside cannot expect that nobody could have seen him (McArthur, 2001). If there is valid indicator and the voluntary

and mischance principle do not apply then there is a violation of one of the privacy rights. As already discussed, under certain circumstance as stated in law these rights might be lawfully limited.

3.2.7 Constitutional rights proposed adaptions

Interpreting the constitutional rights is not straightforward, especially since new technological possibilities urge you to rethink the real thoughts behind the constitutional rights since technologies create new possibilities of violations. In 2000 there was a commission formed by the Dutch government under the lead of mister Franken that looked at the constitutional rights in the digital age. They were of the opinion that articles 11 and 12 were still valid and technically independent. The commission did had the intention to update article 7, which is about freedom of expression, with the paragraph that it is also free to gather information to form your opinion. They also had the intention to change article 10 in respect with the storage of personal related data. They tried to make sure that not only the storage of data was protected but also the processing of information. They also desired to change article 13 towards a technical independent formulation of privacy of communication (Franken, 1999). Unfortunately all these efforts of the commission where in vain, since the whole rapport was dismissed. Later in 2010 there was another commission named Commission Grondwet that also intended to change articles 7, 10 and 13 (Verhey, 2011), but not 11 or 12. However only article 13 is currently in the process of being changed as described earlier, the actual text is different however from the ones proposed by the commissions. The existence of these commissions proves that interpreting the constitutional rights in this digital world is not straightforward.

3.2.8 European and universal human rights

Up until now, the constitutional rights in the Netherlands were examined but since the IoT is worldwide, since it does not have a physical border, it is also wise to look at these rights in a broader context. Privacy rights can also be found in article 8 of the European Convention for the Protection of Human Rights (ECHR). Article 8 of the ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence (Counsil of Europe, 2010). Article 12 of the Universal Declaration of Human Rights states that everyone has the right to protection of interference of his privacy, family, home and correspondence. On top of this, it also says that no one shall be subjected to attacks upon his honor and reputation (UN, 2013). Article 17 of the International Covenant on Civil and Political Rights mandates this right (United Nations, 2013). These rights are very similar to the DC, although the inviolability of the body is not mentioned as explicitly as in the DC. It can be concluded however that the indicators that were set for the Dutch Constitution can also be used for European and global rights.

3.3 Violations of constitutional rights by whom

The DC can be split into classical and social rights. The more classical rights can be seen as rights that protect the citizens from interference from the government and social rights can be seen as rights that can be seen as provisions that the government has to arrange for its citizens (Akkermans, Bax, & Verhey, 2005). The constitutional rights regarding privacy can all be seen as classical rights, thereby protecting citizens from interference from the government. One of the most prominent discussion of the classical rights is to what extend these rights are also applicable in *horizontal relations*, for instance between private companies and citizens (van der Pot, 2004). Leenknegt argues that these rights are indeed

horizontally applicable. He argues that the existence of the WBP is a proof of this, since the WBP is also applied horizontal (Leenknegt, 2002). This horizontal application is also in line with the Human Rights Committee's general comment #16, which states that humans should be protected from privacy violations, no matter whether a private or public body is the violator (Colville, 2013). Therefore, the privacy rights can be violated not just by the government but also by private companies and persons.

3.3.1 Privacy protection

Having a right to privacy is not the same as having protection of privacy. As seen above the Dutch law describes circumstances under which constitutional rights can be limited. And how privacy is protected varies per country since the legal en cultural meaning of privacy varies around the world (Gutwirth, 1993). Although the declaration of human rights is universal, the protection of privacy is not universal; in fact, it is far from universal. As mentioned earlier the WBP is in accordance with Directive 95/46/EG of the European Union. This Directive sets obligatory guidelines for national laws to harmonize European law in relation with data protection. But there still exists differences among the member countries. The proposed law by Teeven to enforce a data breach notification is for instance already obligatory in Germany (Shaw, 2012). The EU is currently in progress of passing the data protection regulation. An EU regulation is law that is valid in each member state. This regulation will increase the privacy protection of consumers. One of the big changes in this regulation is that consumers have more control over their data, also over the deletion of their data, the so-called "right to be forgotten" (European Commission, 2012). This proposed EU law is still being reviewed and adapted, it is not clear yet if and when this law will become effective. Privacy data protection in the United States is very different than in Europe. In the US the data privacy protection is mostly aimed at protection from the government. In practice, the European privacy laws are stricter. The data of European citizens are only allowed to be processed outside the EU if the other country has at least the same data protection as the EU. Data protection in the US does not meet the requirements of the EU standard. Therefore, US companies are in principle not allowed to process data from EU citizens. Since many US companies also operate in Europe, there is the Safe Harbor agreement between the US and the EU. When a US company follows all the rules in the agreement, it can handle information of EU citizens (Levin & Nicholson, 2005). And in some other countries in the world privacy protection is not part of the legal system yet. It is important to realize that this protection of data privacy varies around the world since the internet does not have physical borders. When you are searching the web and you visit a US website then your personal data might be treated differently than when you browse on an EU website.

3.3.2 Data Privacy and property rights

One of the problems with the protection of data privacy is that data is not a physical object. Instead, it is a virtual object that is easily copied. The problem with this is that you have less control over it. If I lend my bike to someone, I do not have it anymore and therefore cannot ride it myself. However, if I get my bike back then I know that the person I lend it to cannot ride it anymore. However, if I give my personal information to a web shop to make an order I do not physically give away something that I can get back. Then you lose control of what happens next with your personal data. In Germany, it is a constitutional right to freely develop your personality. And to preserve this right they have the information self-determination right (In German "Informationelles Selbstbestimmungsrecht"), which means

that they have the right to control where their information flows, this is in line with Westins thought about privacy (Gutwirth, Poullet, de Hert, de Terwangne, & Nouwt, 2012). Therefore, a company cannot give your information to another company without your expressed consent. This in some sense gives you a sort of property right to your data. Purtova shows in her PhD thesis that the introduction of property rights for personal data would indeed be possible within the scope of European law and that this would give people more control over their own data (Purtova, 2011). This would seem fair because a company collecting all this data may have certain rights namely sui generis rights and database copyright. Sui generis rights is the rights that you get for the substantial effort that was put in the collecting of the data and database copyright is the right that you get for originality of the selection of the data (Bainbridge, 2007).

3.4 Main points of this chapter

Main points of the chapter privacy and constitutional rights

- Privacy is difficult to define since people have different opinions about its meaning; however, constitutional privacy rights are applicable to all of us and can therefore be used as an objective basis.
- The following are indicators of a technology that can threaten to violate constitutional privacy rights:
    - There is a possibility that the right of privacy, article 10, is violated if data related to your personal life is collected.
    - There is a possibility that the right of inviolability of the body (article 11) is violated if information about a person's body is available to others.
    - There is a possibility that the right of inviolability of the home (article 12) is violated if information about what is going on inside a home is available to others.
    - There is a possibility that the right to letter and telecom privacy (article 13) is violated if there is a possibility that another party takes note of the information content of a directed communication through (tele-)communications, operated through a third party.
- To judge whether there is an actual violation of privacy rights the term "reasonable expectation of privacy" is applied. This consist out of two important principles namely the voluntary and the mischance principle.
- Privacy rights can be violated by a governmental organization but also by private companies and natural persons.
- The indicators for the four privacy rights can also be used in an EU or universal context.
- Having a right to privacy is not the same as having privacy protection.
- Privacy rules vary around the world, there are already substantial differences between the EU and the US, therefore the safe harbor agreement exists.
- There is a legal possibility to give a property right to personal data.

4 The internet of things compared to the Internet

As stated earlier the privacy discussion in the digital age is not new. The discussion is very large and there are many organizations, like *Bits of Freedom,* and researchers fighting for privacy on the internet. Therefore, a research on privacy can easily become a repetition of research already done. However, the internet of things is a new internet infrastructure that might pose new threats on top of those threats already posed by the internet. Therefore, for the rest of the research the focus will be on new possibilities brought by the IoT that poses other or more serious threats than the internet already does. In the previous chapter, four constitutional rights related to privacy were discussed. Now each of these articles in relation with the new possibilities of the IoT compared to the internet will be discussed.

4.1.1 Article 10

Article 10, the general right to privacy, is mostly about the collection of information in databases and is closely related to the WBP. The IoT will add lots of new information in these databases. It will become easier to profile persons with all this new information availability. A term widely used for all this information availability is *Big Data.* Therefore, the threat of the IoT, compared to the Internet, in relation with article 10 is that there will be much more information available in the databases stemming from all these sensors and RFID tags. As stated in the previous chapter, the WBP dictates stricter rules for *sensitive* information like health status. In the basic concept chapter it was seen that sensors can be placed in or on the human body to collect physiological information, consequently there will probably be more *sensitive* data available in the future, but more about this later in the part about article 11. Besides the addition of *sensitive* and lots of new data the IoT is not actually creating new threats, but it is making the already existing threats larger.

4.1.2 Article 13

Article 13, communication privacy, is about the right to have private conversations. As discussed, the actual content of the message is protected under this article and the protection of the traffic data, necessary to deliver the message, is protected under the right of article 10. That people find the right to private communications important has become clear the last few months with all the news about PRISM. The existence of PRISM became known after a report by Edward Snowden, former employee of the National Security Agency (NSA). PRISM is a program used by the US to spy on email, internet usage and telephone calls. Barrack Obama, US president, has confirmed that this program exists but said that this program is only aimed at people outside the US in order to detect potential terrorists (The Guardian, 2013). It has also become clear that even encrypted messages were decrypted and thus spied upon (Volkskrant, 2013). PRISM is also able to see all the usage data of smartphone, like contacts and location data (NOS, 2013). Many people have been shocked after hearing this news about the existence of PRISM. In the beginning of this research, many people gave a rather indifferent reaction when stated that a research about privacy was done. After this news came out, people started to realize the importance of research on privacy. That new technologies have an effect on the right of this article is clear, and as discussed, the adapted article will be technologically neutral in the sense that all electronic communications will also be protected. The IoT will create many automated communications, thus existing threats will be amplified. But the threats will not be that much different of what is currently already happening. As with article 10, the IoT will not put new threats of violations to the rights of article 13, but it will make the existing threats

larger. And as stated in the last chapter rights from this article can only be claimed if a third party is responsible for the transport of the message. If the IoT is used within a private network then in principle no privacy rights can be claimed from this article.

4.1.3 Article 11 & 12

Gutwirth noted in 1993, that new technologies do not actually create privacy threats but that they amplify the already existing threats (Gutwirth, 1993, p. 34). This is exactly what has been concluded for articles 10 and 13. However, it seems that the threats for article 11 and 12 are so different that they can actually be perceived as new threats. Almost nothing has been written about article 11, the inviolability of the body, and article 12, the inviolability of the home, in relation with new technical possibilities. As discussed in the legal chapter commission Franken and commission Grondwet that were installed to look at the constitutional rights in relation with new technologies did not feel the need to change article 11 and 12. They were of the opinion that the rights were still protected equally despite new technologies. Koops et al. did a comparative study on constitutional rights and new technologies in six countries and they did take article 11 &12 into consideration. From this research, it can be learned that other countries also did not review the right of inviolability of the home in relation with new technologies except for Germany. Germany has included a list, in their inviolability of the home right, with technologies that can be used in certain cases for criminal investigation. Also, the reviewing of the countries with respect to the right of inviolability of the body was very low. Even with discussions about DNA samples, the discussion was directed at protection data privacy instead of protection of body integrity. But it was already mentioned that German and Canadian courts have ruled that information about the body should also be protected under the inviolability of the body. Interesting to mention is that the Canadian Court applies the rule that the closer an object can be related to a body the more body privacy rights should be assigned to the objects (Koops, Leenes, & de Hert, 2007).

The IoT will connect all things, also inside the home and the human body, with internet. All this new technology will give much information about the statuses of our homes and bodies. Koops & Prinsen argue that all this information availability is so large that it will make our homes and bodies “transparent” (Koops & Prinsen, 2005). Therefore, the IoT will threaten the rights in article 11 and 12 in new ways. As stated in the previous chapter article 11 and 12 are currently formulated aimed at physical interference, but it has been argued that these can also be violated with the availability of information gained with information and communication technology that was otherwise only possible with physical interference. Just to give a brief example, currently a heart rate has to be measured directly at the body, but if someone would have a heart sensor, this information can be gathered without physical interference.

The inviolability of the home and the body are very important basic rights and that is probably the reason why they both got a separate article in our constitution. Until now, the discussion about the protection of these rights in relation with new technologies has mostly been aimed at the protection of databases and therefore article 10. Since the IoT has the potential to make all of our homes and bodies “transparent” with the use of RFID and sensors, the rest of this research will focus on these two rights. But since all four privacy

rights are closely related to each other the other rights also play a big role, but the reasoning will take place from the viewpoint of the rights articulated in article 11 and 12.

4.2 Privacy reasoned from the human body and the home

The rest of this research will focus on the rights of inviolability of our body and our homes. In the previous chapter, indicators were created for when the rights of these articles might be violated. When information about a body or a home is available to others, thus not necessarily stored yet, then there were already indicators that privacy rights might be violated. It was also stated that there are rules of when the rights could be legally violated. Internal examinations of the body are greater violations than external examinations, so therefore information from inside the body should be seen as a larger violation than information from the exterior part of the body. In addition, as seen from the Canadian court case, objects related to a body like clothing or a purse can fall under protection of the right of body integrity, but the protection is weaker than of the body itself. Just compare this with when you go to a concert. Special security personnel often check your purse and the pockets of your jacket and sometimes if they have good reasons, they do a body search. Privacy is related with your personal life and this starts with the existence of your own body that you "carry" with you all the time, therefore it could argued that your body deserves more protection than your home. From this a privacy model taking the human body as a starting point can be created, the model is seen in Figure 11. The inner layer deserves the most privacy protection. All rings in the model represent a class of information that deserves privacy rights, given by article 11 or 12 of the Dutch constitution.

Article 12 limits itself explicitly to the entering of a home, although it feels intuitively right to also include the garden and/or a shed in case the home is situated on a private property. In case the home is a house then often there is also a garden. If you are sunbathing in your garden, you expect more privacy than when you are doing this on the beach. In article 138 of the Penal Code (Wetboek van Strafrecht), it is seen as a criminal offense if someone enters your land without permission (Wetboek Online, 2013). And in Belgium, where the constitution should also follow article 8 of the ECHR, it became clear from case law that the land should be included (Rimanque, 2005). Therefore, it is decided to also include this as the outer ring of the model, but it is weakly protected from the viewpoint of the Dutch constitution. If information stipulated in one of the layers in the model below is either stored or communicated, it should not only get a protection from either article 10, general right to privacy, or 13, privacy of communications, but also of article 11, inviolability of the body, or article 12, inviolability of the home. And the more the information is from an inner layer the more protection it should get. The rest of the research will focus on the privacy rights that should be given to information that belongs to one of the layers in this model.

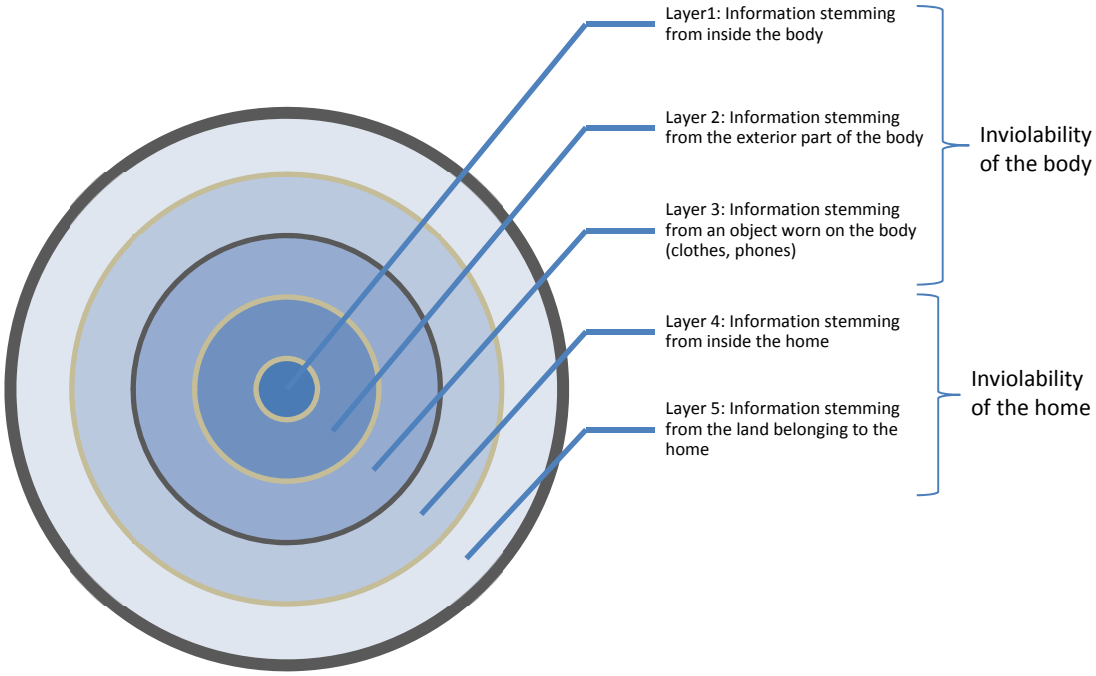


Figure 11: Privacy taking the human body as a starting point, the inner layer deserves the most privacy

4.2.1 Note with respect to this model

This model is explicitly about the physical aspects of the home and the body. This model takes the human body as a starting point, this does not mean however that other aspects of privacy are not relevant to protect. Mental integrity is also very important and it could be argued that this aspect should also be included in this model since this model is related to the body. However, mental integrity is not protected under article 11, inviolability of the body. Mental integrity is protected under article 10, general right to privacy, as can be read in (Overkleeft-Verburg, 2000) and (Leenen & Gevers, 2008). As discussed in the previous chapter article 11 can be seen as a subpart of article 10. Integrity of the body and mental integrity are closely related, and article 11 can be seen as purely protecting the physical part of the body, but of course this can also have an effect on mentality. It could even be argued that integrity of the body is a necessary condition to have mental integrity.

4.3 Main points of this chapter

Main points of the chapter the internet of things vs. the internet

- The real new threat of the IoT is that it is making our bodies and homes “transparent”.
- Not much attention has been giving to the rights in article 11 and 12 in relation to information technology.
- A model of severity of privacy violations can be made taking the human body as a starting point.

5 Data traffic flow

In the previous chapter, a model was given which classifies information that deserves privacy protection according to our constitutional rights. If this information is communicated through a transport line managed by a third party, the information content should be protected under article 13. And if this information is processed it also falls under the protection of article 10, thereby the processing has to comply with the WBP. As has been argued in the legal chapter, this information should also be protected under article 11 and 12 if it is available to others. It would be too bold to say that just the availability of this information would already be a violation of these privacy rights. Only when this information is actually (unwillingly) disclosed to others there is a threat of privacy violation. As discussed, the reasonable expectation of privacy is also important to assess whether there is an actual violation. Before it really can be assessed how the IoT is posing a threat to the constitutional privacy rights, more needs to be learned about how information is shared through communication technologies. Since communication technologies actually do not share information but data, the difference between data and information will first be explained. Then the data flows between different parties can be discussed. Some models exist to explain how this works. Two of the models will be explained, the one by Bekkers & Smits and the one by Solove. Since they are both useful and can complement each other a new model will be presented that combines the models.

5.1 Data versus information

Up until now, the words data and information have been used interchangeably in this document. There is a difference however between the words data and information. Zins has researched the differences between data, information and knowledge and found that there are many different definitions used for these concepts, therefore it is important to explain what is meant by these terms (Zins, 2007). In this research, information means interpreted data. Communications technologies, like RFID, do not deal with information but with data. Data basically just consist of a certain length of bits, containing 1s and 0s. To send information through communication technology, information is converted to data and additional data is added to make sure that the information reaches its desired destination. The receiver gets the data and if the information can be decompiled from the data, than the information communication was successful. As already discussed, the additional data needed to deliver the message is called traffic data and can also contain very relevant personal data (Fischer, 2010). This additional data can for instance be the address of the receiver. Recently a journalist gave TNO access to his mailbox and they were able to recreate his social network just by looking at who and how frequently he sends mails (van de Weije, 2013).

The whole flow of data needed to exchange information is called *data traffic.* Thus, data traffic contains the information content and traffic data as can be seen in Figure 12.

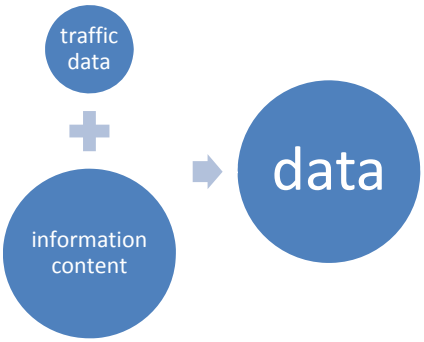


Figure 12: Data is traffic data plus information content

5.2 Model by Bekkers & Smits

Bekkers and Smits looked at the patterns of information traffic and extended the model of Bordewijk & van Kraan (Bekkers & Smits, 1999). This model classifies the type of information traffic according to two parameters:

- Content: Is an individual or a central institution the provider of the information content? In other words, who is in the possession of the data?
- Schedule: Who determines how, when and what is communicated, an individual or a central institution?

This model also considers traffic data; therefore, it is actually looking at the flow of data traffic instead of information traffic. Four different types of data traffic patterns can be distinguished as can be seen in Table 5. Although these four types of data traffic patterns can be distinguished, most forms of communications actually contain more than one of the patterns, so we have to keep this in mind (Fischer, 2010).

- Conversation: Since both the schedule and the content belong to an individual, this is the most privacy sensitive data traffic flow. An example of this type is an email. As previously discussed, the content data of an email is protected under article 13 and the traffic data is protected under article 10.
- Consultation: An example of this type of data traffic is visiting a website. Although the communicated content in this case is public information, the traffic data can reveal a lot about a person since you gain knowledge about the interest of a person.
- Registration: This is also a very privacy sensitive type of data traffic, since the individual cannot really control how and when their information is treated. An example of this type of communication is when someone is photographed on a highway for driving too fast.
- Allocution: When communication falls under this category the data traffic does in principle not contain individual content data or individual traffic data of the individual accessing this information and therefore this form of data traffic is the least sensitive pattern. An example of this type of data traffic is radio. In the next chapter, it can be seen that there is a shift from allocution towards consultation and registration.

	Individual content data	Central content data
Individual schedule	Conversation	Consultation
Central schedule	Registration	Allocution

Table 5: The four types of data traffic patterns. Adapted from (Bekkers & Smits, 1999) & (Fischer, 2010)

Bekkers and Smits also put the four patterns in relation with the communication layer model of the Dutch Media Council. A simplified adapted model of this layer model is given for each of the pattern types; it gives you more insight about how the data actually flows in these different data traffic patterns. The transport layer includes the network and infrastructure services and the informational layers contain the device on which the information is received and the information content itself. A thick arrow represents the information content and a thin arrow represents the traffic data (Bekkers & Smits, 1999) (Fischer, 2010).

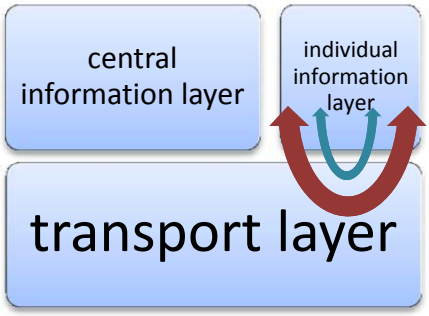


Figure 13: Conversation

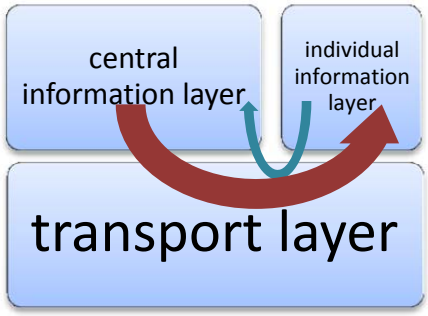


Figure 14: Consultation

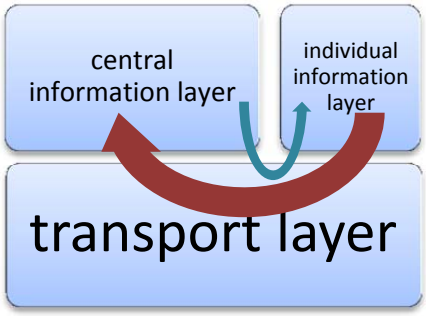


Figure 15: Registration

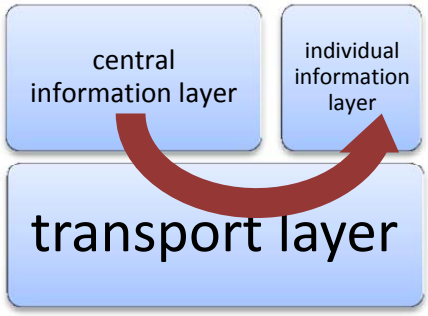


Figure 16: Allocution

If these types of data traffic patterns are related with the privacy model from the last chapter than the data traffic patterns registration and conversation are the most relevant ones to look at. Because in these two patterns, data from the individual layer is communicated and if this data contains information about a person's body or homes than there might be a violation of these privacy rights. The central information layer is not strictly a central institution, this could also be another person, and the most important thing is that the data subject has not the control over that data. In

Figure 17 the different traffic patterns have been put in the privacy model reasoned from the human body. In this model, an incoming or outgoing arrow could have started or ended in each of the different layers. The relevant aspect is if it is leaving or entering the private sphere, which border is the dark circle. Again, a thin arrow represents traffic data and a thick arrow represents information content.

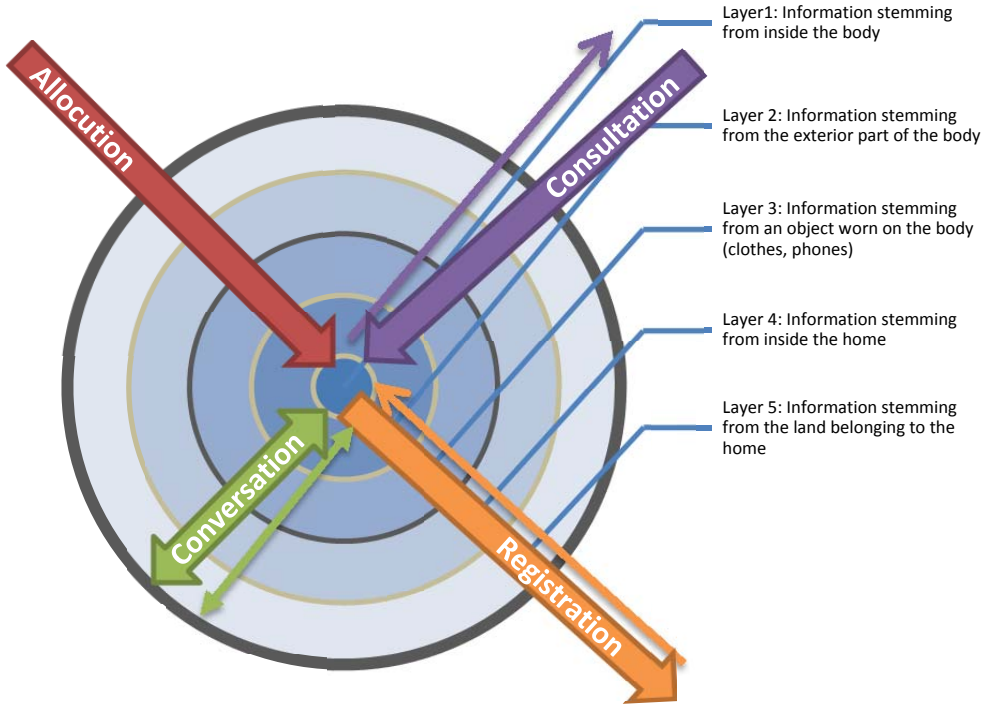


Figure 17: Data traffic in the privacy model

As stated earlier, the viewpoint of this research is from the information that should be protected under article 11 and 12, but article 10 and 13 are still very relevant. If the transport layer is operated by a third party than the information content should also be protected under article 13. And if the information from one of the layers is registered by a central entity this has to be done in compliance with the WBP.

5.3 Model by Solove

The model by Bekkers and Smits show the different data traffic patterns that communication of data can have. The model by Solove has a different conceptualization and separate different stages in the data flow process. These stages are information collection, information processing and information dissemination. The collecting stage is the gathering of information. The processing stage of information includes the storage and usage of the information. In the dissemination stage, data is send forward. At each of these stages, Solove recognizes different privacy threats, which are given (in red) in the model. In the next chapter, some of these threats will be discussed in detail. The model, given in Figure 18, also shows stakeholders in the process, namely the data subject and the data holders (Solove, 2006). At the dissemination stage, the data can flow back towards the data subjects but also to third parties so they have been added to the model of Solove.

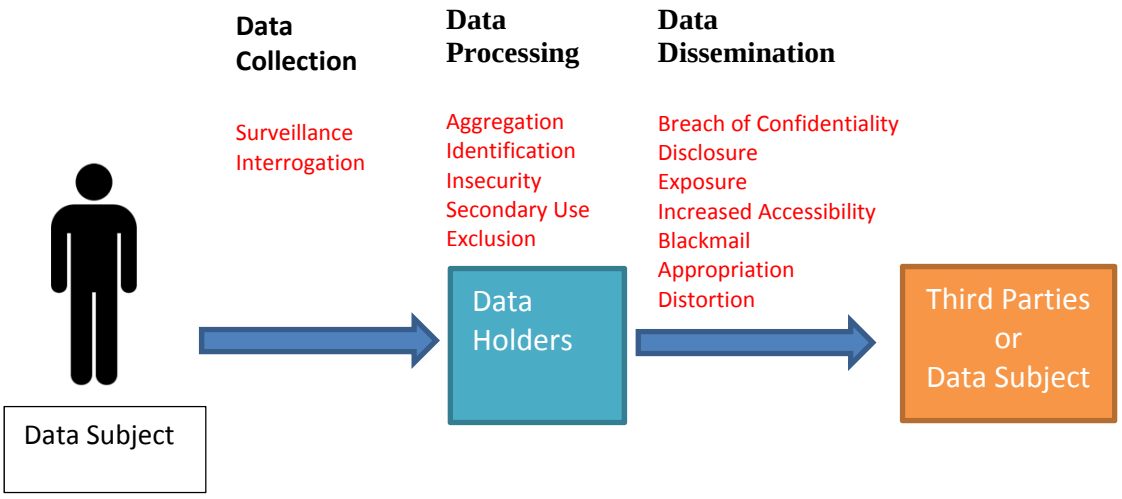


Figure 18: Data flow model adapted from (Solove, 2006)

As you can see in this model more privacy threats are added in each stage, so you could say that once your information is collected it is harder to control your privacy preservation. In this model, it all starts with the availability of data at the data subject site. If a data holder processes the data than the information is collected. This difference between available and processed data is important to note, only when this information is processed by another person or organization there is a change that your privacy rights have been violated. If this model is related with the privacy model from last chapter and the IoT, then on the data subject site there is availability of information content from the home or body made possible by sensor and RFID technology.

5.4 Combined Model

Two models of data flows that can be used to explain the privacy threats posed by the IoT were discussed above. The model of Bekkers & Smits is more applicable to how the communication process takes place and the model of Solove is more applicable for the different stages information, in the form of data, can go through. Bekkers & Smits model does not consider the step after the information content from the individual layer has entered the central layer. Because once the central layer has individual data, the central layer also contains data belonging to an individual person. The information content is from that moment in the control of the central layer, even if this collection was done without the consent of the information subject. If this collection was done lawfully, it had to comply with the WBP and therefore the consent of the data subject was given. But either way, if this information is accessed from the central layer it can either be through allocution or by consultation. This way of thinking about what happens when information enters a central layer is supported by (McMillan, 2002) and by (Quinn, 2005). A radio show talking about a personal relationship of an artist is an example of allocution of personal information. Visiting Facebook or Twitter are examples of consultation of personal information located in a central database. In principle, everyone in the world can see all the posts through consultation unless the concerned individual changed the privacy settings. If consultation on a website is limited to certain persons then the traffic data can also include a password for access control.

If these two models are combined, to be able to assess violations of rights in the privacy model taking the human body as a starting point of last chapter, two separate stages can be identified. Those stages are the data collecting stage and the data flow stage. In the collecting stage, information content originating from a home or body is collected using sensors and/or RFID. This information content belongs to an individual and therefore it can either be collected in a conversation or in a registration data traffic pattern, this can be seen in Figure 19. If this is done by registration the data is collected outside the body and home, then there is an external data holder and thus the information is stored in a central layer. Again, this central layer can also be another individual. The point is that this data is in the control of an entity outside the personal layer. If the collection is done by conversation the information content is stored locally at the body or home, for instance on a smartphone or a designated monitor.

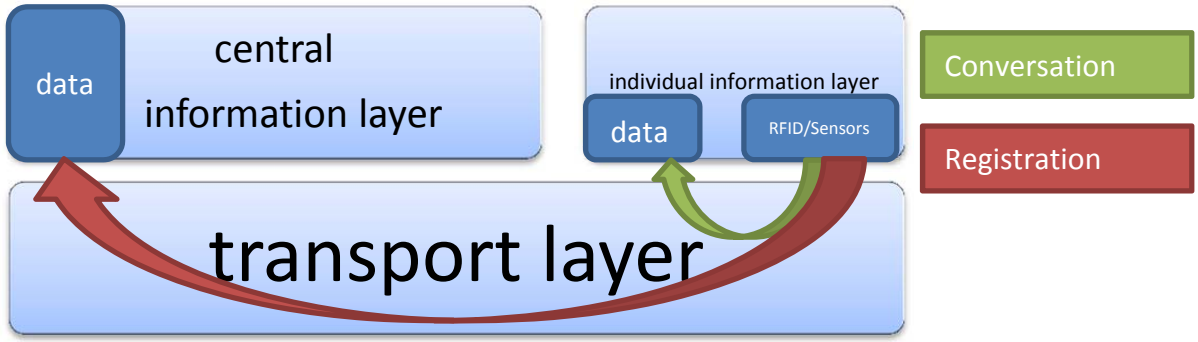


Figure 19: RFID/Sensor collecting stage. The red arrow is registration and the green arrow is conversation

After the collection stage, the information content can be communicated further; this can be back to the data subject or to third parties. In the case that the data subject is also the data holder the communication can either be in a conversation or a registration manner, since the information is still in the individual layer. In the case that the data holder is external, the communication is by allocution or consultation since the information is in the central layer. Before or after the data flow stage processing of data can take place. The combined model is shown in Figure 20. This model will be used in the following chapter to explain how the IoT is threatening our privacy rights. It is chosen to not explicitly put the processing stage in the data flow model, but threats of processing at a data holder will also be discussed in the following chapter.

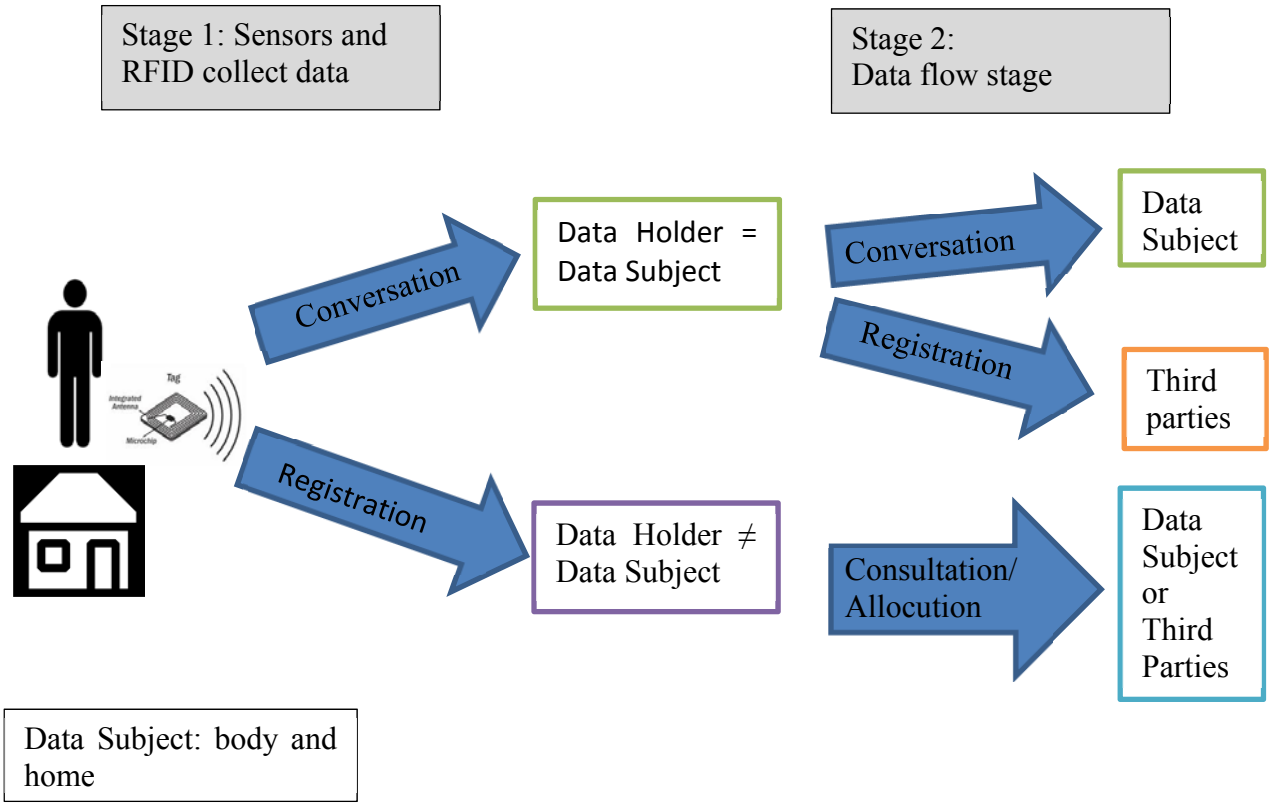


Figure 20: IoT data flow model

5.5 Main points of this chapter

Main points of the chapter data flow

- There is a difference between information and data. Data send through a communication channel contains information content plus traffic data, needed to deliver the information.
- According to the model of Bekkers and Smits there are four types of data traffic flows, namely conversation, consultation, registration and allocution.
- According to the model of Solove there are three different stages at which privacy issues might arise, namely at the stage of data collection, data processing and data dissemination.
- The combined model separates two stages namely the stage of data collection and the stage of data flow.

6 Threats of violations of constitutional privacy rights posed by the internet of things

The basic concepts of the IoT, the constitutional privacy rights, a privacy model taking the human body as a starting point, and data flows have been discussed. In this chapter, everything will come together, thereby assessing if and how the IoT threatens to violate Dutch constitutional privacy rights, the inviolability of the body and the inviolability of the home in particular. In the last chapter, data flow models were given which can be useful to assess privacy threats. In the combined model two important stages were distinguished, namely the data collecting stage and the data flow stage. Both of these stages will be zoomed into, the collection stage in particular and it will be identified if and how the technologies of the IoT pose threats to violate constitutional privacy rights. This will be done with the use of example scenarios where the world without the IoT is compared with the world with the IoT. After the stages and the threats related to the stages are described, also actual physical interferences with the home and body will be discussed. Although the word threat is used in this chapter, some of the threats are already actually happening to some extent.

6.1 Data collecting stage

The first stage is the data collecting stage. Earlier a privacy model, taking the human body as a starting point, was created. Each layer in this model represents a class of information that should either be protected by article 11, inviolability of the body or by article 12, inviolability of the home. In the basic concepts chapter, it was seen that RFID and sensor technologies are technologies capable of making things able to communicate with the rest of the world, so putting things “online”. If these things are attached in or on our homes and bodies, they are capable of capturing information that can be classified in one of the layers in the privacy model taking the human body as a starting point. And the collection of this information can either be done by conversation or by registration, as argued in the last chapter. An overview of this is giving in Figure 21.

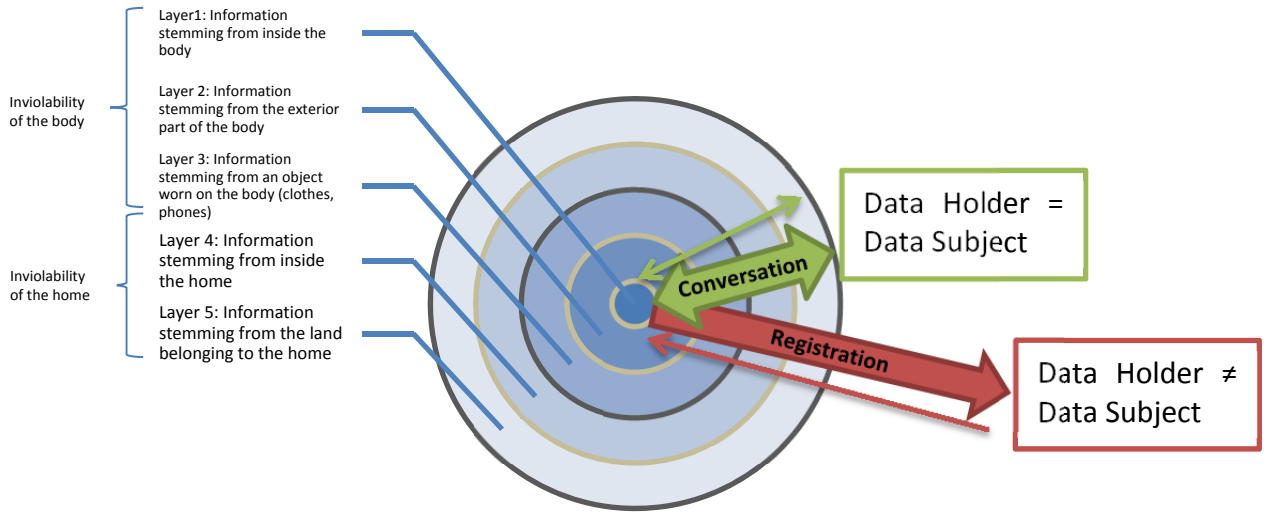


Figure 21: Data collection stage

In the “offline” world, were information from the body or home cannot be collected or communicated by electronic means there are also ways of collecting this kind of information. Several scenarios will be discussed in which the offline world is compared to the world enhanced with the IoT. The scenarios will help to better understand what the impact of the IoT is.

6.1.1 Information collection by conversation

If data collection is done through conversation, information content is collected locally at the home or body; it does not leave the private sphere in this stage. In principle, this is the most privacy friendly manner of information collection since the data subject keeps hold of the data and knows what is in the data that could be disseminated. Let us consider an offline home scenario where all windows have roller shutters and the persons inside the home closed all of them. Assuming there are no infrared cameras or such nearby, there is in principle no way for someone else to collect information about what is going on inside the home and what objects are present unless they are actually inside the home. Nobody can even see if the lights are on or not, due to the roller shutters. The persons inside the home can therefore, at this this point, expect all the privacy in the world. In the vision of the IoT all things, also inside homes, are connected with each other and the internet with the use of the technologies that were seen in the basic concepts chapter. In Figure 22 there is an example overview of a smart home environment where all devices in the home are connected with each other through IoT technologies.

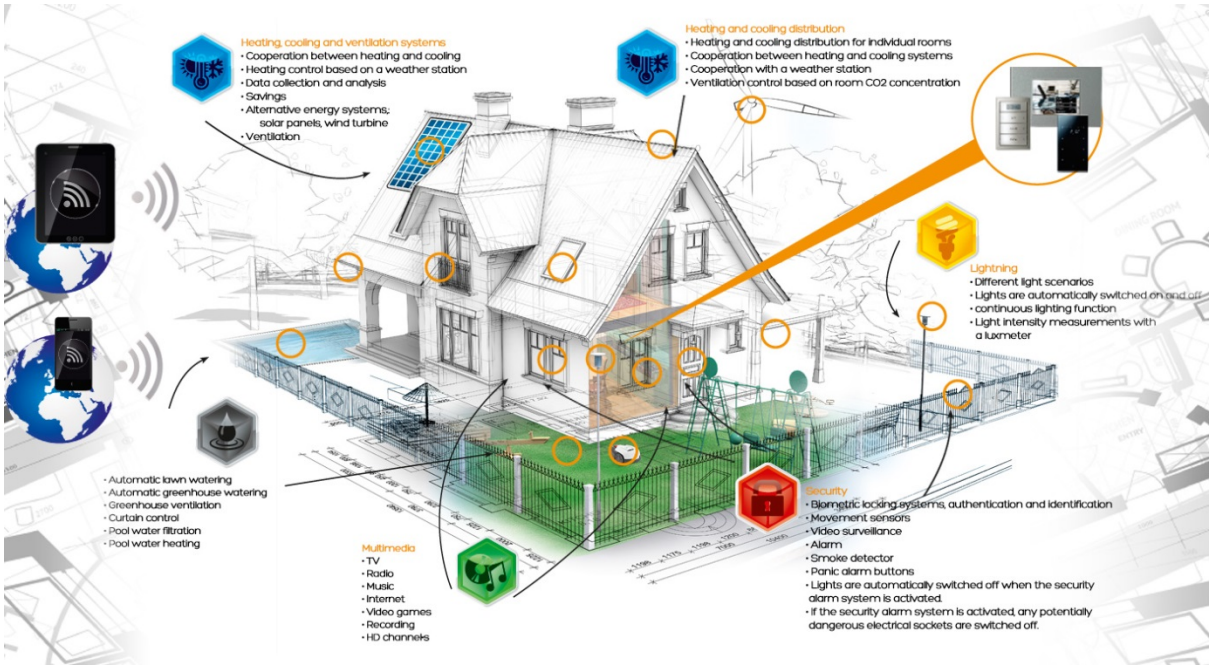


Figure 22: Smart Home Source: (Nutihouse)

All devices are capable of sending information to each other and of responding to the environment. Even if the smart home is set up in such a way that the information always stays in the private sphere, so the collection area is limited to a local area network, there is a chance that someone breaks into or eavesdrops on the communication network. As written in the basic concepts chapter the current sensor topologies are not very secure yet, so it is currently not that difficult to break into a sensor network to gain access to a node or even the sink. And with security it is always a matter of time until someone finds the leak. The range of the communication technologies is determining the range of accessing a node directly. KNX technology has for instance a range of 800m. This means that an intruder could get direct access to this node from 800 meters away. If you can gain access to the sink of the network then you could eavesdrop on all the packages send to and from the sink. Eavesdropping, also called wiretapping or sniffing, can be done with some wireless receivers that are placed outside the home (Chan & Perrig, 2003). Eavesdropping can for instance be done on a wireless WIFI router. Even though the information content might be encrypted, the traffic data that becomes available can already reveal lots of information. It can for instance reveal what kinds of devices are used for the communication.

There are programs that make eavesdropping very easy. An example of such a program is Wireshark. A session has been run with Wireshark on the wireless WIFI router of a private home at a random time. A small part of this session can be seen in Figure 23. By analyzing this kind of data a lot can be revealed. You can assess what kinds of devices are present in the network and what kind of packages they are sending. If these packages are not encrypted you could actually see what was send. Unfortunately, no IoT devices were present in this network but if they were connected through the network, you could have seen those devices sending packages to each other. That information from a WiFi router can be useful for different parties has become clear from a Google case. Google was sued for the fact that their Google street view cars were also collecting information from WIFI routers while driving through the streets, in the end they settled for 7 million dollars for the complaints in the US (pcworld, 2013).

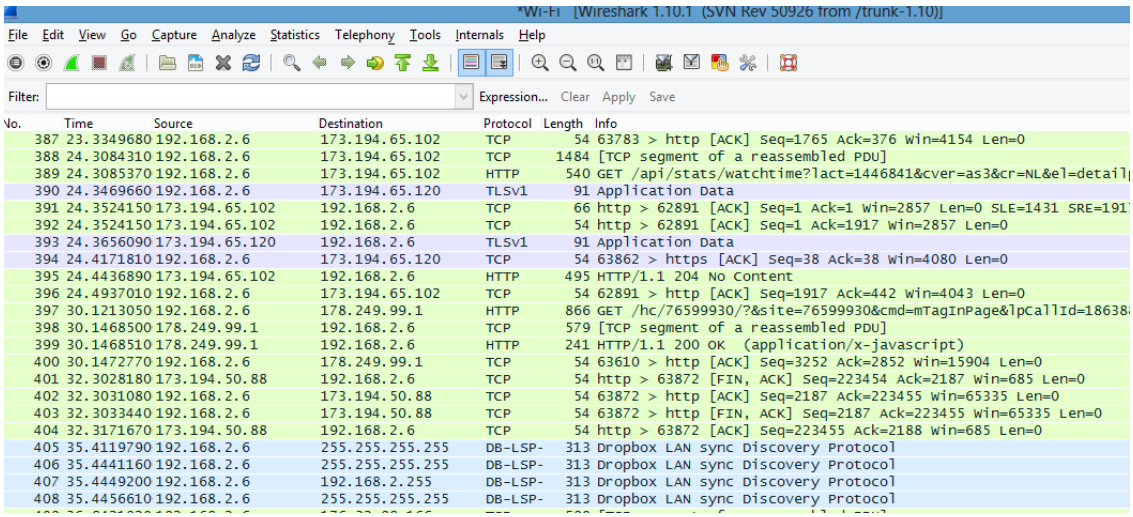


Figure 23: Wireshark Session

The point being made here is that with the use of sensor technologies inside your home or body others can also gain knowledge about things that are going on inside your home or body, even though the intention was to keep the information in the private sphere. Let us consider yet another example. If someone weighs himself everyday on an offline scale and writes down his weight on a piece of paper, then the only possibility of someone else to gain knowledge about this weight without asking, is to break into to home and steal or copy the piece of paper. With a scale in the IoT the scale could, for instance, send the weight automatically towards a smart mobile device like a smartphone that creates graphs of the weight progress. Another person could eavesdrop on the communication send by the scale, to gain knowledge about this and the data subject would never have to know about this. If the offline note was stolen or copied however, you would see traces of an actual break in.

At this moment, the first threat of the IoT can be identified:

Threat 1: By embedding computer and communication power in things inside, or attached to, our bodies and homes it becomes possible to eavesdrop on private information collection from a distance, thereby gaining knowledge about data traffic and/or even content data stemming from a home or a body, that was until now hidden in the private world.

In case information from one of the layers of the privacy model, taking the human body as a starting point, has become available through eavesdropping, the privacy rights of article 11 or 12 are violated. Article 10, general right to privacy, is also violated since personal data is collected without your consent. If the smart home environment is managed through a private network, then no privacy rights could be claimed from article 13, privacy of communications.

6.1.2 Information collection by registration

If the collection is done through registration, the information is not collected by the data subject itself but by an external entity. This external entity can be the government, an organization or a private person. Registration is different from eavesdropping, which was discussed above. Eavesdropping takes place if someone takes note of a private communication, whereas with registration the data is collected directly at an external data holder. Again, some example scenarios will be used to show the differences between registration in the offline world and in the world with the IoT.

Walking down the street

You could walk down the street, look at all the people that you see and write down what they look like and describe the clothing that they are wearing. But we can only collect the information that we are actually seeing. And most of us would probably only be able to tell what kind of jacket someone is wearing and not know exactly the brand or the size of the jacket. The person wearing the jacket is aware of the fact that others can see his jacket. There is no way however to see with the naked eye what is inside the purse of a person, to see what underwear the person is wearing, or what kind of tattoo he has on his back. The individual in question therefore has at least a reasonable expectation of privacy for the things that cannot be seen with the naked eye. As discussed in the first chapter however, RFID technology is designed to register objects without having the object in sight. In the retail business EPC codes can be used with RFID to replace the traditional barcodes. Since

there can be an enormous amount of different EPC codes, literally all items in this world can be identified. This means that while you are walking down the street with an RFID reader all things attached with an RFID tag can be identified. And if those things have an EPC code then a person with an RFID reader would not just be able to see the jacket but would be able to see exactly what you are wearing, where you bought it and what your sizes are. This is illustrated in Figure 24 where someone gets a complete overview of Mr. Jones by scanning his RFID tags. A relevant aspect here is the range of the RFID tag. Only RFID readers in this range are able to scan the tags.

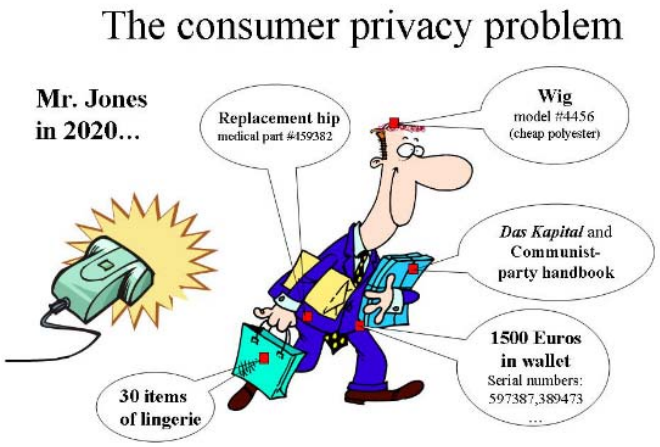


Figure 24: The consumer privacy problem of Mr. Jones **source: (Juels, 2005)**

Passive RFID tags that would probably have been used in this scenario due to its low costs have no way to encrypt the information so all RFID readers would be able to get the EPC codes. One of the principles of RFID is that it uses the power from the reader to send something back. Therefore, the RFID tag cannot be turned off, it is always available for RFID readers. And this "transaction" does not leave a trace at the RFID tag site; the traffic data is invisible at the tag site. You as an owner of the RFID tag will therefore never know that the RFID reader scanned your tags. And since the size of RFID tags are so minuscule you do not even have to know that they are present in your clothing. With this example, some threats of violations can be identified.

Threat 2: An RIFD tag that contains an EPC code can give away lots of detailed information about objects worn on the body or that are present inside a home.

This is a threat since this was not possible in the offline world. It has become harder to keep certain information, belonging to your body or home, confident. Not everyone likes to share their size or the brand of their clothing, for instance, since one might feel insecure about this, or just feel that this is nobody else's business. One could argue that this information could still be assessed by others, but effort has to put into this so the mischance principle does not apply, therefore people have a reason to suspect privacy with respect to this kind of detailed information. With an RFID scanner, detailed information about the items can be revealed instantly. Since information that is stated in one of the layers of the privacy model taking the human body as a starting point can be revealed there is a violation of constitutional privacy rights.

Threat 3: RFID scanners can also scan tags of items that are not visible with the naked eye.

This is a threat since it becomes impossible to keep certain things private by just covering them up. Your reasonable expectation of privacy does not match with your actual privacy. This threat is actually making threat 2 even larger, since also detailed information can be revealed of items that were supposed to be hidden from the naked eye.

Threat 4: Information from a body or a home can be registered unobtrusively with the use of RFID tags.

In other words, the data traffic in the direction of the data subject is not visible as can be seen in Figure 25. This is a problem since there is no way for the data subject to know when information about him was collected and by whom. In article 12, it is explicitly stated that in case of a search warrant the person in question should be notified. If the home is searched with this technology however, the data subject does not even have to find out that a home search has taken place.

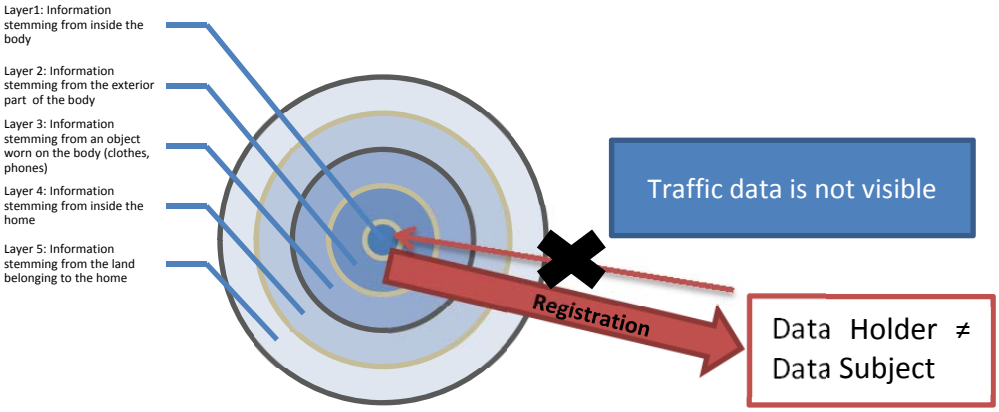


Figure 25: Traffic data is not visible for data subject

Threats 5: RFID tags can be embedded unobtrusively without your knowledge.

This is a problem since it might never occur to a data subject that information about him can be registered. This is especially a problem since RFID tags can be extremely small. In the basic concepts chapter RFID powder with a size of 0.05 by 0.05 by 0.005 mm was discussed. This powder but also regular tags with a size of 1 by 1 by 0.18 mm are not visible with the naked eye. Therefore, these tags could be placed on items without the owner of the items ever finding out that there were RFID tags attached to them.

Threat 6: Information can be registered without your consent

This follows directly from threats 2 and 3. Since the information can be registered without your knowledge this can be done without your consent. This is a problem since there is a

probability that information is collected where you would have never giving your consent for.

Threat 7: RFID tags are always on, you cannot disconnect them

This is a problem since you cannot choose to not send information. Just consider for instance the discount card of a supermarket. A traditional discount card has to be scanned. If you buy certain items that you do not want to be associated with, you can choose to not give your discount card. However if your customer card would be scanned automatically you only have the choice of always being scanned or to not participate in the discount program.

Very similar to eavesdropping, hackers can get access to devices in the IoT to register their information. During this research, many news articles were written about hacks on IoT devices. One example is for instance the smart meters that were hacked by German researchers, thereby even revealing what kind of television show the people where watching (Mocana, 2012). This hacking is another threat to the constitutional rights since it can reveal information belonging to one of the layers of the model taking the human body as a starting point.

Threat 8: IoT devices can be hacked, thereby revealing information that belongs to a human body or a home

This is a problem since very private information is thereby revealed without your consent or even your knowledge. One could say that the hacking of devices is actually a security issue and not a privacy issue. However, your privacy cannot be guaranteed if others can access systems that are meant for private use, because the system is not adequately secured.

Currently in the offline world when an entity wants to know something about a person's body or home and collect the information by itself, so not by dissemination of the data subject, it has to be near the human body or inside the home. With the true vision of the IoT were all things are connected with its own IPv6 address this collection by registration can take place from anywhere, at any time in the world.

Threat 9: If all things are connected through an IPv6 connection the range of information collection is unlimited, it can take place from anywhere at any time in the world.

This is a problem since in principle your information can end up anywhere in the world. This means that you can become a victim of violations of privacy rights from anywhere in the world.

6.1.2.1 Function creep

Another threat related to registration is called *function creep.* This basically means that when a system is designed to do one thing, it might later also fulfills other purposes. As EPC global states on their website about privacy concerns, EPC tags are meant for managing products and are not build for tracking people (EPC Global, 2007). As has been discussed in the basic concepts chapter the EPC codes on the RFID also have enough bits for each item to have its very own identification number. Therefore, two exact pieces of clothing can still be

identified separately. Many papers have been written about object tracking with the use of RFID, (De, Basu, & Das, 2004) show for instance how tracking with RFID tags can be done real-time. RFID is not only ideal for products, it can also be used to recognize or even track persons. If someone wears around 10 pieces of clothing there are 10 unique identifiers that could all be linked to the same person. Every time one of these items is worn again, this person can be recognized, and the unique numbers of the other items can be added to this dataset. You can then create very large databases of unique numbers belonging to one person. Thereby a person can always be identified. If one of these numbers has ever been associated with your name, then it will exactly be known who you are. If the link has not been made with your name you can still be recognized in the sense that they know things about you. They can know what you were wearing last time for instance, and this can be useful in stores by example. If a person looks at a certain washing machine in a store and there is RFID scanner nearby, it can be recognized if one of the unique numbers of the items worn on the body has been scanned there before. The store can then decide to give you a little discount to persuade you to actually buy the washing machine. This can be compared to the advertisement that is already happening on the internet, where you get dedicated advertisement based on your previous search queries. From this the following threat can be identified.

Threat 10: RFID tags can be used to identify persons

If you are always recognized you can never really be left alone anymore. This is closely related with the definition of privacy of Warren and Brandeis. Normally when personal related information is processed this has to happen in compliance with the WBP so the consent of the data subject has to be given. Since all this registration happens unobtrusively, you as a person do not have to know that you are being registered. Although consent must be given, it is hard to control if this is actually happening. Since RFID readers are not that expensive it is a possibility that all companies and organizations use RFID to track persons. And even if RFID tags would be encrypted, this would not solve the problem, since even the encryption can serve as a unique number that can be used for identification.

6.1.2.2 Big data

In the IoT where all things are linked with each other through applications and services, this will add lots of new data in the databases. The availability of information about a body or a home will also lead to more storage of this kind of data. In this data, lots of valuable information can be present. Many companies are working very hard to build all kinds of algorithms to make use of all this data availability, and to create something valuable with this data. In the book Super Crunchers many examples are given about what algorithms could predict, both for current and future situations (Ayres, 2007). One the applications of big data algorithms is profiling of customers, which could be done in combination with the mentioned identification technique of the previous section. In the US, a supermarket named Target has algorithms that can predict the purchasing behavior of its customers, and with the use of the algorithm, coupons are send to the customers to persuade them to do certain purchases. This algorithm is so smart that it even knows if a woman is pregnant, just by the change of products that are bought, like scentless lotion instead of scented lotion. At one point an angry father came into the store after his high school daughter received coupons for baby supplies since his daughter could definitely not be pregnant, but it turned out the

algorithm was right (New York Times, 2012). Just imagine the kinds of big data that are present if all things in daily life also start to share information about our bodies and our homes. Very recently, the new chairman of the Federal Trade Commission (FTC), the US organization that protects consumer rights, has stated that the FTC will be stricter towards large companies, that have fast amounts of data available, in respect with the use of big data algorithms that could be violating privacy rights (The Verge, 2013). However, time will tell whether this actual leads to less privacy violations by these companies.

Threat 11: Algorithms in the IoT can reveal lots of personal information about you

These algorithms are violations of privacy rights since even if certain personal data has not been giving they can still be deducted from all the information availability. For instance if you never told anyone about a disease that you have, this might still be deducted from all the information coming from location data when visiting the clinics, items bought for your treatment and so on.

6.1.3 Registration in replacement of conversation in the collection stage

In the basic concepts chapter it was stated that the smart grids could be seen as an example of the benefits of the IoT. In the movement towards the smart grids, energy companies already started to offer smart meters inside the homes. In the offline world, your energy consumption is collected inside your home and once a year someone from the company comes to collect your usage, he writes down your usage and you have to sign the form to show that you agree with this number. It is very clear for both parties what information is taken back to the energy company. With the smart meters however, your energy consumption is directly registered at the energy company. Technically speaking the data is first collected at the home but it is directly forwarded to the energy companies. Although this can be very useful, you also lose control over what exactly is stored. It also becomes possible to see if people are at home and what kind of electrical appliances are being used (Cuijpers & Koops, 2008). This shift from conversation towards registration can be seen a lot in the IoT since everything can be registered automatically. Your scale could automatically register your weight in an application, your GPS automatically registers your current position, and an OV-Chipkaart automatically registers you “checking in”. All this registration is making the IoT a lot more convenient in its use, but you keep less control over what exactly has been registered. An overview of this shift is giving in Figure 26.

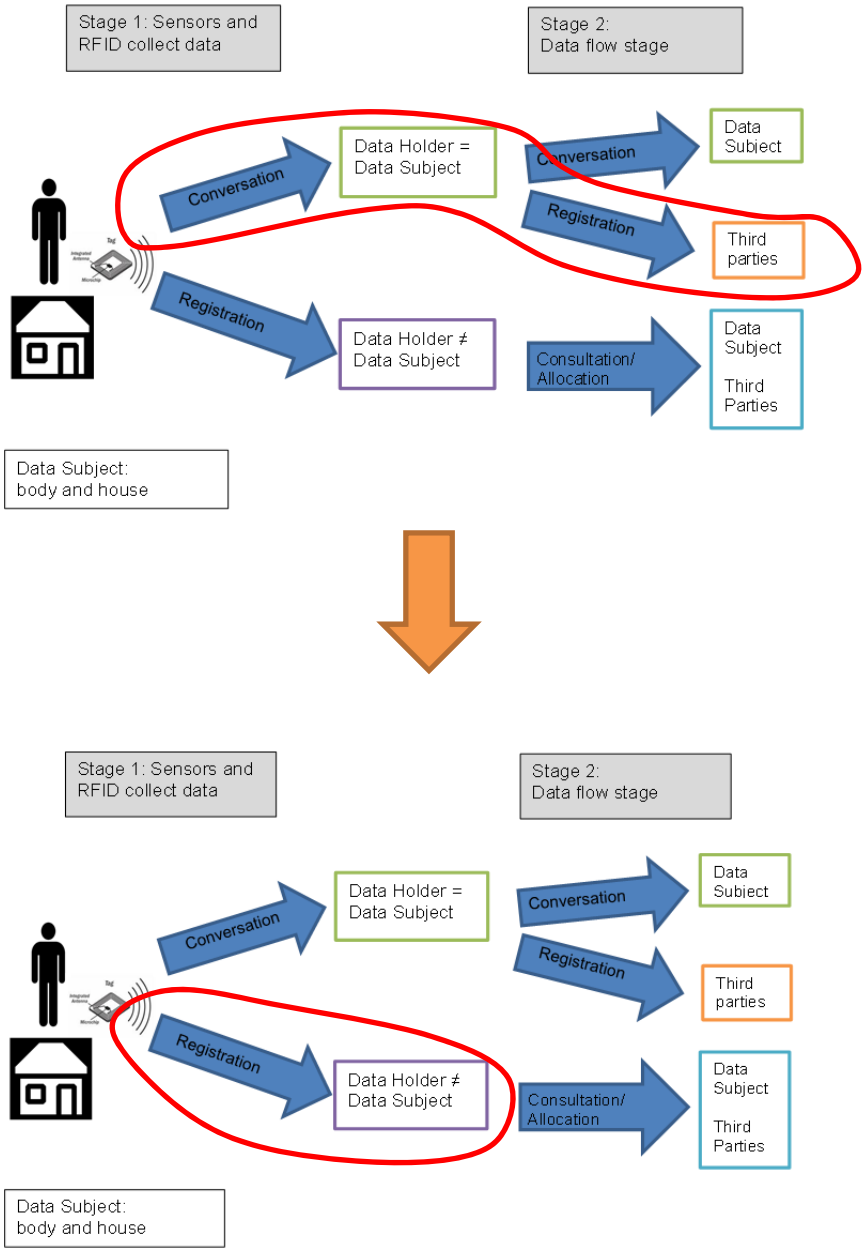


Figure 26: From registration trough conversation towards direct registration

6.2 Data flowing stage

After the data collection stage, you have the data flowing stage. This data can be forwarded by the data subject itself if that person is the data holder or it can be forwarded by an external data holder. As argued above the data flow path to reach an external data holder has changed. Before the IoT, the path followed data collection by the data subject itself towards dissemination by registration. With the IoT, the data can be collected directly at an external data holder. What external data holders can do with the collected data besides processing it for their own purposes will briefly be discussed below.

6.2.1.1 Combined datasets

Function creep can also happen with information that has been registered with your consent. You give your information with consent for a certain purpose but then it is used for another purpose, or combined with another database (Prins, et al., 2011). The combination of databases from different sources can feed algorithms of big data with even more information. In the months May, June and July of 2013 the software program Collusion was ran on one of the computers where this thesis is written on. This is add-on software of the internet browser Mozilla Firefox. It tracks who is collecting what data about your internet usage. Much information was sent to websites that were never visited. And it can be seen that several websites that were giving consent, by accepting cookies, did forward some information to other websites that were never visited.

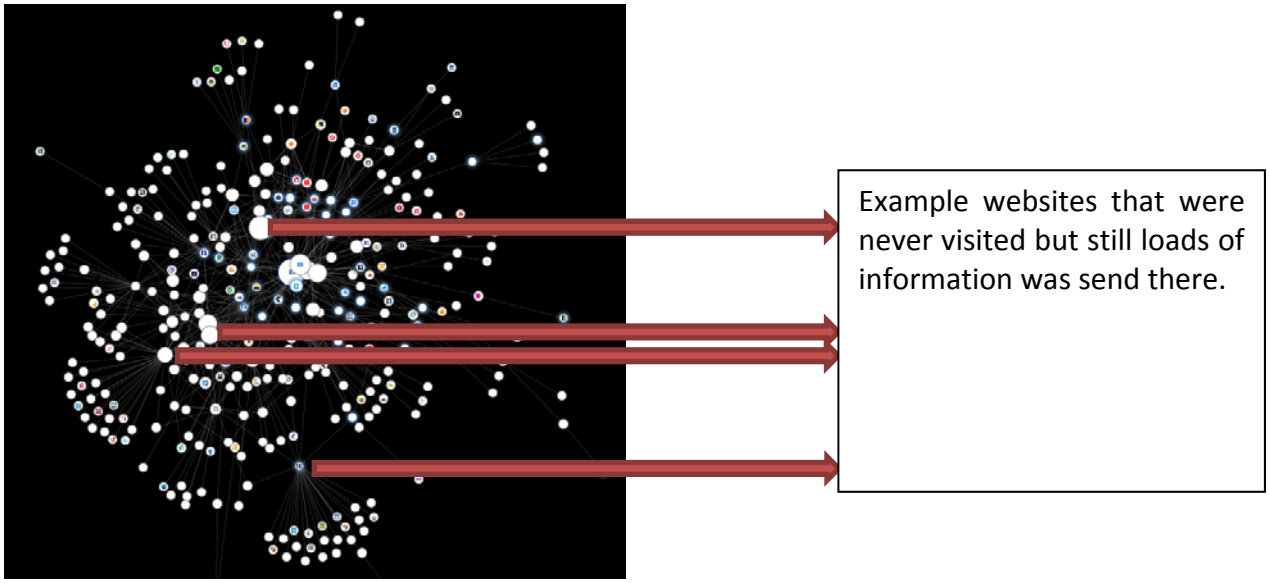


Figure 27: Overview of collusion

Of course, this research is about the IoT and not about the usage of internet browsers. But it serves an illustration of the fact that databases are linked with each other. Especially for advertisement purposes, information about homes and bodies can contain very valuable information. Therefore, it is very likely that companies are willing to pay money for this kind of information. During a visit to an energy company, it became clear that they are looking for ways to combine more datasets with other companies so that their data becomes of a greater value. With all this combination of different datasets, it is difficult to make decisions of whom you should provide information. It is okay to share your information with albert.nl to make sure that your groceries are delivered. But what would happen if they decide to combine this information with the health insurance companies to see what type of products lead to certain diseases. Although this could be relevant to gain certain insights, the health insurance company could maybe decide to use this information in another way, to raise your monthly fee for instance. This third party sharing of information is often legal, since it is described somewhere in the agreement that the company will do this, so people gave their legal acceptance without overseeing the total consequences. People might have thus giving

their legal agreement by clicking the accept button, but this does not necessarily mean that there was an actual “informed consent”.

6.2.2 Criminal investigations

Data flows to third parties are not only useful for advertisement reasons, but data from the IoT can also be very relevant in the light of criminal investigations. The Rathenau institute did a research in 2007 on the use of information by officers in the detection and safety field. They found that these officers have access to more and more information by law. This information gathering is not only restricted to actual suspects but also to people somehow related to potential suspects. Also, these officers often force other parties to give their information for investigation purposes (Vedder, Wees, Koops, & Hert, 2007). All five layers in the privacy model, taking the human body as a starting point, contain information that can “offline” only be legally revealed by a home or a body search. These searches can only be done with a good reason as stipulated by law and these searches cannot be done without your knowledge about this. However since in the IoT information, about your body or home, can be send digitally, it is a possibility that in case of a criminal investigation, investigators do not come to your home to see if you are there. Instead, they could call the energy company to ask if you are home, or ask the internet service providers if you are making use of certain application in your home. The minister of safety and justice Opstelten is in the process of passing a law that makes it possible to hack automated processes for criminal investigation (Rijksoverheid, 2013); this will include the IoT. But with the IoT, this would give them much information about what is going on inside the home, with this law it would be possible for criminal investigators to look into a home without physically being there. Before the IoT, this would only be possible with a search warrant of the home. In the search warrant of the home, the person who it concerned has to be notified. As can be read in the accompanied report of the proposed law, secretly wiretapping of the communication belongs to the authority giving by a warrant that was giving with respect to this law (Opstelten, 2013).

6.3 Physical interference

In conclusion to the data flow model and its threats it can be said that it is a problem that much information about the human body and the home is collected by registration and that this can happen unobtrusively. You lose control over your information. People do not know what exactly is collected about them and they do not know what happens with this information. Information belonging to one of the layers in the privacy model, taking the human body as a starting point, should be taken with care as has been argued. Although this research focused on the informational availability of this kind of information, there are also threats of violations of the rights of inviolability of the body and home in physical ways. As stated in the basic concepts chapter, the systems in the IoT are not very secure (yet), therefore they are easily hacked. If certain things in the IoT are not only contained with sensors and RFID tags but also contain actuator, which is the case in smart sensors, it not only becomes possible to obtain information but it also becomes possible to send commands to the actuator. On the website Forbes it could be read how people are able to easily hack into a person’s home and switch the lights, turn on the hot tub and even open the garage doors, while being miles away (Hill, 2013). The IoT can therefore actually lead towards physical interference. Also if it is possible to scan what items are present in the home for instance with RFID tags and camera sensors in the home, criminals could select what home is worthy of breaking in. And also on the street people could see which purses

have the most valuables. Physical interference inside a body is also possible if it is enhanced with IoT technology. Hacker Barnaby Jack showed that it is possible to actually kill someone with a pacemaker or an insulin pump since both of these made use of wireless communications (Reuters, 2013). In conclusion, the availability of information in one of the layers of the privacy model, taking the human body as a starting point, can eventual lead to a physical violation of the privacy rights.

6.4 Inviolability of the home and the body and threats of violation

It can be concluded that constitutional privacy rights are indeed threatened to be violated by the IoT. The inviolability of the body and the home are both threatened to be violated, by technologies in the IoT, in an informational and in a physical way. Several ways of how these rights can be violated are identified. A privacy invasive model was created taking the human body as a starting point in combination with the privacy rights. It has been argued that it would be a greater privacy violation if information was shared from an inner circle. In the offline world, there are stricter rules to gain information from these inner layers. In case of inviolability of the body, internal examination could only be done by a doctor, while the search of items worn on the body could also be done by security staff at a concert for instance. And in case of inviolability of the home it is even arguable if the outer layer would deserve protection from this right at all, so the outer layer should get the least protection. While in the "offline" world a classification of these different layers exists, in the IoT, the same kinds of technologies are used to collect information in all of the layers. With the example of the pacemaker, it was already seen that the most inner circle could be violated even in a physical way. From this, it can be concluded that the offline world does not match the world with the IoT in relation with the protection of privacy rights.

If one would look at the threats as described in this chapter separately then it might be concluded that each threat separately is not that severe. If one would take the sum of all the threats than the threat posed by the IoT is very high. Although the word "threat" has been used in this chapter, some of the threats are actually already happening; violations of privacy rights are already taken place. Through the IoT, it is possible that information about our home or body is collected without our knowledge. Since the size of RFID tags are very minuscule they can be attached to our things without our knowledge. RFID tags do not need a battery so they are "switched on" forever. We could be identified with all the tags that are placed on items that we carry with us in daily live. All this information availability could eventually also lead towards a physical interference. Since sensor and tags make it possible for external data holders to directly register information from the source it is not transparent what exactly is being collected. Algorithms are now being fed with very personal information and are therefore capable of deriving information that you might not be willing to share with others. These algorithms could even be used to predict things about the future. If the law proposed by Opstelten is passed, then the government could legally spy on automated processes of citizens in the light of criminal investigations. Thereby information of the body and the home could be collected while avoiding the notification that is needed when a home or body search is done. One could argue that this spying could only be done with a warrant, but who is going to control the government? As we have seen this eavesdropping could even be done without the data subject knowing about this from the other side of the world. How would one be able to sue the government for illegally

espionage if it is not known? As has become clear from the program PRISM, some governments really are eavesdropping on private communications. What would happen if the government would actively start to profile citizens, to assess whether one can be related to criminal offences? One might even fear that these algorithms become so smart that they could actually be used to detect the act of committing a crime before the crime has actually be committed, which was the case in the Hollywood movie Minority Report. Algorithms could derive incorrect information about citizens though. During this research, many search queries where used that could be related to criminal activities, while there is no intention at all to commit such a crime. Privacy is related with personal freedom, personal choices and therefore also with being an individual person. These algorithms are concerned with finding the similarities between different people however. In court ruling, the term “reasonable expectation of privacy” is used. But what if it becomes so common that all information about our bodies and home can be collected that we cannot expect privacy at all anymore? It has become clear that the IoT is capable of violation the constitutional rights, but nevertheless IoT are being developed and implemented at a large scale. In the next chapter it will be discussed if this deprivation of privacy could be ethical justified or that we should change the technology.

6.5 Main points of this chapter

Main points of the chapter threats of violations of constitutional privacy rights posed by the internet of things

- In the IoT, there are threats of violations of privacy rights that were not present in the offline world.
- Threats identified in the data collection stage are:
    - By embedding computer and communication power in things inside, or attached to, our bodies and homes it becomes possible to eavesdrop on private information collection from a distance, thereby gaining knowledge about data traffic and/or even content data stemming from a home or a body, that was until now hidden in the private world.
    - An RIFD tag that makes use of an EPC code can give away loads of detailed information about objects worn on the body or that are present inside a home
    - RFID scanner can also scan tags on items that are not visible with the naked eye.
    - Information from a body or a home can be registered unobtrusively with the use of RFID tags.
    - RFID tags can be embedded unobtrusively without your knowledge.
    - Information can be registered without your consent.
    - RFID tags are always on, you cannot disconnect them.
    - IoT devices can be hacked, thereby revealing information that belongs to a human body or a home.
    - If all things are connected through an IPv6 connection the range of information collection is unlimited, it can take place from anywhere at any time in the world.
    - RFID tags can be used to identify persons.
    - Algorithms in the IoT can reveal lots of personal information about you.
- There is a shift from conversational data collection towards data collection by registration.
- In the data flowing stage, it can happen that information from different datasets is combined. Therefore, your information can end up a third party you did not want to have your information.
- Information brought by the IoT can be used for criminal investigations, thereby neglecting the inviolability of the home and the body.
- Physical interference with the body and home is also possible in the IoT.
- If the sum of all the threats are taken it could be said that the threat of privacy violations by the IoT is very large.

7 Ethical Reflection

In the previous chapter, it has been concluded that constitutional privacy rights can be violated with the use of IoT technologies. More specifically, it has been argued that the rights to inviolability of the body and the home can be violated through the IoT. The technique has possibilities that do not match with the values that are present in our constitutional rights, and these rights are part of the constitutional law, which is the supreme law of the Netherlands (Parlementair Documentatie Centrum van de Universiteit Leiden, 2013). This is a problem since if nothing is changed there will be lots of technology available, and being developed, capable of violation our constitutional rights, thus there will be lots of regulating issues. As Engelfriet already mentioned, technology and therefore the possibilities change very fast so it is very hard for regulators to keep up (Engelfriet, 2013). There are two extreme ways of solving this issue, namely changing the technology to match our present privacy values or adapt our privacy values to the upcoming technology. An overview of these options is given in Table 6. In this chapter, both of these options will be discussed as an ethical reflection on the whole privacy issue raised by the IoT. The last part of this chapter will discuss a third option where there is more room for users to decide for themselves what they find acceptable. During this chapter, some possible solutions to the threats posed by the IoT will be discussed shortly.

	Technically possible	Not technically possible
Allowed by privacy law	Law and technique comply	Law and technique do not comply but there is no problem of regulating the technology
Not allowed by privacy law	Law and technique do not comply and there is a problem of how you are going to regulate the technology	Law and technique comply

Change values

Change technology

Table 6: Technique and law do not comply

7.1 Changing our values of privacy

Undoubtedly, technologies have an impact on the way society is shaped. Just recall the changes brought by the industrial revolution or the internet. Winner argued that it is also the other way around, existing values also having an impact on how technology is designed (Winner, 1980). Spahn has given an overview of how philosophers and anthropologist, in different disciplines, have reasoned over time about the relation between humankind and technology. One of the findings is that the underlying debate of these different reasoning is centered on focusing on the negative versus focusing on the positive consequences of technologies, although this opposition has become more balanced over time (Spahn, 2011). One could argue that so far in this thesis the focus was more on showing the negative consequences of technology in relation with our privacy rights. The IoT also has many

benefits to other values we have in our society like decent healthcare, economic growth and sustainability. These values are certainly worthy of pursuing as a society. If one would reason by the utilitarianism theory of Bentham and Mill, then it can be concluded that (in extreme cases) it can be ethically justified to ignore human rights, as long as the positive outcomes overshadow the negative outcomes. Bentham takes a quantitative approach in the sense that if more people have benefits from option 1 than from option 2, then option 1 should be preferred (Royakkers, 2004) (Bentham, 1789) (Mill, 1863). This way of thinking can for instance be found in the arguments by Posner, an influential judge in the US, who argues that personal privacy does not maximize wealth; instead, personal privacy is actually economically inefficient for the society (Posner, 1978). Posner has more recently stated that the social benefits of privacy are of less value than the value brought by public surveillance, since this surveillance can aid in preventing criminal and terrorist activities (The Wall Street Journal, 2013). That national security should be seen as a larger value than personal privacy has been uttered a lot especially since 9/11. The IoT has the capability of adding much new data that might aid in increasing national security, it can therefore be argued that personal privacy can be limited for this national goal. The IoT could even be seen as a panopticum (Russ, Hesse, & Müller, 2008), that makes sure that we do not engage in criminal or terroristic activities behind our closed doors since IoT technologies also have information about what is going on inside the home. As discussed, in the second paragraph of the new proposed article 13, privacy of communications, it is even explicitly stated this privacy right could be limited in the interest of National Security. To what extent privacy should make room for national security is however very debatable as can be read for instance in (Vedder, Wees, Koops, & Hert, 2007) (Cleiren, 2009). Since the news of the program PRISM came out, the discussion has been fed again and many opinions in newspapers seem to direct in favor of privacy as can for instance be found in (Trouw, 2013) (The Wall Street Journal, 2013) (Liga voor mensenrechten, 2013). But despite these opinions, it is argued that programs like these are vital for natural security, the head of the FBI even stated that the program was within the boundaries of the law (AD, 2013).

If a societal perspective is taken then it might be concluded that the benefits of the IoT are of greater value than the dangers of losing some personal privacy, since it can bring things like national security, sustainability, better healthcare, efficiency and economic growth. If this kind of reasoning is followed then it is indeed plausible to adapt our value of privacy since the benefits of the IoT outweigh the negative consequences. During this research, it has become clear that privacy values are already changed by the use of the internet. Many people choose to willingly give up parts of privacy in favor of connecting to others on social network sites for instance. However, as discussed, privacy is also violated unwillingly and even unnoticed for instance by companies who exchange data to maximize their profits. Some companies are now giving customers a store discount in return for their private information, for instance by giving them a personal store membership card. Research shows that without governmental intervention privacy will continue to erode, since privacy becomes too expensive to maintain (Rust, Kannan, & Peng, 2002). Some people even note that privacy does not exist anymore and see the notion of privacy as something negative, namely as a willingness to hide certain things.

Cheng et al. noted, that systems that have the capacity to store data from personal sensors, which can be seen as total recall systems, will inevitably change the notion of privacy, since

no one is going to stop collecting this kind of data if it is up for grasp. These systems can be beneficial; we just have to deal with the consequences (Cheng, Golubchik, & Kay, 2004). If this option is followed, and humans accept the fact that privacy rights may be limited in favor of other respectable values where the IoT can contribute to, then privacy is not seen as a natural right but merely as a legal right that could be overruled.

Maybe it really is inevitable that we have to change our views on privacy and our expectations of privacy due to the new possibilities brought by the IoT. However, this does not solve the problem entirely because we are still left behind with questions. The first question is to what extend we should change our value of privacy. As discussed in the previous chapter all this information availability about the home and the body, can eventually also lead towards physical harm of the body and the home and this is something that would not be acceptable by the liberty principle of Mill (Mill, 1863) (Royakkers, 2004). Should we only give up our privacy to the government and other organizations that can prove to bring benefits from it, and still protect it on horizontal level between civilians? It would be necessary to discuss what values are actually seen as a more important value than the value of privacy. In the 112 example, it can indeed be said that the value of life overshadows the value of privacy, so it is morally acceptable that your location data is automatically shared with emergency organizations to potentially save lives. But is the value of maximizing profits of companies in favor of privacy also morally acceptable? One could argue that maximizing profits of companies is beneficial for the society as a whole since it can lead towards economic growth. However an argument in the opposite direction could also be made, that just a few people will benefit from this and therefore it could not be morally justified.

Another question that remains unanswered is if it can be proven that the IoT is contributing to those other values. Beatrice van der Graaf has argued for instance that all the information stored for national security, not necessarily lead to more safety. She pointed to the fact that there are also instances where all the information was known but somehow unnoticed, and the terroristic attacks still happened (de Graaf, 2013). And can it also be morally justified if information is collected from a body or a home without the person knowing about this? The last question that remains open is who gets to decide what value is seen as being more important than another value. This is especially important since a physical border does not limit data traffic. The jurisdiction about privacy is different though across these borders, as mentioned in the legal chapter there are already many differences between Europe and the US. Therefore, this value trade-off could not be made within the boundaries of a democratic state.

7.2 Changing the technology

The other option would be to adapt the technology to match our current privacy values as present in the constitutional rights. Maybe it would even be possible to keep the benefits of the IoT while adapting the technologies in such a way that privacy is preserved. Nissenbaum argues that many authors have showed that deprivation of privacy not only affects the value of privacy in itself but also affects other values like freedom, autonomy, democracy and relationships in a negative way, therefore privacy should be protected in order to preserve

also those values. Privacy can therefore not only be seen as an intrinsic, but also as an instrumental value (van der Poel, 2009). Since the IoT is capable of collecting information stemming from the body and the home, it can give away information about very personal choices; therefore, it is interesting to look at privacy from the perspective of autonomy.

One of the core elements of the theory of Kant is *autonomy*, which means the ability of each human to rationally decide what is good for them (Kant, 1785) (Royakkers, 2004). Becoming an autonomous person is a very important element of growing up, there are three important elements of autonomy namely emotional, decision-making and value autonomy, which enable us to feel, think and make decisions. Even as an adult, we keep on growing as an autonomous person (Russell & Bakken, 2002). Research has shown that privacy is very important for autonomy since it gives you room to experiment without the fear of being socially punished for your actions (Nissenbaum, 2004). But if we make all of our actions in our homes visible, it would even become hard to freely experiment in our own homes. If an adolescent is home alone for instance, and is supposed to learn for a test the next day, but instead decides to watch television, he might learn the value of studying when he gets a bad grade. Maybe it takes a couple of times before this lesson is learned but if it is learned, this adolescent has become more autonomous. In the scenario where the adolescent lives in a smart home, his mother might see from her work that the television is on, therefore the adolescent might be afraid to do this and decides to study. Although this seems like a good choice, this is not an autonomous choice.

Autonomy is closely related to freedom, since if we have the ability to decide for ourselves what is good in what situation then we can truly be free. Rössler makes an argument that the ability for each person to decide for themselves how they want to represents themselves in certain situations is very important. Respect for one's privacy is respect for one's autonomy and this is not only important for the person in question but also for the society as a whole since a democratic society is based on the existence of autonomous persons (Rössler, 2008). With this being said, we have returned to the definition of Westin that privacy is the control over what to disclose to others.

Since privacy is such an important value, it is wise to explore the possibility that technology incorporates privacy. Nissenbaum proposes the concept of contextual integrity in which flows of information should be appropriate and apply to the norm of the context (Nissenbaum, 2004). If an order from a smart fridge is collected by albert.nl and albert.nl forwards this information towards another company who is actually handling the home delivery, than one could say that contextual integrity is preserved since the information is still used in the same context, namely that of the delivery of groceries. If albert.nl would forward this information to a health insurance company, the contextual integrity is lost however, since the domains of the companies differ. An overview of this is giving in Figure 28.

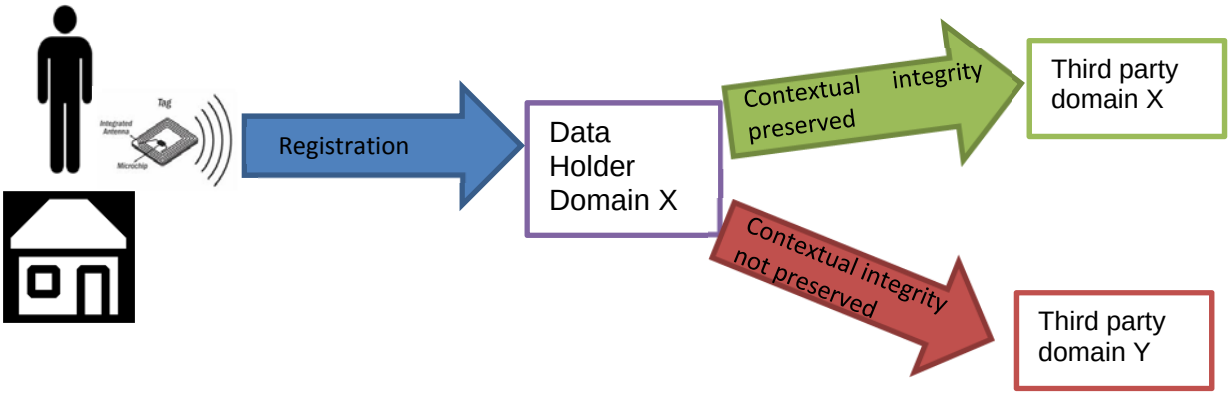


Figure 28: Contextual integrity

If the concept of contextual integrity could be achieved then we could say that we can preserve privacy while keeping the benefits of the IoT. Nissenbaum has so far only giving advice that context-based rules should be made and that those should be embedded in law and rules (Nissenbaum, 2011), however she has not giving a practical implication for the technology yet. If contextual integrity would be built into the IoT technologies, then we would be able to preserve privacy. The IoT is all about understanding the world where it is in, with the use of all of it sensors and such, so maybe it is a possibility to use this information to also preserve privacy. If the technology would be able to understand that your body is in the hospital it is okay that someone reads your heart rate from your heart sensor. If you are in a clothing store it is okay that the lady helping you knows your clothing sizes. To examine whether this could be technically realizable could be a valid follow up study. One could think for instance in the direction of instead of standardizing all the communication protocols into moving towards designing specialized protocols for different circumstances.

Van der Poel points to the process of value sensitive design where values are taken into the technical design progress. In the process, empirical investigations of how users are affected by the technology are an element of this design. The other elements are technical and conceptual investigations (van der Poel, 2009). The EU is trying to enforce this empirical investigation for the value of privacy in the proposed data protection law of the EU. They call it a *Privacy Impact Assessment* (PIA). These PIAs try to find the privacy risks of a specific technology application. These assessments need to be externally validated and they become publicly available (de Hert, Klo, & Wright, 2012). In the Netherlands, the Dutch Data Protection Authority initiated the creation of PIAs for the Netherlands. However the private parties said that they did not want to participate anymore since the proposed method was too complicated and time-consuming (Ministerie van Veiligheid en Justitie, 2011). In addition, some politicians have uttered their concerns that a PIA would just be a bureaucratic act instead of really adding value (Rijksoverheid, 2010). As can be read in the document about PIAs by the Dutch Audit-IT organizations, PIAs are not very suitable for new

technologies since the threats are unknown. Another downfall of PIAs is that they only have to be carried out for systems whereby the system is collecting personal data (NOREA, 2013), and as discussed, sometimes the system is not designed for collecting personal data, but it still happens through function creep.

Another element of the value-sensitive design is the technical investigation. This includes the investigation of new technology mechanisms that could support the values at stake (van der Poel, 2009). Luckily some research has been carried out that could enhance privacy in the IoT. Some technological solutions, also called privacy enhancing technologies, which could reduce the threats of privacy violations in the IoT will be explored below.

7.2.1 Privacy approaches for RFID tags

Juels summarized some solutions for the privacy issues raised by RFID. One of interesting solutions was the killing of RFID tags at retail stores by sending a code to the tag once the item is purchased, since the tag is not needed anymore for stock inventory. This could for instance be done after an automated checkout at the grocery store. The downside of this is that you also loose the benefits that the tag might have had for the customer. For instance, the tags could also have information for the expiration dates of the items that might be useful in a smart fridge. Therefore, it might be a better idea to re-label the RFID tag and remove the unique identifier. Another relevant solution for RFID is blocker technologies that would temporarily block the tags from being scanned (Juels, 2005). It has already been discussed that it is possible to encrypt RFID tags. This would indeed limit the privacy threats of revealing information of the things they are attached to. This would not however limit the threat of being identified since the encryption could also be used as an identifier. However if the tag would be re-encrypted from time to time then it could not be used for identification purposes anymore.

7.2.2 Privacy approaches for sensors

As could be seen in the basic concept chapter, sensors mostly have a larger range than RFID. This makes them more vulnerable since the eavesdropping and direct registration range is larger. And, as has been discussed, even if the information content is encrypted the visible traffic data could still reveal loads of relevant information. The trick is therefore to limit the ability of others to eavesdrop on the communication. This can for instance be done by adding random data to make it harder to systematically eavesdrop on a communication. Li et al. have given an overview of how to preserve privacy in a sensor network, for both the data content itself as the traffic data. They found that there are some techniques available but that they always come at a price; namely energy consumption and accuracy of the data (Li, Zhang, Das, & Thuraisingham, 2009). As described in the basic concepts chapter the power needed for sensors is also determining the size of a sensor node, therefore these solutions are not feasible for all sensor applications. More research on how to preserve privacy of sensors attached to/in the body and the home is definitely needed. Something that one has to keep in mind when thinking about sensors and RFID tags attached to things inside the home or the body is the lifecycle of the things they are attached to. The products in your fridge are changed very frequently, so newer RFID tags with improved security techniques can be implemented very fast. Other items that do not get changed so frequently have to deal with the existing technology longer. A system that is secure at this moment does not mean that is still secured a couple of years later. Newer cars have for instance sensors that automatically open the door when you approach your car. While this

system was probably secure at the time it came out, it is now easy to hack by eavesdropping with relatively cheap devices (AG, 2011).

7.2.3 Making registration visible

The biggest problem with RFID and sensors is that information can be collected without any trace, so as an individual you might never find out that someone else has your information. It therefore becomes impossible to control who has which information about you. A solution for this might be that only tags and sensors are allowed that are capable of also counting the number of times their data has been collected. If you then install a reader, on your phone for instance, that always checks the counting number of your tags and sensors it could register when and where your information was collected because it notices when it is updated. If for instance a certain company tracks you while you are walking inside a store you will become aware that this is happening.

7.2.4 Anonymization techniques

The IoT can bring lots of valuable information that could be used by different parties. Commercial companies could for instance learn a lot about us through the IoT and therefore design products that better match our preferences. Currently information is stored in relation with the customer. However, this information could also be anonymized. Therefore, the information is not related to us personally anymore, but could still be used for data mining. Bayardo & Agrawal describe an effective method in which anonymization is achieved and in which it is not easy to re-identify persons again, which is mostly the problem with anonymization (Bayardo & Agrawal, 2005).

7.2.5 New infrastructure specially designed for connecting things

Some researchers are also exploring the possibilities of the option to have a whole new communication model instead of usage the TCP/IP model of the current internet. This is also called the future internet (Chaouchi, 2010). Maybe it would be easier to create privacy by design in this new system. The current internet is namely designed to enable connectivity; access control only became an issue at a later stadium. How such a system should be developed could be explored further in other research.

7.3 Informational self-determination

Two extreme cases are proposed to deal with the fact that technologies are capable of violating privacy rights. A solution might be found in the middle, where both technology and law are changed to comply with each other. The legal chapter started out with the search of the definition for privacy. It was stated that privacy is closely related to other values like freedom, autonomy and the ability to make your own choices. It was even noted that the most relevant aspect of privacy is that it might vary between persons, context and time.

The best solution to maintain our constitutional privacy rights might therefore be that we let everyone decide for themselves what they are willing to disclose in different circumstances. A recent study by (Knijnenburg, Kobsa, & Jin, 2013) shows that the disclosure behavior of people is very diverse. Some people do share location information but keep information about their interest for themselves. While for others, this might be the complete opposite. Therefore, even if someone is willing to share large amounts of information it cannot be concluded that this person is willing to share all kinds of

information. The control over which information you want to share is thus very important. That is currently very hard to achieve with an RFID tag. An RFID is capable of scanning your interest (derived from the items that you carry with you) but also your location data derived from the act of scanning itself, since the location is known by the reader. Maybe a person would be willing to share one of these kinds of information but RFID is currently an all or nothing technology. Maybe it would be a good idea to build into the IoT that we could easily show which information we would like to share.

If we want to establish that we all get to decide for ourselves what information is disclosed and to whom, information self-determination, it might not be a good idea that information in the IoT is directly registered by an external data holder. It might be better to collect information from sensors and RFID by the data subject itself, maybe on a central device like a mobile phone or a designated computer in our home and that information can be collected from that central device with the acceptance of the user. Then it becomes clear what information is exactly collected by whom. If information from this central device is then forwarded you could include a certain timestamp. If businesses or the government addresses you with certain information about you, they have to include the timestamp of when the information was collected. Then it becomes controllable of who might have forwarded your information without your permission. This would give the data subject a sort of property right on their data. Of course, the central device has to be secured. A central device like a mobile phone has more computing power than a regular sensor so there for this might be easier to do. How such a system would work exactly might be a good follow up study. The allocation of timestamps would have to be regulated in order to make it a fair process. The acceptance of forwarding information should be arranged differently than the cookie law is arranged. In the cookie law, almost everyone immediately clicks yes, since they know they cannot visit the website if they press no. Therefore, people are giving their legal agreement but not their “informed consent”. There should be something like a privacy manager where you can select what kinds of information you would like to share with whom.

Several options have been explored of how we have to deal with the fact that our privacy rights are threatened to be violated by the IoT. From the ethical reflection, we can learn that the systems in the IoT are not yet very secure and that it is not easy to make it privacy friendly. We have also learned that the IoT brings very important values, and that some might argue that it is worth to give privacy up to achieve these goals. However, we have also looked at the relation between autonomy, freedom and privacy. And from that standpoint, it is very important to always have enough room for privacy in the society. Not only because it is beneficial to develop ourselves as individuals but also because it benefits the democratic society as a whole. The last part of this chapter was concerned with a third option where the control of what to disclose with others could be controlled by people themselves.

7.4 Main points of this chapter

Main points of the chapter ethical reflection

- Since constitutional rights can be violated with the use of the IoT, there will be issues of regulating the technology. Two opposite approaches can be taken to overcome this, changing our values or changing the technology to match our values.
- Changing our privacy values can be ethical justified by taking a utilitarianism approach.
- There are possibilities to change the technology to better incorporate privacy rights, but secure technologies have to be developed further.
- Privacy, autonomy and freedom are closely related.
- If one would look from privacy from an autonomous view then information self-determination would be preferred.

8 Conclusions & Discussion

The main research question was:

Are the constitutional privacy rights threatened to be violated by the internet of things?

To give a very short answer to this, yes they are threatened to be violated. It will now be elaborated how this conclusion was drawn and how the IoT is threatening to violate the privacy rights.

The research started with a descriptive overview of IoT technologies. It was shown that the IoT consists of two large technology groups that make it possible to interconnect all things in the world and which enable them to sense the environment in which they are situated. These technology groups are RFID, used for identification, and sensor technologies, used to sense the environment. It was also seen that the true vision of the IoT would only come true if all things would be directly accessible through the internet. IPv4 is not suitable for this since there a not enough unique numbers that could be allocated. IPv6 would be feasible however.

The legal aspect of this report started with the search of a definition of privacy where all can agree upon to be able to objectively assess privacy threats. It was analyzed that the expressed definition of privacy varies amongst persons and therefore it was decided to look at privacy from a legal perspective since it gives an objective basis of values approved by legislation. Even if one does not agree with the law, everyone should in principle still follow the law. Privacy was mainly assessed from the constitutional rights perspective. Four rights were found that are related to privacy. These are article 10, the general right to privacy, article 11, inviolability of the body, article 12, inviolability of the home and article 13, privacy of communications. Although the constitutional rights perspective was chosen to be able to have an objective basis were privacy threats can be tested upon, the interpretation of constitutional rights in the light of IoT technologies are not straightforward. This is due to the fact that the constitutional rights were passed at a time were no information technologies existed yet.

An argument has been made that the rights of inviolability of the body and the home should be interpreted as rights of protection from physical as well as from informational interference. Moreover, it has been argued that the IoT has the potential to violate these two rights in ways that were not possible before the IoT. A model was created consisting of layers of information from the body and the home where the human body was taking as a starting point. Information in the inner ring is considered to be the most privacy sensitive information in this model.

Before the threats posed by the IoT were assessed, a data flow model was created that combined the model of Solove with the one from Bekkers & Smits. The model of Solove was more concerned with the different stadiums data can go through, while the model of Bekkers & Smits was more concerned with how data is actually communicated. The combined model took both elements into consideration.

After the combined data flow model was presented the actual threats of violations of inviolability of the body and the home were assessed. The largest threat of RFID technology is that registration can happen without the knowledge of the person carrying RFID tags. The person might not even know that he is carrying items that contain RFID tags. Therefore, a lot of detailed information could be collected without giving (informed) consent to this. The biggest threat that was seen with sensor technologies is that it is very hard to secure access control. Even if the information content is intensively encrypted then traffic data could reveal very relevant information. All these new information availabilities stemming from the IoT feed big algorithms that are trying to find out who we are, what we would like to buy and even if we are likely to commit a terroristic attack. In the type of information flows we have seen a shift, first information was collected by the data subject itself and then giving to external parties. However, with the IoT it becomes easier to directly register information content stemming directly from the source. Therefore, it is not transparent of who exactly collect what and where the information is used for. Therefore, we could lose control over our information. It was also concluded that the perceived threat of the IoT on privacy is even larger if one would assess the sum of all the threats instead of perceiving the threats individually.

As an ethical reflection, we have explored the idea of limiting our values of privacy in favor of the benefits that the IoT could bring, like better health care, sustainability, national security and economic growth. If one would look purely from a utilitarian perspective then one could approve of this, although it remains debatable which values should be seen as a greater value than privacy. Privacy is however not only important to protect as an intrinsic value, but also as an instrumental value since it is important for other values like freedom and autonomy. And as argued a limitation of privacy would also limit those rights. Therefore, the ethical part examined some technical solutions to overcome the privacy threats. Although some solutions exist, they could not cover all privacy threats while preserving all the benefits of the IoT. It was proposed to preserve privacy as a contextual integrity; information that was giving to a certain purpose could be by third parties as long as the purpose remains the same. Also the collection of data could be done in relation with contextual integrity. If one were at a hospital, it would be acceptable for a doctor to collect data from your heart sensor while this would not be appropriate in the grocery store.

The constitutional rights chapter of this research started with the question if we could actually be implementing Big Brother or even the brave new world with the IoT. The IoT really has the potential to serve as a Big Brother since it can collect all kinds of information about our bodies and our homes. If we would be able to see what is going on in our homes from a distance, we would be able to (unintentionally) spy on other members of the household, which could have an effect on their behavior. In the ethical part, the example was giving that a student might not dare to watch television instead of doing homework; just by the fear that his/her parents might see that the television is turned on. Although doing homework might be the better choice than watching television, this is not an autonomous choice. As we have seen from the existence of the program PRISM and the proposed law by Opstelten, governments are also spying, or willing to spy, on our private communications. These private communications can contain information that could have previously only been collected during a body or a home search. Governments could also be applying algorithms on all these communications to determine whether someone might be

committing a criminal offence behind their closed doors. Since we are slowly giving up our privacy rights in favor of other values, it might be the case that in the near future the IoT actually is serving as a Big Brother keeping all citizens from misbehaving behind their closed doors. Since the IoT might limit our autonomous choices, not only since we can be watched by others but also since some IoT can make decisions for us, it could also be imaginable that the IoT might be implementing the brave new world, although this is less likely in the near feature. Thinking about these possible consequences the following lyric suddenly has a different feel:

> *"Every breath you take every move you make,*
> *Every bond you break every step you take,*
> *I'll be watching you.*
>
> *Every single day every word you say,*
> *Every game you play every night you stay,*
> *I'll be watching you."*
> *(*The Police, Every Breath you Take)

Nevertheless, if action is taken to amplify the perceived value of privacy in society it will not have to come as far as the Big Brother or the Brave New World. But it might be too late already. Once information is available and being used, it is very hard to stop the collection of this information. Privacy is a constitutional right however and this should never be forgotten. In relation to this research, some recommendations for legislators, data holders, engineers and privacy scholars are giving below.

8.1 Recommendations

8.1.1 Update of article 11 and 12

Our constitutional rights to body and home integrity should not only be protected from physical but also from information interference as has been argued in the legal chapter. It would therefore be wise to add this explicitly in the constitution. The most proper solution would be to add paragraphs, to the constitutional rights, explicitly stating that informational interference is also seen as a violation of the right. Only if this is explicitly mentioned our inviolability to our home and body can fully be protected.

8.1.2 Transparency

One of the problems that were found in this research is that the information flows are not transparent. People do not exactly know what happens with their information. Many people have become aware of the fact that the US government has programs that spy on internet traffic. But also the Dutch government is gathering information about us. It is not clear however, what is exactly done with this information. This transparency issue only becomes larger when information is collected directed from the things surrounding us, since you do not even know what was collected and when. Therefore, it would be reasonable that it becomes mandatory for all data holders to make it transparent what is done with the information. One could argue that we already have this through the privacy policies of the companies; however, they are not easy or straightforward to understand so they do not make the data flow transparent at all.

8.1.3 Privacy awareness

During this research, it became very clear that not everyone is aware of the impacts that privacy invasions could have. Therefore, it would be wise to create more awareness of the value of privacy in the Netherlands. It might for instance be a good idea to teach (secondary) school students what their privacy rights are and let them think about what they find acceptable of sharing with others. This could for instance be done in the social science course where the students are already introduced with some ideas of society. Some school students are now digitally bullied by others, this already starts at primary schools (Mediawijsheid, 2013) (NOG, 2013), this can have huge consequences for the person being bullied since the harassment could be seen by the whole world if this was done on a public web page. However, this harassment could also have consequences for the bully himself since the internet stores everything. This digital bullying is already a good reason to teach school students about privacy. That school students have to be taught about privacy does not imply that other people in the society should not be made aware of risks of privacy violations; this is also very important but it is more difficult to achieve. One step of creating more awareness could be made with more transparency, which was discussed in the last section.

8.1.4 Privacy taken into the design of the technology

So far, the design of technologies has mostly been focused on enabling accessibility. One way this has been achieved is by the standardizations of communications protocols. If the technology is created with privacy values in mind then it might be easier to find solutions where privacy is better protected. However, privacy is not an easy concept and not easily codified. Therefore, it would be wise for an instance like the CBP to put effort into codifying the values of privacy so that engineers could easier incorporate it. One could even say that it is unacceptable that technology can be designed without having constitutional rights in mind.

8.1.5 Privacy in relation with other values

It has been argued that privacy has an effect on freedom and autonomy. In the trade-offs that are being made these other values are not taken into consideration. Maybe it would be wise for privacy scholars to emphasize on the effects on those other values instead of just focusing on privacy as an intrinsic value. Maybe people would than take the consequences of privacy deprivation more seriously.

8.2 Discussion points

There are items that remain open for discussion in relation with this report. Below some discussion points are given.

8.2.1 Public versus private space

This discussion between public versus private space has not been explicitly debated during this research report. Some say that everything that happens in public should belong to public information. However implicitly, in this research report the standpoint of Nissenbaum has been taken where there is also room for privacy in the public space (Nissenbaum, 1998). Whether or not this standpoint is right remains a point of discussion.

8.2.2 Four classifications of privacy

If one would look very strictly at the classifications of the four types of privacy namely body, territorial, communicational and informational privacy one might conclude that the four articles also purely protect one type of privacy. Article 10 would then protect informational privacy, article 11 would protect body integrity, article 12 would protect territorial privacy and article 13 would protect communicational privacy. If one would follow this reasoning one might conclude that the privacy model taking the human body as a starting point, should actually be classes of information protected under article 10 instead of article 11 or 12. However, in this research arguments have been made that article 11 and 12 also protect informational privacy of the home and body. Let us consider article 11 first. Some choose for instance to show more of their skin than others by their clothing. This is clearly related to their body integrity. If information about their body despite their effort in covering it up is still revealed this is a violation of their body integrity. The argument for the home is very similar. In your own home, you should be able to do what you want and only when there are good arguments one should reveal what is going on inside the walls. However, it remains a discussion point that could be explored in further research. It also becomes clearer that electromagnetic waves have a physical effect and could affect your health. Then you could say that sensors and RFID always have a (small) physical effect. Therefore, when information is collected there is always physical interference with the body. But as has been discussed also the availability of the information could lead towards physical interference, since it could for instance reveal that you are carrying valuable items with you.

8.2.3 Privacy model taking the human body as a starting point

For this report, it is chosen to take the human body as a starting point for a privacy model. It could be argued however that mental integrity should have been taken as the starting point. Then not only inviolability of the home and the body would have been included in the model but also the general right to privacy, freedom of communications and also freedom of speech, article 7 of the DC. However, for the scope of this research it was chosen to limit to the inviolability of the home and the body. It would be an interesting discussion of what would be the order of the different layers if mental integrity is taken as a starting point.

8.2.4 Data flow model

In the combined data flow model, only data originating from a body or a home was taking into consideration. It could be argued however that traffic data entering the private sphere caused by a consultation should also be taken into the model, since this might also reveal information about the body or the home. It was decided to not include this into the model to make the model not too complex. And it could be argued that consultation is most of the times combined with registration in the IoT, since most services keep track of their users. However, it remains a point of discussion.

8.2.5 Privacy is dead already

Privacy can be seen as a boiling frog problem. The boiling frog problem states that if you throw a frog into hot boiling water it will jump right out. If you put him into cold water and slowly turn up the heat the frog will just boil to dead (Eckersley, 1988). This might also have been the case with privacy. If you would have asked people 20 years ago if they would be willing to share everything they do in their lives, whether you are in your private home or not, with the rest of the world they might have said: NO WAY. Just recall the reaction to Orwell's Big Brother at the time. Since we slowly started to allow others to collect data

about us, we might be the frog with privacy rights not noticing that the water is getting hotter and hotter. Maybe it is already too late and we let privacy boil to dead. It is not rare when you hear a quote like the one from the (at the present former) CEO of Sun Microsystems*: "You have zero privacy anyway. Get over it".* However, people should wake up and realize that their personal information is very important. People are also willing to fight for money and as Meglena Kuneva European Consumer Commissioner put it: "*Personal data is the new oil of the internet and the new currency of the digital world"* (Kuneva, 2009). Another quote worth mentioning that people should keep in mind: "*If you're not paying for it; You're the product"* (Ditzpatrick, 2010). During this research, it was noticed that some people do value the notion of privacy when asked, but they point out that it will be taking from them anyway and that there is nothing they can do about it and therefore they are just willing to accept this. Whether or not privacy still exists is an interesting discussion.

8.3 Limitations

In this section, the limitations of this research will be discussed.

8.3.1 No legal background

This research discusses legal topics, although no legal education was followed. Due to this, it might be the case that a person educated in law would interpret certain legal aspects differently. It would be interesting to check whether this might actually be the case. Insight in these differences could be very interesting. The constitution is applicable to all citizens and it could be argued that it should be writing in such a way that it is (approximately) interpreted by all citizens in the same way, despite different educational backgrounds.

8.3.2 Up to date literature

The IoT is a trending topic and during this research, many papers were written about this topic. Although effort has been put in using new literature, new relevant literature might have come out that could have been relevant for this research but was not included. But there is always a point where you stop finding new materials and write your report with the materials already found.

8.3.3 New European laws are on the way

Already at the beginning of the research, it became clear that Europe is in the process of introducing a European data protection act. The European law currently restricts itself to mandatory guidelines, so there are differences across European countries. But since the proposed law is still being changed and adapted, it is not sure yet what will be in this law. It can be that this new data protection act would put some elements in a different perspective. However, the main conclusions should not change too much.

8.3.4 Focus

The focus of this research was mainly on RFID and sensors technologies. This might have been too limited. Other technologies like public surveillance cameras, including the upcoming use of drones, and the Google Glass can also be very privacy invasive. A major concern with the Google Glass is for instance the ability to recognize faces with the device. Google as a reaction said that it would not allow face recognition applications. However, someone already found a work around and did use his Google Glass for face recognition (Henn, 2013). The Google Glass can however also be seen as extra sensors in the IoT.

8.3.5 Empirical validation

Although it was not the aim of this research one could argue that this research lacks empirical validation of the models, since the models are not tested in practice. This could be done in future research.

8.3.6 Disagreements versus conceptual analysis

For this research it is tried to look at the concept of privacy and the instances of privacy as objective as possible, something that should be expected of scientific research. But since the subjective nature of the concept of privacy, disagreements might have driven the research sometimes towards certain interpretations. Effort has been put however to limit purely personal thoughts about privacy and to always find scientific backup.

8.4 Future research

During this report already some ideas for future research have been given. In this part some other ideas for future research are given.

8.4.1 Identity theft and the internet of things

In 2012 already between 650000 and 870000 person became a victim in the Netherlands of identity fraud (NOS, 2013). Currently the internet of things is adding more and more data where people can be identified with. It would be a nice follow up study to research the effects of the IoT on identity theft, a special instance of identity fraud. Is the IoT making the possibilities of identity theft larger or smaller?

8.4.2 Contextual privacy in practice

Could contextual privacy as proposed by Nissenbaum be technically realized by the IoT? If we design systems to be aware of the context then they could maybe also learn which information is appropriate for that context.

8.4.3 Trust and privacy in the IoT

Since the technology and the data flows become more and more complex it becomes harder for people to have insight in what is going on. Therefore, it would be interesting to study the relation of privacy and trust. Trust in the technology but also in the company and the government using the technologies. In addition, the idea of trusted services managers for IoT applications could be explored.

8.4.4 Responsibilities of safeguarding privacy

Who is responsible for safeguarding privacy? Is it the technician, the consumer, the companies, judges, controlling bodies like the CBP or the government? And to what extend are these responsibilities reasonable. Is everyone aware of their responsibility?

8.4.5 Governing the borderless IoT

Privacy policies vary across the world as we have seen in the legal chapter, but yet internet allows us to access anything, anywhere and anytime. Could a system be designed where a central body regulates internet?

8.4.6 Autonomy and the IoT

An interesting research would be to assess what the effects from the IoT are on autonomy. In an interconnected world where all things are capable of acting on our behalf to make us more sustainable and more efficient, what would happen to our ability to decide for ourselves what is morally good or wrong?

Bibliography

AD. (2013, August 22). *FBI-directeur: 'Speciale rechtbank keurde PRISM goed'*. Opgeroepen op August 22, 2013, van AD: http://www.ad.nl/ad/nl/5595/Digitaal/article/detail/3458334/2013/06/13/FBI-directeur-Speciale-rechtbank-keurde-PRISM-goed.dhtml

AG. (2011, January 20). *Sleutelloze auto makkelijk te hacken*. Opgeroepen op August 23, 2013, van Automatiseringsgids: http://www.automatiseringgids.nl/nieuws/2011/3/sleutelloze-auto-makkelijk-te-hacken

Akkermans, P., Bax, C., & Verhey, L. (2005). *Grondrechten.* Heerlen: Kluwer.

Ashton, K. (2009). That Internet of Things Thing. *RFID Journal*, 1.

Ayres, I. (2007). *Super Crunchers.* New York: Bantam Dell.

Bainbridge, D. (2007). Database copyright and the database right. In D. Bainbridge, *Introduction to Information Technology Law* (Sixth ed., pp. 72-119). Harlow: Pearson.

Bandyopadhyay, D., & Sen, J. (2011). *Internet of Things - Applications and Challenges in Technology and Standardization.*

barcodesinc. (2013). *Choosing the Right RFID Technology*. Opgehaald van barcodesinc: http://www.barcodesinc.com/info/buying-guides/rfid.htm

Bayardo, R. J., & Agrawal, R. (2005). Data Privacy Through Optimal k-Anonymization. *Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on* (pp. 217-228). IEEE.

Bekkers, R., & Smits, J. (1999). Forms of Telecommunication. In R. Bekkers, & J. Smits, *Mobile Telecommunications: Standards, Regulation, and Applications* (pp. 1-15). Boston-London: Artech House.

Bentham, J. (1789). *An introduction to the principles of moral and legislation.* Oxford: Hafner Press 1948.

Beresford, A. R., & Stajano, F. (2003). Location Privacy in Pervasive Computing. *Pervasive Computing, 2*(1), 46-55.

Brock, D. L. (2002, February 1). *White paper: The Virtual Electronic Product Code.* Opgeroepen op June 16, 2013, van Auto-ID center: http://htp.autoidlabs.org/uploads/media/MIT-AUTOID-WH-011.pdf

Buratti, C., Conti, A., Dardari, D., & Verdone, R. (2009). An Overview onWireless Sensor Networks Technology and Evolution. *Sensors, 9*, 6869-6896.

CBP. (2013). *Het advies van het College bescherming persoonsgegevens van het conceptwetsvoorstel tot wijziging van artikel 13 Grondwet (z2012-00746).* Den Haag: College Bescherming Persoonsgegevens.

CBS. (2011). *Mobiel internetten fors toegenomen .* Centraal Bureau voor de Statistiek .

Chan, H., & Perrig, A. (2003). Security and Privacy in Sensor Networks. *Computer, 36*(10), 103-105.

Chaouchi, H. (2010). *The Internet of Things.* London-Hoboken: ISTE-Wiley.

Cheng, W., Golubchik, L., & Kay, D. (2004). Total Recall: Are Privacy Change Inevitable? *Proceedings of the the 1st ACM workshop on Continuous archival and retrieval of personal experiences* (pp. 86-92). ACM.

Clarke, R. (1999). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms.* Canberra: Xamax Consultancy. Opgehaald van Xamax Consultancy: http://www.rogerclarke.com/DV/Intro.html

Cleiren, C. (2009). Veiligheid en privacy, een blijvende zorg. *Strafblad*, 91-93.

College Bescherming Persoonsgegevens. (2013, April 28). *Melden verwerkings persoonsgegevens*. Opgehaald van cbpweb: www.cbpweb.nl/Pages/ind_melden.aspx

Colville, R. (2013, July 2). *Press briefing notes on Egypt*. Opgeroepen op July 26, 2013, van United Nations Human Rights: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13496&LangID=E

Commission of the European Communities. (2009, June 18). *Internet of Things — An action plan for Europe.* Opgeroepen op August 9, 2013, van Eur-Lex: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF

Counsil of Europe. (2010). *European Convention on Human Rights.* Strasbourg: Counsil of Europe.

Cuijpers, C., & Koops, B.-J. (2008). *Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM.* Tilburg: Universiteit van Tilburg.

Data Protection Working Party. (2011, May 16). *Opinion 13/2011 on Geolocation services on smart mobile devices.* Opgeroepen op August 7, 2013, van CBPWeb: http://www.cbpweb.nl/downloads_int/wp185_en.pdf

de Graaf. (2013, August 11). Zomergasten. (W. de Jong, Interviewer)

de Graaf, F. (1977). *Rechtsbescherming van persoonlijkheid, privéleven, persoongegevens.* Utrecht: Rijksuniversiteit te Utrecht.

de Hert, P., Klo, D., & Wright, D. (2012). *Recommendations for a privacy impact assessment framework for the European Union.* Brussel: EU.

De, P., Basu, K., & Das, S. K. (2004). An Ubiquitous Architectural Framework and Protocol for Object Tracking using RFID Tags. *Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2004)* (pp. 174-182). IEEE.

Ditzpatrick, J. (2010, november 23). *If You're Not paying for it; You're the Product*. Opgehaald van lifehacker: lifehacker.com/5697167/if-youre-not-paying-for-it-youre-the-product

Dominikus, S., & Schmidt, J.-M. (2001). Connecting Passive RFID Tags to the Internet of Things. *Interconnecting Smart Objects with the Internet Workshop*. Prague.

Dossier X. (2008, May 4). *RFID, Verichip*. Opgeroepen op August 12, 2013, van Dossier X: http://www.dossierx.nl/trust-no-one/rfid-verichip.html

Dynastream Innovations Inc. (2013). *ANT Message Protocol and Usage .* Dynastream Innovations Inc.

Eckersley, R. (1988). *Casualities of Change.* Canberra: Australian Government Publishing Service.

Engelfriet, A. (2013). *De wet op internet.* Eindhoven: IusMentis B.V.

Engels, D. (2003, February 1). *Technical Report: The Use of the Electronic Product Code.* Opgeroepen op June 16, 2013, van Auto-Id Center: http://forum.autoidlabs.org/uploads/media/MIT-AUTOID-TR009.pdf

EPC Global. (2007, January). *Electronic Product Code (EPC): An Overview*. Opgeroepen op August 14, 2013, van gs1.org: http://www.gs1.org/docs/epcglobal/an_overview_of_EPC.pdf

EPCglobal. (2013). *GS1 EPC Tag Data Standard 1.7.* Brussels: GS1 AISBL.

EURLex. (2013, April 28). *31995L0046*. Opgehaald van EURLex: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

European Commission. (2012, January 25). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for*

businesses. Opgeroepen op July 2, 2013, van Europa: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

Fischer, J. C. (2010). *Communications Network Traffic Data.* Eindhoven: PrintService TU/e.

Foster, K. R., & Jaeger, J. (2007). RFID Inside: The Murky Ethics of Implanted. *IEEE Spectrum*, 24-29.

Franken, H. (1999). *Commissie grondrechten in het digitale tijdpwerk.* Rotterdam: Phoenix & den Oudsten.

Garcia, F. D., Gans, G. d., Muijrers, R., van Rossum, P., Verdult, R., Schreur, R. W., & Jacobs, B. (2008). Dismantling MIFARE Classic. *Computer Security-ESORICS*, 97-114.

gemeente Vlissingen. (2004). *Draaiboek voor de toepassing van de Algemene wet op het binnentreden.* Vlissingen: gemeente Vlissingen.

Gons, E. (2012, December 10). *Leweb 2012 the internet of things; a visual overview in live! iPadsketches.* Opgeroepen op March 1, 2013, van Wilgenbroed: http://wilgengebroed.nl/leweb-2012-the-internet-of-things-a-visual-overview-in-live-ipadsketches/

GS1 Nederland. (2012, November 22). *'Coderen makkelijker én goedkoper dan verwacht'*. Opgeroepen op August 15, 2013, van GS1 Nederland: http://www.gs1.nl/actueel/%E2%80%98coderen-makkelijker-%C3%A9n-goedkoper-dan-verwacht%E2%80%99

Gubb, J., Buyya, R., Marusic, S., & Palaniswam, M. (2012). *Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions.* Opgehaald van cloudbus.org: http://www.cloudbus.org/papers/Internet-of-Things-Vision-Future2012.pdf

Gutwirth, S. (1993). *Waarheidsaanspraken in recht en wetenschap.* Brussel: VUBPRESS.

Gutwirth, S. (1998). Complexe Privacy. In S. Gutwirth, *Privacyvrijheid! De vrijheid om zichzelf te zijn* (pp. 15-44). Amsterdam: Rathenau Instituut.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., & Nouwt, S. (2012). *Reinventing Data Protection?* New York: Springer.

HART. (2013). *WirelessHART Overview*. Opgeroepen op June 23, 2013, van HART Community Foundation: http://www.hartcomm.org/protocol/wihart/wireless_overview.html

Henn, S. (2013, July 17). *Clever Hacks Give Google Glass Many Unintended Powers*. Opgehaald van NPR: http://www.npr.org/blogs/alltechconsidered/2013/07/17/202725167/clever-hacks-give-google-glass-many-unintended-powers

Hill, K. (2013, July 26). *When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet*. Opgeroepen op August 12, 2013, van Forbes: http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/

Hoepman, J.-H. (2011). In Things We Trust? Towards trustability in the Internet of Things. *arxiv*, 1-9.

Hornyak, T. (2008). RFID Powder. *SCIENTIFIC AMERICAN*, 68-71.

Hunton & Williams LLP. (2011, May 31). *German DPAs Publish Comprehensive FAQs on Statutory Data Breach Notification Requirement*. Opgeroepen op August 10, 2013, van Privacy and Information Security Law Blog: http://www.huntonprivacyblog.com/2011/05/articles/german-dpas-publish-comprehensive-faqs-on-statutory-data-breach-notification-requirement/

Huxley, A. (1932). *A Brave New World.* London: Vintage.

IDTECK. (2009). *Overview of the RFID System*. Opgehaald van IDTECK: http://www.idteck.com/support/rfid.asp

IERC. (2012). *The Internet of Things 2012 New Horizons.* Halifax: Platinum.

ITU. (2005). *ITU Internet Reports 2005: The Internet of Things .* Geneva: ITU.

Jovanov, E., Milenkovic, A., Otto, C., & de Groen, P. (2005). A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering and Rehabilitation, 2*(6). Opgehaald van http://www.jneuroengrehab.com/content/2/1/6

Juels, A. (2005). *RFID Security and Privacy: A research Survey.* RSA Laboratories.

Kansal, A., Goraczko, M., & Zhao, F. (2007). *Building a Sensor Network of Mobile Phones.* Cambridge: IPSN.

Kant, I. (1785). *Grundlegung zur Metaphysik der Sitten.* Kampen: Agora 2000.

Karimi, K., & Atkinson, G. (2012). *What the Internet of Things (IoT) Needs to Become a Reality.* freescale ARM.

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks, 1*, 293-315.

Knijnenburg, B. P., Kobsa, A., & Jin, H. (2013). Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies*, 1-19. doi:http://dx.doi.org/10.1016/j.ijhcs.2013.06.003

Knol, P., & Zwenne, G. (2009). *Telecommunicatierecht.* Deventer: Kluwer.

KNX. (2013, May 8). *Introduction*. Opgeroepen op June 23, 2013, van KNX: http://www.knx.org/knx-standard/introduction/

Koops, B., & Prinsen, M. (2005). Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit. *Nederlandsejuristenblad*, 624-630.

Koops, B.-J., Leenes, R., & de Hert, P. (2007). *Constitutional Rights and New Technologies.* Tilburg: TILT.

Koops, B.-J., van Schooten, H., & Prinsen, M. (2004). *Recht naar binnen kijken.* Den Haag: Sdu Uitgevers.

Kuneva, M. (2009, March 21). *Keynote Speech: Roundtable on Online Data Collection, Targeting and Profiling.* Brussel. Opgehaald van Europa.

Lee, J.-S., Su, Y.-W., & Shen, C.-C. (2007). A Comparative Study of Bluetooth, UWB, ZigBee, and Wi-Fi. (pp. 46-51). Taiwan: IEEE.

Leenen, H., & Gevers, J. (2008). *Handboek gezondheidsrecht. Deel 1 Rechten van mensen in de gezondheidszorg.* Bohn Stafleu Van Loghum.

Leenknegt, G. (2002). The Protection of Fundamental Rights in a Digital Age. *ELECTRONIC JOURNAL OF COMPARATIVE LAW, 6*(4), 326-345.

Levin, A., & Nicholson, M. J. (2005). Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground. *university of ottawa law & technology journal, 2*(2), 357-395.

Li, N., Zhang, N., Das, S. K., & Thuraisingham, B. (2009). Privacy preservation in wireless sensor networks: A state-of-the-art survey. *Ad Hoc Network, 7*, 1501-1514.

Liga voor mensenrechten. (2013, Juni 20). *Big, bigger, biggest! Over de waarde van privacy in tijden van massa-surveillance*. Opgeroepen op August 22, 2013, van Liga voor mensenrechten: http://www.mensenrechten.be/index.php/site/nieuwsberichten/big_bigger_biggest_over_de_waarde_van_privacy_in_tijden_van_massa_surveilla

Logius. (2013, April 28). *Wet bescherming persoonsgegevens*. Opgehaald van Overheid.nl: wetten.overheid.nl/bwbr0011468/geldigheidsdatum_28-04-2013

Matin, M., & Islam, M. (2012). Overview of Wireless Sensor Networks. In M. A. Matin, *Wireless Sensor Networks - Technology and Protocols* (pp. 3-24). Rijeka: InTech.

McArthur, R. L. (2001). Reasonable expectations of privacy. *Ethics and Information Technology, 3*, 123–128.

McMillan, S. (2002). A four-part model of cyber-interactivity Some cyber-places are more interactive than others. *New Media and Society, 4*(2), 271-291.

Mediawijsheid. (2013). *Online pesten*. Opgeroepen op September 9, 2013, van Mediawijsheid: http://www.mediawijsheid.nl/online-pesten/

Mendelts, P. (2002). *Interpretatie van grondrechten.* Utrecht: Universiteit Utrecht.

Mill, J. (1863). *Utilitarianism.* London: Collins 1979.

Ministerie van Veiligheid en Justitie. (2011). *Notitie Privacybeleid bijlage 1.* Den Haag: Ministerie van Veiligheid en Justitie.

Mironenko, O. (2011). Body scanners versus privacy and data protection. *COMPUTER LAW & SECURITY REVIEW, 27*, 232-244.

Mocana. (2012, January 9). *Smart Meters Reveal Movie and TV Viewing Habits*. Opgeroepen op August 15, 2013, van Mocana: https://mocana.com/blog/2012/01/09/smart-meters-reveal-movie-and-tv-viewing-habits/

Neptune Technology Group Inc. (2010). Comparing Operational and Cost Efficiencies of Star and Mesh Network Topologies.

New York Times. (2012, February 16). *How Companies Learn Your Secrets.* Opgehaald van New York Times: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0

Newell, P. B. (1995). Perspectives on privacy. *Journal of Environmental Psychology, 15*(2), 87–104.

Ni, L. M., Liu, Y., Lau, Y. C., & Patil, A. P. (2004). LANDMARC: Indoor Location Sensing Using Active RFID. *Wireless Networks, 10*, 701–710.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy, 17*, 559-596.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review Association, 79*(119), 119-158.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus, 140*(4), 32-48.

NOG. (2013, March 2). *Twee keer zoveel basisscholieren digitaal gepest*. Opgehaald van Nationale Onderwijsgids: http://www.nationaleonderwijsgids.nl/basisonderwijs/nieuws/16418-twee-keer-zoveel-basisscholieren-digitaal-gepest.html

NOREA. (2013). *Privacy Impact Assessment (PIA).* Amsterdam: NOREA.

NOS. (2013, September 8). *"NSA kan smartphones aftappen"*. Opgeroepen op September 9, 2013, van NOS: http://nos.nl/artikel/549011-nsa-kan-smartphones-aftappen.html

NOS. (2013, April 4). *Plasterk: aanpak identiteitsfraude*. Opgehaald van NOS Nieuws: http://nos.nl/artikel/491922-plasterk-aanpak-identiteitsfraude.html

Nutihouse. (sd). Opgeroepen op August 13, 2013, van http://nutihouse.com/

Ok, K., Coskun, V., Aydin, M. N., & Ozdenizci, B. (2010). Current Benefits and Future Directions of NFC Services. *ICEMT 2010 Conference.*

Opstelten. (2013). *Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III).* Kamerstuk.

Orwell, G. (1948). *Nineteen eighty-four.*

Overheid.nl. (2012, October 1). *Wijziging van artikel 13 Grondwet.* Opgehaald van Overheid.nl: internetconsultatie.nl/briefentelecommunicatiegeheim

overheid.nl. (2013, July 11). *Algemene wet op het binnentreden*. Opgeroepen op July 11, 2013, van overheid.nl: http://wetten.overheid.nl/BWBR0006763/geldigheidsdatum_11-07-2013

Overkleeft-Verburg, G. (2000). Het grondrecht op eerbiediging van de persoonlijke levenssfeer. In A. Koekkoek, *De Grondwet: een systematisch en artikelsgewijs commentaar* (pp. 155-178). Deventer.

Parlementair Documentatie Centrum van de Universiteit Leiden. (2013, April 23). *Artikel 10: Privacy.* Opgehaald van Nederlanse Grondwet: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbl6ah4zz

Parlementair Documentatie Centrum van de Universiteit Leiden. (2013, April 23). *Artikel 11: Onaantastbaarheid lichaam.* Opgehaald van Nederlandse Grondwet: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnblu821m2

Parlementair Documentatie Centrum van de Universiteit Leiden. (2013, April 23). *Artikel 12: Huisrecht.* Opgehaald van Nederlandse Grondwet: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbm9pegm3

Parlementair Documentatie Centrum van de Universiteit Leiden. (2013, April 23). *Artikel 13: Briefgeheim.* Opgehaald van Nederlandse Grondwet: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbn1m96qm

Parlementair Documentatie Centrum van de Universiteit Leiden. (2013, April 28). *Inleiding*. Opgehaald van Nederlandse grondwet: www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbm9pegm3

Parlementair Documentatie Centrum van de Universiteit Leiden. (2013, June 7). *Politiewet 1993*. Opgeroepen op June 7, 2013, van Nederlandse Grondwet: http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vi32nm24b5yu

pcworld. (2013, March 13). *Google to pay $7 million to US states for Wi-Fi eavesdropping*. Opgeroepen op September 9, 2013, van pcworld: http://www.pcworld.com/article/2030705/google-to-pay-7-million-to-us-states-for-wi-fi-eavesdropping.html

Posner, R. (1978). An Economic Theory of Privacy. *Regulation*, 19-26.

Prins, J., Vries, M. d., Graaf, B. d., Eijkman, Q., Schuilenburg, M., & Dijkstra, C. (2011). Function creep en privacy. *Justitiële verkenningen, 37*(8), 1-87.

Purtova, N. N. (2011). *Property Rights In Personal Data: A European Perspective.* Oisterwijk: Uitgeverij BOXPress.

Quinn, M. J. (2005). Chapter 5: Privacy. In M. J. Quinn, *Ethics for the Information Age* (pp. 187-244). Boston: Pearson Addison Wesley.

Reuters. (2013, July 26). *Famed hacker Barnaby Jack dies a week before hacking convention*. Opgeroepen op August 15, 2013, van Reuters: http://www.reuters.com/article/2013/07/26/us-hacker-death-idUSBRE96P0K120130726

RFID journal. (2013, September 9). *How much does an RFID tag cost today?* Opgehaald van RFID journal: http://www.rfidjournal.com/faq/show?85

Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006). The Evolution of RFID Security. *PERVASIVE computing*, 62-69.

Rijksoverheid. (2010, March 15). *Evaluatie wet bescherming persoonsgegevens*. Opgehaald van Rijksoverheid: http://www.rijksbegroting.nl/algemeen/gerefereerd/1/4/1/kst141587.html

Rijksoverheid. (2013, May 1). *Opstelten versterkt aanpak computercriminaliteit*. Opgeroepen op August 1, 2013, van Rijksoverheid: http://www.rijksoverheid.nl/nieuws/2013/05/02/opstelten-versterkt-aanpak-computercriminaliteit.html

Rijksoverheid. (2013, June 21). *Wetsvoorstel meldplicht datalekken naar Tweede Kamer*. Opgeroepen op July 1, 2013, van Rijksoverheid:

http://www.rijksoverheid.nl/nieuws/2013/06/21/wetsvoorstel-meldplicht-datalekken-naar-tweede-kamer.html

Rimanque, K. (2005). *De grondwet toegelicht, gewikt en gewogen.* Antwerpen: Intersentia.

Ringelestijn, T. v. (2013, May 5). *Niet gelukkiger na 365 dagen offline*. Opgeroepen op August 7, 2013, van Bright.nl: http://www.bright.nl/niet-gelukkiger-na-365-dagen-offline

RIVM. (2013, July 8). *Duizenden deelnemers eerste Nationale iSPEX-meetdag*. Opgeroepen op August 1, 2013, van Rijksinstitutuut voor Volksgezondheid en Milieu: http://www.rivm.nl/Documenten_en_publicaties/Algemeen_Actueel/Nieuwsberichten/2013/Duizenden_deelnemers_eerste_Nationale_iSPEX_meetdag

Rogers, A., Jones, E., & Oleyniko, D. (2007). Radio frequency identification (RFID) applied to surgical sponges. *Surgical endoscopy, 21*(7), 1235-1237.

Rössler, B. (2008). De glazen samenleving en de waarde van privacy . *Socrates-lezing 2008* .

Royakkers, L. (2004). Normatieve Ethiek. In L. Royakkers, I. van der Poel, & A. Pieters, *Ethiek & Techniek* (pp. 54-81). Baarn: HBuitgevers.

Russ, A., Hesse, W., & Müller, D. (2008). Ambient Information System – Do They Open a New Quality of IS? . *SISGAND-EUROPE*, 93-108.

Russell, S., & Bakken, R. J. (2002). *Development of Autonomy in Adolescence.* Opgehaald van http://www.ianrpubs.unl.edu/epublic/archive/g1449/build/g1449.pdf

Rust, R. T., Kannan, P. K., & Peng, N. (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science, 30*(4), 455-464.

Scansource. (2013). *RFID Frequencies.* Opgehaald van Scansource: www.scansource.eu/en/education.htm?eid=8&elang=en

scientias.nl. (2013, March 16). *Implanteerbare sensor volgt kanker in het lichaam*. Opgeroepen op August 9, 2013, van scientias.nl: http://www.scientias.nl/implanteerbare-sensor-volgt-kanker-in-het-lichaam/27408

Shaw, T. (2012). Information Security and Privacy Laws and Regulations. In T. Shaw, *Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists* (pp. 27-108). American Bar Association.

Sidhu, B., Singh, H., & Chhabra, A. (2007). Emerging Wireless Standards - WiFi, ZigBee and WiMAX. *World Academy of Science, Engineering and Technology, 25*, 308-313.

Smith, A. (2013, January 13). *Samsung Smart Fridge Dishes Up Recipe Ideas and Coupons*. Opgehaald van Mashable: mashable.com/2013/01/12/samsumg-smart-fridge-recipes

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477-560.

Spahn, A. (2011). Technology. In J. Birx, *21st Century Anthropology A Reference Handbook* (pp. 132-141). Sage: Los Angeles.

Tak, A. (1973). *Het Huisrecht.* Hoenderloo: Hoenderloo's Uitgeverij en Drukkerij.

techzine. (2013, March 25). *Bluetooth implantaat waarschuwt voor hartaanval*. Opgeroepen op August 9, 2013, van techzine: http://www.techzine.nl/nieuws/33812/bluetooth-implantaat-waarschuwt-voor-hartaanval.html

The Guardian. (2013, July 9). *PRISM*. Opgeroepen op July 9, 2013, van The Guardian: http://www.guardian.co.uk/world/prism

The Verge. (2013, August 19). *New FTC chief warns Google, Twitter, big data companies to respect consumer privacy*. Opgeroepen op August 20, 2013, van The verge: http://www.theverge.com/2013/8/19/4637948/new-ftc-chief-big-data-companies-transparency-speech

The Wall Street Journal. (2013, April 29). *Bloomberg Is Right About Privacy, Says Posner*. Opgeroepen op Agust 21, 2013, van The Wall Street Journal: http://blogs.wsj.com/law/2013/04/29/bloomberg-is-right-about-privacy-says-posner/

The Wall Street Journal. (2013, August 16). *Noonan: What We Lose if We Give Up Privacy*. Opgeroepen op August 22, 2013, van The Wall Street Journal: http://online.wsj.com/article/SB10001424127887323639704579015101857760922.html

Trouw. (2013, August 13). *Wat is belangrijker: veiligheid of privacy?* Opgeroepen op August 22, 2013, van Trouw: http://www.trouw.nl/tr/nl/5133/Media-technologie/article/detail/3456186/2013/06/10/Wat-is-belangrijker-veiligheid-of-privacy.dhtml

Tsirbas, H., Giokas, K., & Koutsouris, D. (2010). “Internet of Things”, an RFID – IPv6 Scenario in a Healthcare Environment. *MEDICON 2010, IFMBE Proceedings, 29*, 808–811.

Turck, M., Dong, S., & FirstmarkCapital. (2013, May 27). *Spime Watch: Internet of Things Landscape from TechCrunch*. Opgeroepen op August 8, 2013, van Wired: http://www.wired.com/beyond_the_beyond/2013/05/spime-watch-internet-of-things-landscape-from-techcrunch/

Tweede Kamer. (1997). *vergaderjaar 1996-1997, 25 403, nr.3.* 's-Gravenhage: Sdu Uitgevers.

UN. (2013, April 30). *The Universal Declaration of Human Rights*. Opgehaald van un.org: www.un.org/en/documents/udhr/

United Nations. (2013, July 26). *International Covenant on Civil and Political Rights*. Opgehaald van United Nations Human Rights: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

van de Weije, B. (2013, June 29). Wie ben ik? TNO ging op zoek in mijn 32272 mails. *de Volkskrant*.

van der Poel, I. (2009). Values in Engineering Design. In A. Meijers (Red.), *Philosophy of technology and engineering sciences* (Vol. 9, pp. 973-1006). Elsevier.

van der Pot. (2004). *Handboek Van Het Nederlandse Staatsrecht.* (D. Elzinga, R. d. Lange, & H. Hoogers, Red.) Deventer: Kluwer.

van 't Hof, C., van Est, R., & Daemen, F. (2010). *Check in / Check uit; De digitalisering van de openbare ruimte.* Rotterdam: NAi Uitgevers.

Vedder, A., Wees, L. v., Koops, B.-J., & Hert, P. d. (2007). *Van privacyparadijs tot controlestaat?* Den Haag: Rathenau Instituut.

Verhey, L. (2011). Grondrechten in het digitale tijdperk: Driemaal is scheepsecht? *TvCR*, 152-167.

Volkskrant. (2013, September 6). *NSA kraakt ook versleutelde informatie op internet*. Opgeroepen op September 6, 2013, van Volkskrant: http://www.volkskrant.nl/vk/nl/13524/Het-PRISM-schandaal/article/detail/3504688/2013/09/06/NSA-kraakt-ook-versleutelde-informatie-op-internet.dhtml

Want, R. (2006). An Introduction to RFID Technology. *Pervasive computing*, 25-33.

Want, R. (2011). Near Field Communication. *Pervasive Computing*, 4-7.

Warren, S. D., & Brandeis, L. D. (1890). The Right To Privacy. *Harvard Law Review, 4*(5), 193-220.

Weber, R. H. (2009). Internet of things - Need for a new legal environment? *Computer Law & Security Review, 25*, 522-527.

Weber, R., & Weber, R. (2010). *Internet of Things - Legal Perspectives.* Berlin Heidelberg: Springer-Verlag.

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American*, 94-110.

Westin, A. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues, 59*(2), 431-453.

Wetboek Online. (2013, July 11). *Artikel 138*. Opgeroepen op July 11, 2013, van Wetboek van Strafrecht: http://www.wetboek-online.nl/wet/Sr/138.html

Wetboek Online. (2013, July 2). *Wetboek van Strafvordering*. Opgeroepen op July 2, 2013, van Wetboek Online: http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html#315

Winner, L. (1980). Do Artifacts Have Politics? In L. Winner, *The whale and the reactor: a search for limits in an age of high technology.* (pp. 19-39). Chicago: University of Chicago Press.

Yeo, M. (2010). Propaganda and Surveillance in George Orwell's Nineteen Eighty-Four: Two Sides of the Same Coin. *Global Media Journal -- Canadian Edition, 3*(2), 49-66.

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks, 52*, 2292–2330.

Zacharisas, S., & Newe, T. (2010). Technologies and Architectures for Multimedia-Support in Wireless Sensor Networks. In H. D. Chinh, & Y. K. Tan, *Smart Wireless Sensor Networks* (pp. 385-406). Rijeka: InTech.

ZDNet. (2011, June 14). *Eetbare RFID in maaltijd van de toekomst*. Opgeroepen op September 9, 2013, van ZDNet: http://www.zdnet.nl/news/128594/eetbare-rfid-in-maaltijd-van-de-toekomst/

Zins, C. (2007). Conceptual Approaches for Defining Data, Information, and Knowledge. *JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE AND TECHNOLOGY,, 58*(4), 479-493.

Z-Wave Alliance. (2012). *About Z-Wave Technology*. Opgeroepen op June 23, 2013, van Z-Wave Alliance: http://www.z-wavealliance.org/technology

Appendix

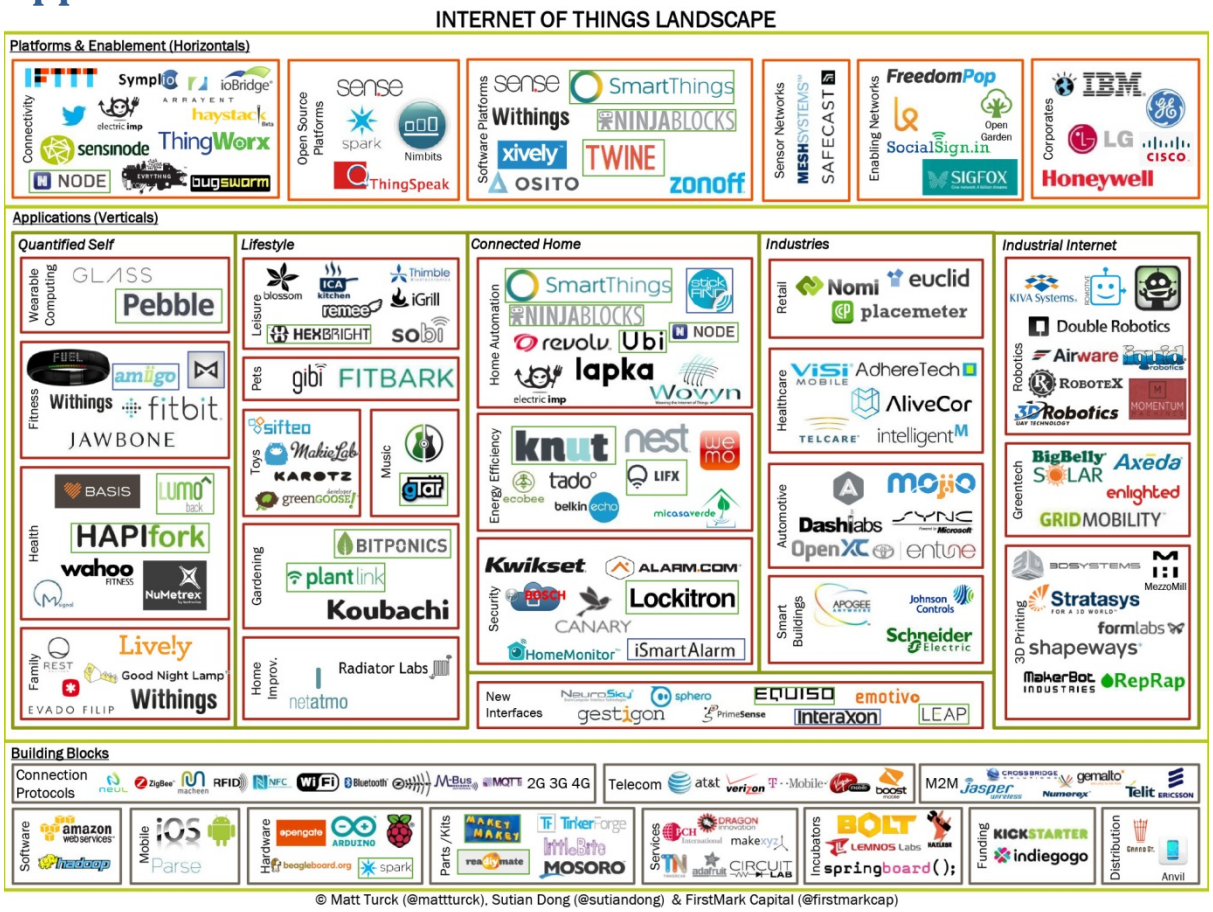


Figure 29: IoT landscape and areas of business opportunities source: (Turck, Dong, & FirstmarkCapital, 2013)