UNIVERSITY OF BERGEN

Department of linguistic, literary and aesthetic studies

DIKULT350
Master´s Thesis in Digital Culture

Spring 2020

Exploring methods for securing users against potential loss of privacy in the context of the Internet of Things

Malene Gilje Fonnes

Acknowledgements

Through the process of writing my master's thesis, I have learned a lot about myself and the existing world of the Internet of Things.

I would like to thank my supervisor, Daniel Apollon, for continuously keeping me on my toes and for the guidance and support throughout the thesis. Your knowledge is inspiring.

I would also like to thank my family and friends for listening to me talk for hours about privacy and IoT.

Abstract

The master´s thesis is an exploration analysis and discussion on occurring challenges within privacy, security, data ownership and ethics associated with the Internet of Things (IoT). The merging of interaction in the physical and virtual world is intensifying the necessity to understand the complex transactions between human and technical systems. While the capabilities of the technology of the Internet of Things makes it possible to perform tasks and processes more efficiently, the Internet of Things raises new regulatory and ethical challenges for users and citizens. This thesis aims at exploring and assessing various approaches to addressing the users´ subjective or objective losses of privacy in their interactions with the Internet of Things.

Sammendrag

Følgende avhandling er en analyse og diskusjon av utfordringer knyttet til personvern, sikkerhet, dataeierskap og etikk i teknologien Internet of Things (IoT). Utvikling av teknologi fører til økende sammenfletting av den fysiske og virtuelle verden som igjen fører til større utfordringer for brukere av IoT. Masteroppgaven gir et historisk overblikk over de avgjørende bidragsyterne innen teknologi. Videre er utfordringer innen personvern, sikkerhet, dataeierskap, og etikk i samspill med brukerne belyst. Potensielle løsninger på disse utfordringene er foreslått og diskutert. Hovedperspektivet i avhandlingen er forankret i å utforske teoretiske løsninger og mulige metoder for å sikre brukere og deres personvern i interaksjonene med IoT-enheter. Konklusjon på avhandlingen viser hvor viktig det er å ivareta fokuset på interaksjon mellom mennesket og teknologien, samt behov for endringer innen design prosessen for å sikre brukere og enheter. Den teknologiske utviklingen vil være kontinuerlig, av den grunn må fokus på brukerens samspill med teknologien være tilsvarende.

Keywords: Internet of Things, IoT, privacy, user perspective, security, ethics, data ownership
Nøkkelord: Internet of Things, IoT, personvern, brukerperspektivet, sikkerhet, etikk, dataeierskap.

1. Introduction

The Internet of Things (IoT) consists of billions of physical devices embedded with the necessary software and hardware components that can support processing and networking capabilities. The dynamic environment of IoT offers many opportunities with its capabilities of linkability and connections between smart objects, things and humans. IoT-devices enhance elements within efficiency, cost reduction, timesaving, innovation, effectiveness, optimization and mobility. The technology aims at improving the quality of people's lives by generating new applications that facilitate daily activities. The Internet of Things is almost infinite which builds up a motivation and interest to test its potential. Processes and tasks within various industries have been revolutionized with the use of IoT-devices. The key characteristics of the technology have found a gateway into the physical aspect which have blurred the line between the physical and virtual world. A breach in IoT-devices may create severe fatal issues as they can be embedded into our physical bodies and places where technologies have not had access to before. The interactions between humans and technical systems can be powerful if it is utilized correctly. Thus, increasing the necessity to research potential methods for conserving the protection and security of users and devices of IoT through the design and creation of new technological aspects. According to researchers and authors that will be discussed throughout this thesis, the regulations and security measurements that are available in the IoT-devices that exist today, are not enough to sustain a certain control over the information that is collected through these devices. As a consequence of the development of IoT and the available security features, a breach may have more physical harm than any other previous technology. Therefore, it becomes even more important to find solutions to the security and privacy challenges that users are faced with in their interaction with IoT-devices.

The research question for this thesis is “Which methods are available for allowing users to secure themselves against possible subjective or objective losses of privacy in an Internet of Things environment?”.

Throughout this thesis, the aim is to provide knowledge and awareness for the technology and the challenges IoT faces with the security and privacy issues that have been found in users´ interaction with IoT-devices. The context of the history of IoT will be elaborated to provide a background for the development and its ability to evolve. Additionally, specific security and privacy challenges will be discussed, and possible solutions will be explored. Ownership of the data and information that is collected through these devices will be elaborated in context of the ethical aspect and legal regulations.

The theories that have been chosen for the thesis, are the concept of cognitive assemblages, quantified self, convergence, and sociotechnical perspective. These concepts and perspectives are used as theories as it aims to have a user perspective in context of the Internet of Things. Through numerous articles, researchers have emphasized the lack of responsibility taken by IoT-producers to ensure protection for both users and devices, however, in order to increase the level of protection, there must to be a demand from IoT-users. It is due to users´ choices that security and privacy concerns have been raised. It is through their interaction that these issues occur. Therefore, by maintaining the focus of this thesis on the users of IoT, the desire is to find possible solutions or guidelines to how to ensure a more sufficient protection of users and their personal information without limiting their interactions with IoT-devices.

2. Methodology

The methodology that is used for this thesis is the desktop research which involves previous literature regarding user perspective, Internet of Things, privacy, security, data ethics and data ownership in the Internet of Things. Throughout numerous articles and papers about current issues in the Internet of Things, most of them discuss the responsibility that lays on the producers of IoT-devices, and how the users are vulnerable due to their interactions with these devices. With insufficient security measurements and correct regulations based on clear definitions established by legal authorities, users are vulnerable, and their personal data are available for both internal and external entities. Therefore, this thesis will focus on users in terms of the privacy, security and data ownership issues in the technology of the Internet of Things. Without a proper secure design and production, users are vulnerable from the initial

interaction. However, the entire burden should not be solely on IoT-producers as users of IoT choose to use the device. Several studies that focus on IoT and users, show that convenience and benefits outweigh the importance of privacy. It is therefore interesting to see the motivation behind the usage of IoT-devices, and why IoT-users choose convenience and benefits rather than protecting themselves and their personal information. As a starting point of this thesis, the outlook is that users should take more responsibility for themselves throughout their interactions with IoT-devices, however, without the ability to do so, it is difficult to gain control while taking advantage of the technological developments. Therefore, the thesis will study possible alterations to design and process to increase the level of secure interactions.

Following is a summary of the process of conducting a desktop research and how the literature was analyzed and filtered to find relevant literature for this thesis and its research question.

2.1. Desktop research

The desktop research involves selecting different criteria for what might be relevant or not for the thesis and its research question. The process of desktop research is collecting data about the topic “Internet of Things”, “user perspective”, “privacy”, “security” and “data ownership”, and selecting the relevant literature found during this process. There are different search criteria that contribute to categorizing the collected data to find relevant information. In some aspects, the literature about security, privacy and user perspective in terms of the Internet of Things is limited, therefore, the criteria might be expanded to cover interactive technologies or other digital technologies that might be seen in similar aspects as IoT.

During the desktop research, an important focus has been directed towards the aspect of user perspective as many of the previous literature sources have had a limited focus on the user perspective in terms of the Internet of Things. Many sources have mentioned and emphasized the lack of security and privacy measures in the IoT-devices and outlined that security and privacy have not been a priority in the design process of these devices. With a dynamic

technology such as the Internet of Things, it is important to research and find possible solutions that can contribute to the further development of the technology while ensuring the protection of the users and their personal data. And that is why I have chosen to write about the Internet of Things from a user perspective angle.

2.1.1. Search criteria

To perform desktop research, it is necessary to choose several search terms to filter through the many websites and literature that exist. Primarily, the research will be online. For the outline of the thesis and the research for relevant literature about privacy, security and user perspective in the Internet of Things, the keywords are as following, “Internet of Things”, “IoT”, “privacy”, “security”, “user perspective”, “data ownership” and “ethics”. The search terms have been used separately and together. Mainly the term “Internet of Things” and “IoT” have been searched alongside “privacy”, “security”, “user perspective”, “data ownership”, and “ethics”. Most of the articles and papers that were collected through desktop research state that there is a lack of security measures in terms of protecting and securing users of IoT. There has been an emphasis on the many opportunities due to the Internet of Things, however, many of the literature sources have also highlighted the dangers and risks of a reduced control over personal information while interacting with IoT-devices.

As the thesis aims at examining the complex interactions between users and devices of the Internet of Things, and the vulnerabilities that may occur through these interactions, the main focus is on user perspective, and how IoT-users can take action and precautions in their interaction with IoT-objects. Several literature sources state that there is a lack of security and privacy measures in the design of IoT-objects but in these literature sources, there is a lack of information of how users of IoT are responsible for protecting and securing themselves in their interactions with technology.

3. The history of the Internet of Things

Keith D. Foote states that the concept of the Internet of Things was not officially coined before 1999 (2016). Kevin Ashton, which was at the time an assistant brand manager, coined

the concept of the Internet of Things during a presentation for Procter & Gamble in 1999 (Hoffman et al, 6, 2015). Ashton described how "adding radio frequency identification and other sensors to everyday objects will create an Internet of Things and lay the foundations of a new age of machine perception" (Hoffman et al, 6, 2015). Computers and the Internet are almost solely dependent on human beings for information but due to lack of time, attention and accuracy, there is a limitation of human capability of obtaining data about things in the physical world (Foote, 2016). Ashton wrote an article for the RFID Journal in 1999 where he states that:

> "If we had computers that knew everything there was to know about things, using data they gathered without any help from us, we would be able to track and count everything and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best" (2009).

Ashton´s beliefs were that Radio Frequency Identification (RFID) was the requirement for the Internet of Things, and with the ability to tag all things, computers could track, manage, and inventory them. However, a disclaimer is that to some extent, tagging of items have been achieved through other technologies such as "digital watermarking, barcodes, and QR codes" (Foote, 2016). In terms of the inventory control, there is an advantage in the use of the Internet of Things. This is based on the technology of the Internet of Things as there is a nearly endless supply of opportunities in interconnecting our devices and equipment. However, initially Ashton´s idea was in relation to the supply chain of Procter & Gamble (Hoffman et al, 6, 2015).

To have a better understanding of the technology of the Internet of Things and its possible future, it is important to review not only the history of object-sensing technologies, but also the gradual evolution of social and cultural representations linked with interacting with interoperable objects. The next section will outline and emphasize some of the major events of the IoT history.

3.1. Timeline

According to Andrew Braun, the Internet of Things may seem to be the new technology that has recently started trending (2019). However, since the technology of the Internet of Things is dependent on cheap, low-power components, widespread Internet connectivity, and motivation from both the corporate and the consumer side, it has just recently had the resources to evolve in the rapid speed as it currently is (Braun, 2019). The notion of Internet of Things may apply to widely heterogeneous objects, and range from simple appliances to megastructures, e.g. smart hairbrushes and smart cities. Therefore, the history of IoT is important to address to be able to go in-depth of future challenges and acknowledgement of the Internet of Things. The history will shed light on the leap from having little to none objects connected to the Internet to having more connected devices than people on earth (Braun, 2019).

Braun has highlighted several events in the IoT-timeline as defining moments in the history of the technology. Although developments and other major events have occurred, the timeline has a focus on the major events concerning the Internet of Things. It is important to mention that the timeline Braun has outlined as a major event is solely used as a base for studying the history of the Internet of Things.

One of the x events that is highlighted through the timeline produced by Braun is the year of 1969 which is defined as the beginning. 1969 is the year where the precursor to the modern Internet, ARPANET was developed and used by the U.S Defense Advanced Research Projects Agency (DARPA) (Braun, 2019). ARPANET is claimed to be foundational to the "Internet" part of the Internet of Things (Braun, 2019). Several years later, in the 1980s, the ARPANET was opened to the public which increased the possibility for people to connect objects to the Internet.

3.1.1. The Coca-Cola vending machine

Because of the ARPANET, four programmers David Nichols, Mike Kazar, Ivor Durham and John Zsarnayatat at the Carnegie Mellon University, had the opportunity to connect a

Coca-Cola vending machine to the Internet (Braun, 2019). Jordan Teicher states that some techies “tinkered with a soda machine and made history” (2018). According to Teicher, before there was a modern Internet, there existed a Coca-Cola vending machine that could inform its customers of its content through a network (2018). Seen in the context of the IoT-devices that exist today, connecting a Coca-Cola machine to the Internet may be viewed as primitive. However, considering hardware and protocols that were available at the time, the connected vending machine is viewed as the world´s first IoT-device. David Nichols has stated that the motivation for connecting the vending machine to the Internet was based on several factors such as his fellow students´ need for caffeine, the distance from his office to the vending machine, and its schedule for refills (Teicher, 2018). After proposing his idea to some fellow students, they began working towards an Internet-connected vending machine.

By connecting the vending machine to the Internet, the programmers had the ability to see if the vending machine had cold sodas prior to purchasing them. The earlier challenge with the vending machine was that the vending machine was in a different part of the university than where Nichols´s office was located. Additionally, several fellow students were fond of Coca-Cola, therefore, the vending machine might either be empty, or the content was warm by the time Nichols went to purchase a soda. Although the technology and components that are important elements in the Internet of Things were lacking at the time, the motivation and design-process might be similar to the IoT-devices that exist today and are under development for future use.

The design was based on that several different visual signals were installed on the machine, and those signals would indicate different things such as the amount left in each column, and if the column was full or empty. To obtain this data from the machine, a board which had the ability to sense the amount, was installed. From the board on the vending machine to a gateway on the department´s main computer, there was a line that connected them which transferred the data collected from the vending machine. The main computer was connected to the ARPANET. A program was then written which checked the status of each column´s light a few times per second (Teicher, 2018). The final phase involved dedicated software on to the main computer which allowed anyone connected to the ARPANET or the local Ethernet at Carnegie Mellon to access the information from the vending machine (Teicher,

2018). The result was that they had access to the vending machine to see how many sodas were left and if they were cold before walking to the machine and purchasing a soda.
However, according to Jeff Elder, the vending machine was a wired device (2019). The Internet´s first "thing" was therefore, a toaster.

3.1.2. The Internet´s first "thing"

John Romkey connected the Sunbeam Deluxe Automatic Radiant Control toaster to the Internet in 1990 (Elder, 2019). It could be successfully switched on and off. Romkey was an Internet pioneer who co-authored the first set of communication protocols allowing IBM computers to connect to the early Internet in 1982 (Elder, 2019). The process of connecting the toaster to the Internet was a result of a challenge presented to Romkey. According to Romkey, the toaster was a clever device prior to becoming a "smart" device (Elder, 2019). Romkey stated that "When you put bread into it, it would automatically lower the bread and begin toasting, so all we had to do was control power to the toaster using a big, clunky notebook computer and wire them together" (Elder, 2019). And that is how Romkey connected the toaster to the Internet and made it the Internet´s first "thing".

When Romkey was questioned about his thoughts on IoT, his response was "I have mixed feelings. There are such wonderful possibilities for science, medicine, the environment, and just everyday convenience. And there are such nightmarish science fiction scenarios, particularly around security vulnerabilities that are epidemic in the IoT" (Elder, 2019). Additionally, Romkey emphasizes that the first IoT-device shows that "people have always enjoyed putting ridiculous things on the Internet" (Elder, 2019). What started as a challenge and a further development of the vending machine that was connected to the ARPANET through a line, resulted in the Internet´s first "smart" thing; a toaster.

3.1.3. The Global Positioning System

In 1995, a major event towards providing one of the most vital components for many IoT devices was completed. It was the first version of the long-running GPS satellite program. According to Scott Gurvey, the Global Positioning System became fully operational in 1995 (2015). The GPS receivers obtain signals from revolving satellites which facilitate them to determine altitude and longitude with enough accuracy that it can be used for most navigation

tasks (Gurvey, 2015). In terms of its value in regard to the technology of IoT, the first version GPS satellite program provided location for the IoT-devices, and has been the missing link (Gurvey, 2015). Gurvey described GPS as a one-way communication satellite that broadcasts to client devices (2015). Due to the advanced connectivity that is provided by the Internet of Things, actors can exchange data about positions with servers and other actors (2015). The connectivity of the devices that exist today simplifies the actor requirements due to that GPS continues to determine the users´ position but additionally transmits that data to its servers (Gurvey, 2015). With the development of the Global Positioning System, the cost is reduced for the users and it provides an easier method for real time interaction (Gurvey, 2015).

With the advancements of technologies that combine the different components of the Internet of Things, a more precise phrase was defined in 1999. This was when Kevin Ashton used the phrase “Internet of Things” for the first time.

One of the ultimate IoT devices is the Internet Refrigerator. The idea was that with screens and trackers, the users could keep track of the content in the fridge. It was announced by LG in 2000. James Cook states that despite the idea of an Internet-connected fridge was simple, the interest of the devices has never been high (2016). However, the reduced interest for the device might be due to the high price. The technology of the Internet of Things opens up for many different opportunities in terms of tracking, monitoring, surveillance, efficiency and timesaving.

As a development from when Ashton first used the phrase of the Internet of Things and the many subparts of the IoT was established, the major events concerning the timeline of IoT was more rapid than it had been before.

In 2007, the first iPhone was announced. The iPhone offered a new way for the public to interact with the world and their surroundings, in addition to other Internet-connected devices. The first international IoT-conference was held in Zurich, Switzerland in 2008. The same year, the number of Internet-connected devices increased to surpass the number of humans (Braun, 2019). The development of the Internet of Things and its devices continues from this point; Google starts testing self-driving cars, St. Jude Medical Center releases

Internet-connected pacemakers, Bitcoin starts operations, and the Chinese government names the Internet of Things as a key technology (Braun, 2019).

3.1.4. First major security breach

The history and timeline of the Internet of Things highlights the big positive events in terms of how the different subparts of the IoT have been developed, and how those subparts have been combined into the Internet of Things.
While the emphasis of early inventors was on the potential of connected appliances, the recent proliferation of various devices has raised serious safety, security and privacy concerns.
The first IoT-medical device that suffered a major security breach – The St. Jude´s device case – provides an enlightening case of current and future ethical and political challenges Robertson et al describe how a team of hackers hired by the cybersecurity startup MedSec discovered that St. Jude Medical Inc´s pacemakers and defibrillators had "security vulnerabilities" that could be life threatening (2016). Despite having access to the information, they did not warn St. Jude about the security vulnerabilities. Instead they decided to contact Muddy Waters Capital LLC investment firm, a company run by Carson Block (Robertson et al, 2016). By contacting Block, they saw an opportunity of making a profit of the information illegally obtained from the hack of St. Jude Medical Inc´s pacemakers and defibrillators (Robertson et al, 2016).

Although the security breach did not happen when it was released, it shows an important event in the history of IoT since security and privacy challenges are becoming more common and more regular. Until now, the major events that have been discussed, have shown positive developments and achievements through the development of the Internet of Things. However, as time has shown, several challenges and issues surrounding the IoT have been too difficult for traditional security measures to solve.

3.1.5. New innovative devices (2010-2019)

Braun states that important events between the year 2010 and 2019 have had a focus on further developments of the IoT-device (2019). These devices include self-driven cars, smart thermostats, Google Glass, Amazon's Echo, blockchains, artificial intelligence integration into IoT platforms and increased broadband penetration to mention a few major events (Braun,

2019). The beginning of the timeline shows the major developments of tools and subparts that the IoT-technology incorporate, and how the IoT is defined as well as how it was developed. The development of new innovative devices has been made possible by cheaper, easier, and more broadly accepted material which leads to small waves of innovation all over the industry (Braun, 2019).

According to Sicari et al, the major events in the timeline of the history of the Internet of Things show that it is due to the availability of wireless communication systems such as RFID, WiFi, and 4G that has driven the technology forward (3, 2018). Sicari et al states that currently the concept of IoT is "many-folded" as the Internet of Things involves many different technologies, services and standards (3, 2018). Sicari et al describes an IoT system as "a collection of smart devices that interact on a collaborative basis to fulfill a common goal" (3, 2018). If it had not been for a continuous process and design of the elements that the technology of the Internet of Things incorporates, the producers of IoT would not have the opportunity or ability to further develop those IoT-devices that are used and active today. Due to the technological base that IoT has, the deployments have the ability to adopt different processing and communication architectures, technologies, and design methods, depending on its target (Sicari et al, 3, 2018). Despite the many opportunities retrieved from IoT´s compatibility, the wide scale of the IoT systems may make it more vulnerable to security threats than the current Internet as it increases the possibilities of the interactions between humans, machines, and robots (Sicari et al, 3, 2018).

3.2. Industry 4.0

The motivation behind the Fourth Industrial Revolution is, according to Bill McCabe, a necessity to explore and identify things in high level technology that could contribute to advance the world and enhance the technology (2016). It is stated that the revolution did not occur until 2011, however, that is when the German Federal Ministry of Education and research started to study various trends that were occurring. By researching various trends that were occurring, they could gain the opportunity and ability to simplify the work experience while allowing us to be able to do more in a shorter time (McCabe, 2016). McCabe states that Industry 4.0 is an extension of existing elements (2016). Due to the beginning of the research

in 2011, the Germans had collected much research by 2012 and based on the collected data, they had the opportunity to present the collected data on the subject to potential customers and industry professionals (McCabe, 2016). With a better understanding of the potentials of the Internet and the power of the Internet, the use of information relay over the Internet helped to further push the Internet of Things (McCabe, 2016). In 2014, other companies outside of Germany began the same process and provided more virtualization and input that further effective work solutions were created (McCabe, 2016). It is because of the several actors that contributed to the process that the Internet of Things became aligned with the industrial revolution (McCabe, 2016).

The revolution of Industry 4.0 has contributed to new things evolving such as advanced medical technology, effective cost saving mechanics for production plants and more (McCabe, 2016).

3.3. Technical components of the Internet of Things

It is important to highlight the element of heterogeneity of IoT devices and heterogeneous environment in the IoT technologies. The vulnerabilities of these specific components are also addressed. Alhalafi et al states that the Internet of Things consists of a huge network of interconnected networks with devices that are constrained by the resources embedded in them (2, 2019). Due to the scarce resources in the IoT-devices, they are not able to take advantage of the complete “security suites” which are typically used in networks (Alhalafi et al, 2, 2019). Within the IoT, there are interconnections of several networks. In terms of the technologies that are used in the IoT, there are several core technologies that support it. Amongst them are Radio Frequency Identification (RFID) which have been mentioned previously, Near Field Communication (NFC), and Wireless Sensor Network (WSN) (Alhalafi et al, 3, 2019). As stated by Alhalafi et al, the usage of RFID in IoT enables IoT-objects to have smart chips that contribute to the ability of the object to sense information in their surrounding environments, compute and communicate with other devices or human beings (3, 2019). Although there are advantages of using the RFID, the component is more prone to denial of services, eavesdropping, skimming, relay and side channel attacks which may jeopardize the security and privacy of IoT-users (Alhalafi et al, 3, 2019). Which leads to the use of WSNs as they are preferred in this type of application due to cost effective,

efficient, consume low power, and capabilities within both intelligent and processing elements (Alhalafi et al, 3, 2019). The WSNs support remote sensing application and information collection in IoT networks. WSNs are vulnerable for wormhole, neighbor discovery, ping lood, ICMP, flood and syn flood attacks (Alhalafi et al, 3, 2019).

The technology of NFC is used for supporting the communication within a small distance of a few centimeters with low power and data rate needs such as communication with smart cards and access control (Alhalafi et al, 3, 2019). NFC is prone to phishing, user tracking, relay and data forging attacks (Alhalafi et al, 3, 2019).

3.3.1. Interoperability

Keyur K. Patel et al classifies IoT into three types of interaction categories; People to people (P2P), People to machine/thing (P2M(T)) and things/machine to things/machine (T2M); interacting through the Internet (1, 2016). The categories the technology of IoT is classified into describes the ability the technology has to interact and communicate with many different elements and across boundaries that have been difficult to communicate through before. An important aspect of the Internet of Things is interoperability. The IEEE standard glossary of software engineering technology defines interoperability as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged"[1]. According to Mahda et al, the current IoT market is disintegrated because of "the extreme degree of heterogeneity in device protocols, controllers, network connectivity methods, application protocols, standards, data formats and so on" (3, 2018). Additionally, the authors state that the shortage of interoperability in IoT is because of the lack of standardization (3, 2018). Producers are deliberate designing and defining different IoT platforms, protocols and interfaces in such a way that they are incompatible with solutions produced by other IoT-producers (Mahda et al, 3, 2018). Different verticals and mostly closed ecosystems are designed; these are often called "stove pipes" or "silos" whereas "the components in one silo do not have the ability to communicate with the components in another silo" (Mahda et al, 3, 2018). An example of the missing link in communication between the components can be seen in the need of a dedicated application which is preloaded onto the smartphone prior to access to the different smart things (Mahda, 3, 2018). Based on

[1] IEEE Standard Glossary of Software Engineering Technology

that, IoT-users will have many devices, each with their own application that is working independently of each device (Mahda, 3, 2018).

3.3.1.1 Interoperability classification in the Internet of Things

Mahda et al have classified the several levels of interoperability in the IoT as device level interoperability, network level interoperability, syntactic level interoperability, semantic level interoperability, cross-platform interoperability, cross-domain interoperability (6, 2018). Based on the classification of interoperability, Mahda et al suggest that at device level gateways and smartphone solutions are the main method to address the connectivity issues, in terms of networking level, IPv6 and other standard technologies such as SDN, NFV and Fog are suggested as possible solutions (9, 2018). In the Syntactic and Semantic perspectives, web technologies such as open APIs, RESTful web services, JSON-like dictionary, mashups and semantic web technologies which are able to provide a high degree of interoperability, are mention (Mahda et al, 9, 2018). Cross-platform and cross-domain which are seen as higher level, could take advantage of collaboration and agreement between IoT-producers to achieve interoperability (Mahda et al, 9, 2018).

3.4. Established characteristics of IoT

As a precondition to analyze the Internet of Things and the user perspective with an emphasis on privacy, security and data ownership, it is necessary to establish the different characteristics that are required to have the definition as an IoT technology. For this thesis, the following characteristics have been established as a baseline for the Internet of Things technology. The established characteristics are collected from different definitions of the technology and its abilities for interactions and interoperability.

3.4.1. The Internet of Things definition

There are several definitions of the Internet of Things, ranging from a global infrastructure for the information society, a technology that allows people and things to be connected but the most agreed upon definition, is that the Internet of Things is created to increase information sharing that leads to a better world for all human beings. Although an opportunity to increase

information sharing is a positive element, it is necessary to stay aware of the consequences that may occur alongside these opportunities. Through the act of integrating an IoT-device into everyday life, there are several aspects that should be considered. Despite the increased amount of opportunities given with an IoT-device, there may be some issues in that same transaction. The definition of transaction that is used in this thesis, refers to the act of giving something up in order to gain something else.

Atlam et al states that in the system of the Internet of Things, there is an involvement of "realizing a global infrastructure of interconnected networks of physical and virtual objects" (4, 2019). These objects that are discussed in terms of the Internet of Things are interconnected, through wireless networks. They have the ability due to their interconnectivity, to share information across various IoT-devices. In the wake of these interconnections, new "novel applications and services" are created (Atlam et al, 4, 2019). The aim behind the technology of the Internet of Things is to improve the quality of people's lives by generating new applications that facilitate daily activities, hence the optimization of everyday activities and tasks (Atlam et al, 4, 2019). Atlam et al states that there are a set of essential characteristics to classify the technology of the Internet of Things (4, 2019). These range from large scale, intelligence, sensing, complex system, dynamic environment, massive amount of data, heterogeneity, limited energy, connectivity, self-configuring, unique identity and context awareness (Atlam et al, 4, 2019). It is necessary to mention that it is due to these features that the IoT-devices have interfaces that enables users to collect the required information from the devices, record their status and manage them remotely.

A world where the digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent (Patel et al, 1, 2016).
The Internet of Things refers to the general idea of things with an emphasis on everyday objects that are readable, recognizable, locatable, and addressable through information sensing devices and/or controllable via the Internet, regardless of the meaning of the communication (Patel et al, 1, 2016). Patel et al highlight that the everyday objects that are outlined in terms of IoT are not the typical things we ordinarily think of as electronic devices but objects such as food, clothing, chairs, animals, trees, water, and etc. (1, 2016). Below is an illustration showing the application domains of the Internet of Things. Besides the

fundamental applications that are shown in the illustration, there are several distinct applications. Within these are smart homes, smart grids, connected cars, industrial IoT, smart supply chains, smart retail, smart banking, smart investment, smart insurance and smart farming (Tzafestas, 3, 2018).

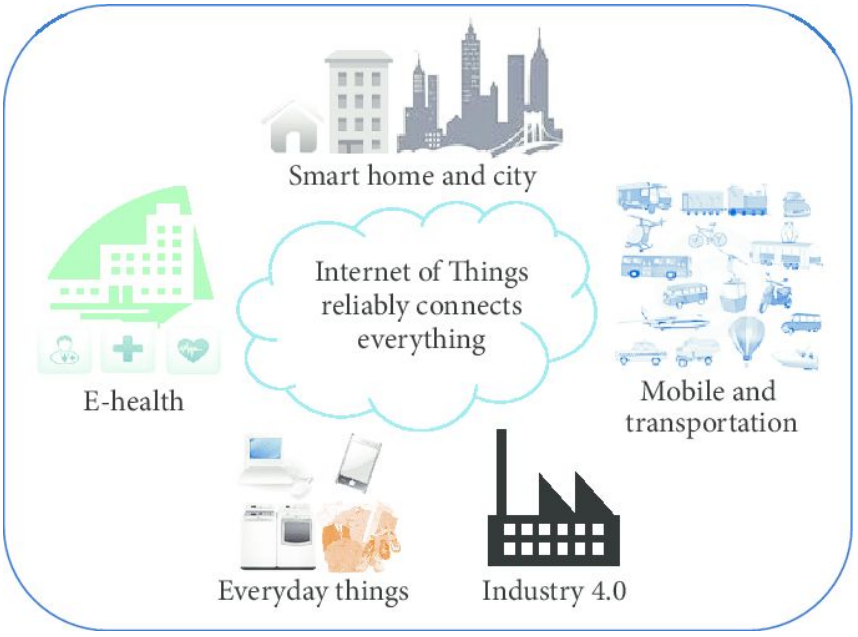

Illustration 1.0: Application domains of IoT. Source: "Multipath Load Balancing Routing for Internet of Things" (Tseng, 2016).

The characteristics of the assemblage of various items, e.g., protocols, hardware interfaces, and information architectures which in this thesis will be considered as constitutive of the technology of the Internet of Things (IoT) and its devices, will be distinguished from other various devices and technological architectures that may seem closely related, or even incorporate aspects of IoT, but do not exhibit the same global characteristics, and as a consequence, may not be qualified as IoT

Illustration 1.1 of the linkability of the Internet of Things. Source: "Securing Your Internet of Things (IOT)" (Blakes, 2017).

4. Theoretical perspectives on the Internet of Things

The theories that will be used in this thesis will focus on cognitive assemblages, quantified self, convergence, and socio-technical perspective.

4.1. Cognitive assemblages

In the book "Unthought", Katherine Hayles distinguishes between "thinking" and "unthought" with a focus on consciousness and unconsciousness (1, 2017). Discoveries in neuroscience have confirmed the existence of nonconscious cognitive processes. Hayles suggests that there are rich possibilities with nonconscious cognition in terms of the conceptualizing interactions between humans and technical systems that contributes to a better understanding of the political, cultural and ethical stakes of developed societies (2, 2017). In the term "thinking", Hayles writes about the thoughts and capabilities that are associated with higher consciousness (2, 2017). Previously, the focus has been on consciousness, however, there has been an increase in scholarly interest about the element of unconsciousness and its power. To be able to understand the full extent of it, a radical

rethinking of cognition is necessary (Hayles, 1, 2017). Rich possibilities may be opened when nonconscious cognition is considered, thus the conceptualizing interaction between humans and technical systems. Hayles has defined "consciousness" as "an awareness of self and others shared by humans, many mammals, and some aquatic species" (9, 2017). Higher consciousness has been reinforced through verbal monologue which emerges "the self-aware of itself as a self" (Hayles, 9, 2017).

Hayles explains the conceptualizing interaction between humans and technical systems through the act of turning on a cell phone (2, 2017). The human becomes part of a "nonconscious cognitive assemblage" that consists of relay towers, network infrastructures (switches, fiber optic cables and wireless routes) and other components (2, 2017). However, when the cell phone is shut off, the infrastructure still exists, however, the human subject is no longer part of that cognitive assemblage (Hayles, 3, 2017). With the term nonconscious cognitive assemblage, Hayles refers to a term that includes technical and human cognizers (2, 2017). The power of such assemblages, is according to Hayles, maximized when functioning as a system, consisting of "well-defined interfaces and communication circuits between sensors, actuators, processors, storage media, and distribution networks (2, 2017). Included in these components are humans, biological, technical and material components (Hayles, 2, 2017). Thus, implying that for a maximized force, the human and the technical systems have to participate alongside each other. This is reinforced by the importance of understanding the specificities of human-technical cognitive assemblages and their ability to contribute to an alternation of life on the planet.

As a disclaimer, within neuroscience and cognitive science, nonconscious cognition is not a new concept but contains more power than realized. However, nonconscious cognition is being recognized as an important component of the human cognitive activity, and not only the conscious cognition. It is due to the limitations of consciousness that have driven the research towards other cognitive capacities forward as they attempt to understand the human neurological processes (Hayles, 9, 2017). The term "cognition" refers to a broad capacity that extends beyond consciousness into other neurological brain processes, in both other life forms and complex technical systems (Hayles, 9, 2017). A process of interpreting information in such a way that it is assigned with meaning (Hayles, 118, 2017). The notion of cognitive

assemblages, is according to Hayles, used to describe complex interactions between human and nonhuman cognizers, and their abilities to enlist material forces (115, 2017). In a cognitive assemblage approach, properties such as flexibility, adaptability and evolvability, are considered from a systemic perspective as "an arrangement of systems, subsystems, and individual actors through which information flows, effecting transformations through the interpretive activities of cognizers operating upon the flows" (Hayles, 118, 2017). According to Hayles, it is important to understand the "specificities of human-technical cognitive assemblages and their power to transform life on the planet" (3, 2017). The reasoning behind its importance, is due to dilemmas related to the development of technical autonomous systems and the human aspect. With complex human-technical assemblages, the cognition and decision-making powers are distributed through the relation between human and technical systems, and thus cannot eliminate one aspect of that relation (Hayles, 3, 2017). Hayles have stated that computational media is the "quintessentially cognitive technology" and that human are the "quintessentially cognitive species", and the established relationship between them creates a complex interaction (34, 2017). As an advantage of cognitive capabilities, computational media have a "stronger evolutionary potential than any other technology" due to its "smart" capabilities that provide methods of integration into other technologies (Hayles, 34, 2017). Based on these statements provided by Hayles, it suggests that there is a need to study and research the complex interaction between computational media and humans, and the factors that may affects their communication, and thereby the result of said communication. Lastly, Hayles emphasize that the bigger the cognitive components of a technological system, the more unpredictable are their specific developments such as flexibility, adaptability and evolvability. The Internet of Things is a great example of cognitive components and developments.

4.2. The Concept of quantified self

According to Deborah Lupton, the concept of self-tracking is the act of which people are able to record specific features of their lives by using digital technology to monitor, evaluate and optimize themselves (2, 2016). Self-tracking may also be referred to as lifelogging, personal analytics and personal informatics. The data that is collected through self-tracking is analyzed, interpreted and visualized in form of statistics, graphs or other data visualizations to

understand the collected data, and determine how the data can provide insight for the user´s life. The act of self-tracking involves users confronted with their own personal information and that in many cases, are invited to engage with this information in a manner of optimizing and improving their lives (Lupton, 4, 2016). They are, therefore, engaging in self-surveillance. Jill Walker Rettberg states in "Seeing Ourselves Through Technology" that the slogan of the Quantified Self Movement is "Self Knowledge Through Numbers" (73, 2014). By having the ability to measure something, it may give the sense of control (Rettberg, 72, 2014).

Self-tracking and the collection of data are implemented in many different social contexts and institutions such as workplace, education, medicine and public health, insurance, marketing and commerce, energy sustainability initiatives, the military, citizen science, and urban planning and management (Lupton, 4, 2016). Digital self-tracking challenges the boundaries between public and private surveillance as public surveillance is brought into the domestic sphere, at the same time as extending the private surveillance into the public domains (Lupton, 4, 2016). The choice to participate becomes limited as the boundaries between public and private are blurred. Lupton has classified five modes of self-tracking that have, in her opinion, emerged in recent times; private self-tracking, pushed self-tracking, communal self-tracking, imposed self-tracking and the exploited self-tracking (4, 2016). These five modes define and distinguish how self-tracking has become diversified.

4.2.1. Smart objects contribute to an extension of self-tracking

The continuous development of mobile, wearable digital devices and associated software have contributed to provide more insight of the collected data from the user´s life and has made it possible to collect, analyses, search, aggregate, visualize and compare information more rapidly than before (Lupton, 3, 2016). Mobile digital devices, devices and environments equipped with digital sensors, have increased the possibilities for data archiving and sharing and cloud computing have contributed to the ever more detailed measurement and monitoring of people´s activities, bodies and behaviors in real time (Lupton, 5, 2016). Self-track may either directly use the devices that users interact with, wear on their bodies, or software for their mobile or desktop computer, in addition to that they may generate data from "smart" objects in which the users engage with (Lupton, 5, 2016). The increased number of "smart"

objects provides higher capabilities of self-monitoring. This can be seen in terms of how smart vehicles can monitor driving habits, mattresses can monitor sleep patterns, chairs can sense physical movements, and homes can monitor its inhabitant´s movements. These examples are emphasized to provide insight to some of the particular "smart" objects and what their capabilities are in monitoring people's personal information (Lupton, 6, 2016).
Due to the development of the Internet of Things, some of the "smart" objects have the ability to exchange data with each other. Lupton suggests that the concept of "self"-tracking may be extended well beyond the individual human body (6, 2016).

Digitized self-tracking promotes a culture of dataveillance. Dataveillance exploits different methods. Among these, are two types of dataveillance that need be distinguished from each other; the first being dataveillance that is undertaken for self-tracking purposes. The second type of dataveillance that uses monitoring technologies incorporate methods which people may be unaware of. These methods are, e.g., closed-circuit television (CCTV) camera and sensors, monitoring people's movement in public space, national security agencies and policing bodies´ surveillance of communication metadata and Internet companies´ commercial data-harvesting activities (Lupton, 3, 2016).

Lupton states that the culture of self-tracking has emerged in a socio-cultural context in which "various rationales, discourses, practices and technologies are converging" (14, 2016).
Lupton also situates self-tracking in a wider context, emphasizing

> "concepts of the self that value self-knowledge, self-awareness and self-entrepreneurialism; a moral and political environment in which taking responsibility for one's life as an individual rational actor is privileged and promoted; the development of audit culture; the capacity of digital technologies to monitor an increasing array of aspects of human bodies, behaviours, habits and environments; the spread of surveillance technologies and diversification in their use; the metricization and datafication of an increasing range of human and non-human phenomena; the emergence of the digital data knowledge economy, in which both small data and big data are valued for their insights and have become tradable commodities; and the realization on the part of government, managerial, security, commercial and criminal

> actors and agencies that the data derived from self-tracking can be mobilized for their own purposes“ (15, 2016).

Furthermore, the phenomenon of self-tracking contributes in various ways the participation of digital technology in the configuration of “selfhood, embodiment and social relations” (Lupton, 15, 2016). The digitization of bodies and selves are increasing in a multitude of ways, and digital self-tracking devices and software recording personal information are claimed by Lupton to only be one element of the process (15, 2016).

Deborah Lupton mentions that data assemblages which are produced by data practices as an outcome of self-tracking as self-tracking is viewed as an “active” data practices unlike the “passive” forms of personal data collection that are viewed as characteristic of other forms of transactional user interaction with online technologies (15, 2016). Lupton classifies data assemblages as a complex socio-technical system which is composed of many actors that are mainly concerned with data production (15, 2016). Data assemblages are always alterable, effective, and conscious to new inputs and interpretations. It is through the configuration of data assemblages that detailed profiles about users are formed by leveling out the heterogeneity of the information. In regard to self-tracking, data assemblages are configured through “systems of thought, forms of knowledge, business or government models, human users, practices, devices and software, and sometimes by networks of other users and agents other than the self-tracker himself” (Lupton, 15, 2016). Despite the practices that began as personal and private, the different ways the digital data are generated, stored, managed and used once they are digitized, the data becomes complex and enfolded within these networks and economies (Lupton, 15, 2016).

Despite the fact that the majority of the data generated through self-tracking are proposed for the users and how they can use the generated data to change their lives or obtain a better knowledge about themselves, there is little to no knowledge about who can access their data or use it. The project of what Lupton calls “reflexive self-monitoring” involves reflection on the intended usage of the data, the validity of the data, how to display or visualize their data and obtain insights from their personal data (17, 2016). Beyond the process of reflexive self-monitoring, there are some self-trackers that go in-depth beyond the generated data to

understanding where their personal data are algorithmically generated and stored, how the data may be obtained by others and what these actors may use their personal data for (Lupton, 17, 2016). These self-trackers collect their personal data in critical and resistant ways, as a method to obtain a control over their own data to have a clear view of how much control they have over their own information. The methods that are used to maintain a certain control, are generating and controlling their own algorithmic identities in their process of dataveillance. Lupton states that these practices of maintaining control over their own personal data are a response to a "growing awareness of the ways in which personal data are structured, archived and appropriated by commercial, criminal, government or surveillance agencies" (18, 2016). Despite a personal interest in themselves through self-tracking, they are becoming gradually aware of how their personal data are becoming used for commercial purposes (Lupton, 18, 2016).

Following different studies performed by Lupton has performed in order to explore personal data practices and understandings, the findings suggest that the users have a vague idea about the usage and exploitation of their personal data by actors (18, 2016). However, there is uncertainty regarding the details surrounding the matter and what options they have available to protect themselves and their personal data.

4.3. Convergence

Fantana et al states that integrated environments that are capable of running a diversity of user-driven applications and connecting various sensors and objects, are limited (18, 2017). Such integrated environments are currently missing, developing these sorts of environments may be a method of developing the Internet of Things ecosystems. According to Fantana et al, open APIs might offer a variety of channels for the delivery of new applications and services. It is emphasized that open APIs are important to separate the level of abstraction for different application-specific data analysis and processing, at the same time as allowing application developers to influence the underlying communication infrastructure, use and combine information generated by various devices (Fantana et al, 2, 2017). The same authors state that by allowing developers to influence communication infrastructure, it will contribute to producing added value across multiple environments (Fantana et al, 2, 2017).

The overall goal of IoT is “to create and foster ecosystems of platforms for connected smart objects, integrating the future generation of devices, network technologies, software technologies, interfaces and other evolving ICT innovations, both for the society and for people to become pervasive at home, at work and while on the move” (Fantana et al, 20, 2017). Additionally, it is stated that integrated environments will contribute to an increased effectiveness, efficient security, and privacy mechanisms into various devices, architectures, platforms, and protocols (Fantana et al., 20, 2017). Including characteristics such as openness, dynamic expandability, interoperability of objects, distributed intelligence, and cost and energy-efficiency (20, 2017).

Medina-Borja states that there is a growing interest in reducing the issues connected to the effective implementation of smart environment, smart cities, smart health, and smart infrastructure. Some of the suggested solutions is by applying a service framework to the interaction of technologies with each other and with humans (1, 2015). The possibilities of having interactions between different technologies and humans have been enabled by important advances in sensing, actuating, and computational and communication technologies. It is on behalf of these advances that Medina-Borja claims that a house may have the capabilities of learning the behavioural patterns and preferences of its residents, and thereby, adjusting certain aspects of their houses in order to meet the preferences of its resident (1, 2015). The capabilities discussed by Medina-Borja are based on the convergences where there is an increased interaction between smart objects, technologies and humans. However, as a disclaimer, it is necessary to mention that this process may already be happening to some extent. Smart objects may in the future have cognitive capabilities that will allow them to know their owner´s preferences and behavioural patterns in such a way that they are able to customize their “service” (Medina-Borja, 1, 2015).

Eloff et al defines the Internet of People, Things and Services (IoPTS) as a vision where people, things, and services are logically integrated into networks of networks as active participants that exchange data about themselves and their interpreted surrounding environments over a web-based infrastructure (2, 2009). The characteristics of the IoPTS is its massivity which can be seen in terms of people, services and things that generate information

which supports massive databases (Eloff et al, 2, 2009). IoPTS have advanced capabilities of tracking people, objects and things with a focus on multiple frontiers (Eloff et al, 2, 2009). The authors emphasize that with the unlimited personal, thing and service content distribution the boundaries for regulation of actors are blurry (2, 2009). The current approaches are not equipped enough to provide trustworthy infrastructure that provides secure protection of the data and privacy for personally identifiable information of individuals in the era of IoPTS (Eloff et al, 2, 2009).

4.4. Socio-technical perspective

Ngowi et al states that a socio-technical system involves a complex interaction between technology and the social subsystems (1, 2018). The main aim of the theory of socio-technical systems is optimization of the results from such interaction by designing systems that are able to adapt to the needs of human and complex social environment requirements in contrast to humans adapting to the needs of the system (Ngowi et al, 1, 2018). According to Ngowi et al, the majority of the factors that influence the systems are social components being open-ended and able to adapt to changing environments such as “culture, organization, the context of use, usefulness, policies, and regulations” (1, 2018). The concept of Socio-Technical systems was developed by the Tavistock Institute of Human Relations to further develop processes for “improving user satisfaction, enrich work practices, add value and include humanistic ideas in work processes” (Ngowi et al, 1, 2018). According to Medina-Borja, service systems can be described as sociotechnical configurations of people, technologies, organizations, and information designed to deliver services that create and produce value (1, 2015).

4.5. Merging of the theoretical perspectives

Concerns regarding privacy, security and ethical aspects in digital technologies have not recently occurred but the development of digital technologies such as the Internet of Things which emerges from the physical and virtual world, are reinforcing the importance of studying the complex interactions between humans and technical systems. The impact of these concerns regarding IoT may be more alarming than those concerning previous digital technologies as the characteristics of IoT allows for a more intrusive presence in the humans´ physical sphere. Therefore, it increases the necessity to understand the relationship between

humans and technological systems to enforce the positive elements and eliminate the negative aspects that may occur in the interactions between digital technologies and humans. Through the interactions between humans and technical systems, humans become part of the unconscious cognitive assemblages, and the potential power of such an interaction, is maximized when functioning as a system. Cognitive assemblage is an important aspect that should be central through the research and elaboration of the privacy, security and ethical issues that are occurring in the interactions between humans and the Internet of Things.
The quantified self suggests that it exists a major interest in the act of self-monitoring to learn more about yourself, thus increasing the importance of understanding the complex relationship between humans and technology. With the limitations of integrated environments that are driven by users and include various sensors and objects, an increase in such environments may be a method of incorporating effectiveness, efficient security, and privacy mechanisms into various devices, architectures, platforms, and protocols. Integrated environments should be a focus as the interactions between smart objects, technologies and humans are considerably increasing. Smart objects are developed with an aim to be easily integrated into users´ everyday lives, and such integration reinforces the concerns regarding the privacy and ethical challenges that occur through human interaction with the Internet of Things.

The theories of cognitive assemblages, quantified self, convergence and socio-technical perspective that have been elaborated in this chapter, will be discussed in more depth in context of the Internet of Things alongside the challenges that IoT-users are confronted with throughout their interactions with smart devices.

5. Emerging challenges affecting privacy

Daniel Solove states in “Understanding Privacy” that privacy is a broad concept as it covers many different elements such as “freedom of thought, control over one's physical body, solitude in one´s home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations” (13, 2008). Although the concept is difficult to define and concretize, privacy is an essential issue for

freedom and democracy (Solove, 13, 2008). Solove suggests that to have the ability to solve some of the issues regarding privacy, it is necessary to develop an approach to help guide policymakers and legal interpretations. Despite laws regarding privacy, there are numerous failures and difficulties solving the challenges of privacy (13, 2008). Due to the challenges of defining the concept of privacy, it becomes more difficult to assess the level of vulnerability when privacy is threatened, and which legal actions are necessary to solve these issues. According to Solove, it is due to the difficulty in defining the concept of privacy and its importance that privacy laws are ineffective (13, 2008). In some cases, oblivious to the functions the privacy laws should serve in such matters.

5.1. Privacy in countries around the world

Privacy is preserved as a fundamental right in the constitutional law of countries around the world (Solove, 13, 2008). As a disclaimer, Solove emphasizes that in the U.S. Constitution, the word "privacy" is not explicitly mentioned but is featured as "the sanctity of the home and the confidentiality of communications from government intrusion" (13, 2008). The debate about issues of privacy have been pursued for decades on a scale from gossip to eavesdropping to surveillance (Solove, 16, 2008). Although the development of new technology has been continuous, the new information technologies during the twentieth century have made privacy a frontline issue around the globe (Solove, 16, 2008).
It has been emphasized that when there is attention drawn to the threats against privacy and the focus is on protecting privacy, it is uncertain as to what is meant by 'protecting privacy'. That itself is a challenge. A well-defined definition of privacy is needed in order to establish laws and regulations to be able to protect the privacy of individuals and private groups. Without privacy laws and regulations, there are enormous uncertainties about how the protection of privacy should be handled. With a foundation that is unclear and uncertain, it creates more challenges and issues along the way.

The literature that is referred to, is mainly retrieved from an author that views privacy from a western viewpoint, therefore, to be able to have an overview of the privacy regulations around the globe, it is necessary to mention privacy regulations in different countries. Since it is not

possible for this thesis to discuss every country, countries that may have different regulations than the western world, have been chosen. Additionally, a western viewpoint besides the US is elaborated. The aspect of incorporating different regulations and maintaining different human rights can be seen in context of the covid-19 pandemic and the legal authorities´ engagement in personal information. A clear distinction between western and eastern parts of the world is that governments in eastern parts have demanded the use of tracking-applications while the western part of the world have encouraged rather than demanded. The cultural aspects of each country have an impact on the definitions and legal regulations of data protection privacy. The following is a short elaboration of said legal regulations in some countries in the eastern part of the world and the EU.

5.1.1. China

“China Internet Security Law” is a regulation to increase cybersecurity and national security and is applicable to network operators and businesses which are in critical sectors such as telecom, information services, financial services, and so on (Aruba, 2019). In November 2018, controversial clauses were added, and this clause allows state agencies the legal authority to perform inspections on network security of China-based companies without informing the companies (Aruba, 2019). As for foreign companies, they are required to store their data on Chinese-regulated local services which intel that they must cooperate with Chinese national security agencies if requested. Hence potentially creating a vulnerable situation for foreign companies as for business secrets and sensitive information (Aruba, 2019).

5.1.2. Singapore

In February 2018, Singapore signed the law “Cybersecurity Bill” which acts as a framework for data privacy for providers of information infrastructures (Aruba, 2019). Through Singapore's “Personal Data Protection Commission” (PDPC), a mandatory breach notification is considered to decrease the consent requirements on data controllers (Aruba, 2019).

5.1.3. South Korea

South Korea is viewed as one of the toughest countries in the world on data protection and privacy compliance. The law "Personal Information Protection Act" contributes to provide an "overarching guidance" and is additionally supplemented by several sector-specific laws (Aruba, 2019).

5.1.4. India

In 2018, a bill called the "Personal Data Protection Bill" was introduced. The bill aims at providing a framework to protect personal data of individuals and thus creating trust between people and the external entities that processes their personal data (Aruba, 2019). The bill was approved by the Indian Parliament in 2019, which suggests that India is attempting to preserve data privacy rights.

5.1.5. EU Data Protection Directive (DPD)

The EU Data Protection Directive (DPD) was adopted by the European Union in 1995 and is officially labelled "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (Lord, 2018). It aims at regulating how personal data is collected and processed in the European Union. According to Weber, the EU Data Protection Directive has attempted to influence the processing of data but solely if the collected data is defined as personal data (2, 2015).

The regulations decided by the DPD target certain types of information and in the case of the Internet of Things, the definitions established by the EU DPD are not sufficient nor relevant enough to secure the IoT-users´ privacy (Weber, 2, 2015). However, as a disclaimer, the EU has adopted a law called the General Data Protection Regulation (GDPR). In terms of Norway, the law was implemented July 2018 by the EU. The GDPR is a law that aims at regulating how personal information is processed by actors and is used as an instrument for better securing individuals[2]. The methods and processes of collecting and storing personal information about consumers are affected by the GDPR as it implements regulations for

[2] GDPR and privacy

companies and actors in how they collect, process and store personal information. It is stated that it is not prohibited nor dangerous to process, collect and analyze personal information but there are certain rules and regulations that are required by the GDPR[3]. An article on the website "GDPR Today" states that with an increase in the popularity of IoT-devices, the interaction with GDPR is increasing at the same rate (2019).

There is an increase of data protection requirements but as shown through this short summary of the data protection laws in China, Singapore, South Korea, India and the EU, there is not a global standard across the world. This creates challenges in defining a globalized standard to ensure that IoT-users and their personal information are protected through their interactions with the devices. With different countries following different rules of conserving data privacy rights, it is difficult to maintain a certain level for regulations as every country has different views on the subject.

5.2. The dilemma of convenience vs. privacy

According to Solove, countless commentators have announced that privacy is under "attack" (17, 2008). Nelson states that "Privacy, it seems, is not simply dead. It is dying over and over again" (quoted by Solove, 17, 2008). Despite numerous statements about threats on privacy, some argue that due to people's actions, it may seem as though privacy is not an important factor. Franzen states that "The panic about privacy has all the finger-pointing and paranoia of a good old American scare, but it is missing one vital ingredient: a genuinely alarmed public. Americans care about privacy mainly in the abstract" (8, 2002). Solove states that according to polls, the indications are that people "care deeply" about privacy, personal information and intimate details about their lives, and how they are willingly given out on the Internet (17, 2008).

Solove emphasizes a statement from a Canadian scholar Calvin Gotlieb as he declares that "most people, when other interests are at stake, do not care enough about privacy to value it" (Solove, 17, 2008). Another element in the discussion is that the concept of privacy is unclear and undefined, in terms of genuinely understanding the concept. When there is a claim that privacy should be protected, it is "unclear precisely what they mean" (Solove, 19, 2008). The

[3] GDPR and privacy

lack of clarity surrounding the concept of privacy contributes to difficulties in the process of establishing policies or resolving cases due to the challenges comprehending the privacy harm (Solove, 19, 2008). As a result of these challenges, Solove claims that privacy is not balanced equally in terms of other interests (20, 2008). The value of privacy must be determined based on its importance to society, not in terms of individual rights.

Serena Zheng et al have conducted a study with eleven semi-structured interviews with smart homeowners (1, 2018). For the study, the authors have focused on four key elements in context of privacy; convenience and connectedness, user opinion about the collection of data by external entities, Users trust in IoT device manufacturers and the users´ awareness of privacy risks in relation to inference algorithms that collect data from non-audio and visual devices (Zheng et al, 1, 2018). Within their definition of smart home IoT, they have included learning thermostats, energy tracking switches, video doorbells, smart baby monitors, and app-and voice-controlled lights, shades, and speakers (1, 2018). Through the description of their study, they have emphasized the increasing popularity of smart home IoT-devices, and the increasing concerns related to privacy and smart home IoT. The concerns Zheng et al have focused on are storage, usability, data ownership, and who has access to create, manage, track and regulate IoT-devices and its collected data (1, 2018). According to Zheng et al, the market for smart home devices has minimal regulations or standards for protecting the privacy of the users (2, 2018). With an increase in IoT-devices, a clarification of the privacy implications is very important to raise awareness of. A clarification of potential privacy risks may contribute to a possible minimization of risks without laying the burden of protecting themselves and their personal information solely on the users (Zheng et al, 2, 2018). The results from the study indicate that potential benefits outweigh users´ privacy. This will be discussed further in chapter 8.

5.3. Privacy in the Internet of Things

The concept of privacy is an important human right in many different countries around the world as it is meant to protect individuals and their personal information in a society filled with many elements that are uncontrollable. Personal data should be regulated and controlled by the individuals themselves, and every action taken using these data should be approved by

the people that it belongs to. However, when the definition and the concept of privacy is unclear and undefined, the action of controlling and protecting one's personal information is difficult. Especially when the users that generate the data are not aware of which actors have access to their data, the usage of their data and by whom has access to share and analyze it. As technologies develop alongside the development of society, more sensors and video cameras are being used, both in private and public spaces. Based on the increased use of these types of equipment and collection of data, the citizens have a decreasing knowledge about what is collected where, and what the collected data is being used for. Alongside the lack of information regarding the collected data and how the data is collected, the citizens have limited methods of avoiding this technology (Foote, 2016).

As regards to the use of IoT devices, the desire to use the product might outweigh the need to protect personal information and privacy. The possible negligence of IoT-users may be related to the fact that their awareness of the lack of privacy regulations and security measurements when interacting with IoT-devices may be minimal. If there is only a small number of IoT-users who are aware of the privacy and security issues surrounding the devices, such users may not be fully aware of the vulnerabilities they are exposing themselves to. The desire of using IoT-devices might be greater than the need of protecting their privacy.

The development of new technologies should be accompanied by corresponding efforts to strengthen the protection of privacy of individuals. A more efficient and widespread protection has become even more challenging with globally networked information technologies, among these, the Internet of Things. Elisa Bertino writes that due to the technological elements of IoT-technology, the human body is becoming a rich source of information (2, 2016). The information often contains metadata such as location, time and context. Therefore, due to the large amount of collected data, it becomes easier to gain more knowledge about the users such as personal habits, behaviors and preferences (Bertino, 2, 2016). Aspects highlighted by Bertino’s statement about the human body being a rich source of information will be discussed in more depth in chapter 8.

According to Yun Shen et al, IoT-devices have many vulnerabilities and flaws in the design (1, 2019). Therefore, there is an increase of IoT specific malware which affects the security and privacy of the IoT-users in their interaction with IoT-devices (Shen et al, 1, 2019).

Despite an increase of IoT specific malware, IoT-producers have until now neglected to strengthen these requirements for a secure use of the devices.

In the context of IoT, it is necessary to operate with more adapted privacy requirements addressing both data protection and user personal information, e.g. confidentiality, as many of IoT-devices obtain sensitive information from individuals and private groups. In the users´ interaction with IoT-devices, they should be able to require protection of their personal information. Sicari et al states that they should have the ability to guarantee that their personal information related to their movements, habits and interactions with other people are secure (4, 2018). The Internet of Things should be used to its full capacity and explore its full capability; however, the exploration and usage should not be on the expedition of our privacy. According to Sicari et al, privacy requirements in IoT is "currently only partially covered and there is a wide space of research issues to be investigated" (19, 2018). The authors have emphasized on one of the issues which is related to the necessity to have a more defined privacy policies and correspondent development due to IoT´s level of scalability and dynamic environment (19, 2018). Sicari et al suggest that capturing privacy requirements should be in the early stages of development and as part of the design process (20, 2018). Such suggestions will be explored later in the chapter.

Rolf Weber states that due to the high amount of collected data, there is a great potential of privacy risks when using IoT-devices (2, 2015). There is a growing concern with collected information which makes it possible to identify users and their behavioral patterns (Weber, 2, 2015). Information which was previously considered personal information about users, and which was not collected or analyzed with earlier technologies, are now being continuously collected and stored as a commercial or political resource. The distinction between data, personal and non-personal will be elaborated in more depth in chapter 7. The attempts to filter collected data are based on a selection of filters chosen by the providers, hence making it difficult to assess if it contributes to an increase or a reduction in safety risks through the process. Additionally, the process of filtering the collected data is performed by the providers and chosen by them which reduces the opportunities users must decide which information are included and which are not. The elaboration of these elements shows that there is a need to evaluate several data protection laws and privacy laws related to specific types of data. Weber

states that due to the large scale of IoT-applications, the new technological opportunities have organizational, social and cultural implications (2, 2015).

The methods that are used to collect and aggregate information in the Internet of Things are different and more advanced than previous technologies. Sicari et al states that due to the characteristics of the Internet of Things, traditional countermeasures are not adequate to ensure the protection of the privacy of the users (1, 2015). The countermeasures that were previously effective and secure enough to maintain a certain protection of the users´ privacy are not sufficient enough to ensure the same protection in the IoT. Some of the security and privacy challenges associated with IoT include difficulty in establishing safe and secure communication. According to Alhalafi et al, this is because the technology comprises different components at the network edge making it challenging to ensure that all the components communicate safely and securely (3, 2019). New security measures for privacy and data integrity must be created due to the large amount of collected information which are considered private information (Weber, 2, 2015). IoT-devices usually retrieve certain data which are often aggregated with data collected from other devices, and then sent through a router to a communication device (Wi-Fi or cellular) that transfers the data to a cloud server for processing (Weber, 2, 2015).

Perera et al advocates an enforcement of privacy at system design level based on the claim that the two major privacy risks are secondary usage and unauthorized access (3, 2016). Within the risk secondary usage, the authors have defined it as collected data that are not used for the consented purposes by the data owners, and can therefore, lead to privacy violations (Perera et al, 3, 2016). Unauthorized access is defined as “when someone gains access to data without proper authorization during any phase of the data life cycle” (Perera et al, 3, 2016). The two major privacy risks that have been highlighted by Perera et al, show that the major risks connected to privacy and IoT-users are with reduction in control over private information. The knowledge about usage and accessibility is not clear as the users´ control over personal information is dependent on the transparency of the IoT-producers as it is reliant on how well users are informed by them (GDPR Today, 2019). The elements that are highlighted as to which different methods producers of IoT-devices obtain consent from consumers are sometimes hidden. The example emphasized by GDPR Today, is a device

called “Sammy Screamer” which is produced by the company BleepBleeps (2019). With this particular device, the only times the users are informed or shown any type of information regarding the company's privacy policy is either a link on the company's website or in the sign-up phase where it is necessary to connect the users´ phones to the IoT-device. Despite the fact that it is not possible to use the IoT-device without installing the application. By signing up and connecting the phone to the device, the users are silently agreeing to the company's privacy policy. According to the article, such methods of “forcing” the users to connect their smartphones and signing up to the application, creates problematic situations in context of the GDPR (2019). It is stated that “this type of implied consent is ruled out by GDPR” (GDPR Today, 2019). Additionally, similar to many other consent forms which users scroll through and accept without reading the fine print, the text link that guides the users to the privacy policy of the company that produces “Sammy Screamer” is quite small which leads to issues such as difficult to read, and therefore leads to a quick accept of the privacy policy (GDPR Today, 2019). The article suggests that through IoT-users´ interaction with IoT-devices, the IoT-producers should create consent forms that are “freely given, specific, informed and unambiguous” rather than “forcing” or deliberately designing the complicated consent forms (2019). As it is possible to see through this example provided by the article by GDPR Today, there are clear privacy risks with the use of IoT-devices. Therefore, new methods of ensuring the protection of users of IoT are necessary.

As a disclaimer, the problematic situations concerning consent forms are not unusual in the context of digital technologies. The Internet of Things may not have created new issues by encouraging users to connect their smartphones to smart object, but it has neither contributed to simplify the understanding of the consent forms. The language of the consent forms is most frequently difficult to understand without prior knowledge about privacy rights and security measurements. It has been stated in the past that the issue with consent forms is that users do not properly read nor understand the depth of what they are consenting to. In relation to IoT-devices, the issue with consent forms is more relevant than before. Therefore, it still exists a necessity to simplify the language in the consent forms in such a way that it is easily understandable and contributes to increased awareness of what users are consenting to. Without an understanding and awareness of the privacy concerns users are faced with in their interactions with IoT-devices, a rewritten consent form can only do so much.

It is accentuated by Perera et al that IoT-systems are designed to support different kinds of scenarios, and in many cases, privacy concerns have not been considered by IoT-applications and platforms (1, 2016). The authors support this statement by referring to the partial lack of "systematic methods" for designing privacy which may contribute to guide the software development process in the Internet of Things (1, 2016). Perera et al highlights that in the process of making the IoT-applications development easier; a variety of IoT middleware platforms have been proposed and developed. The platforms offer distributed system services that have standard programming interfaces and protocols which may help to solve the problems associated with "heterogeneity, distribution and scale in the IoT-applications development" (Perera et al, 1, 2016). These services are called "middleware" as they are placed in the middle; a layer above the operating system and networking system and below domain-specific applications (Perera et al, 1, 2016).

Weber states that the first supranational organization that has an aim of dealing with business and legal environment of IoT, is the European Commission, which has mobilized a large group of experts with the goal to examine relevant aspects of a possible IoT normative framework (2, 2015). As of writing, the work has ended. In this context, Weber refers to the results of a public consultation based on a broad questionnaire identifying challenges with IoT (2, 2015). The questionnaire was aimed at identifying IoT challenges, and through this questionnaire, six hundred responses were collected (Weber, 2, 2015). The results of the questionnaire regarding privacy and data protection show that there are different opinions among the public. On one hand, most interested citizens and consumer organizations suggest that a greater focus on privacy and data protection in the IoT is a necessity (Weber, 2, 2015). On the other hand, the results from the industry show that the current data protection framework would be enough (Weber, 2, 2015). Even though the work of the European Commission has ended, several countries such as Japan, China and USA are continuously attempting to analyze the challenges with IoT and find possible solutions. As a conclusion of the results, Weber suggests that the results show that the producers aim to expand their business operations while consumers still wish to both maintain their fundamental privacy rights and to find a solution to the question of collection and usage of personal information (2, 2015). The public consultation shows that it is necessary with an emphasis on user consent alongside the users´ right to delete data (Weber, 3, 2015). Furthermore, a study conducted on

eleven homeowners of smart homes will be discussed in more depth in chapter 8 as some of the results support results from the questionnaire conducted by the first supranational organization.

Previously, the general public has assumed that IoT raw data are not classified as personal, and therefore cannot be exploited to identify an individual. With the use of combining collected data and analytical methods, the IoT-users´ identity may be confirmed (Weber, 2, 2015). Data collection through IoT-devices is done automatically and systematically. Therefore, due to the design and configuration of IoT data architectures, it may occur that such architectures are not de facto complying the EU regulations, e.g. DPD and GDPR. The use of hidden consent forms is causing users of IoT-devices to lose knowledge over which personal information they have lost control over. New rules are therefore necessary to establish for the Internet of Things. Additionally, Weber emphasizes that "the regulation of a global technology requires a worldwide approach in order to be most effective" (2, 2015). Furthermore, it is stated that due to the difficulties in reaching an agreement on "basic data protection and privacy issues", the solution is unlikely to be achieved soon (2, 2015). With the different legal authorities and their options around the globe, it becomes difficult to settle on a globalized regulation that fits every country around the world. With different legal measurements and different IoT-producers around the world, one country can only do as much. If there was a common agreement among the countries in the world that secure privacy of users of digital technologies, it may contribute to ensure more qualified protection for users and their personal information. The disagreement on the importance of privacy rights makes it more difficult to arrive at a joint agreement regarding legal regulations concerning privacy issues in IoT.

However, as it has been stated previously in this thesis and by Weber, the different levels of data protection in the different countries contributes to the challenge of finding a common agreement worldwide (3, 2015). Despite these challenges, it is important to continue the research and discussions around the privacy issue in IoT to be able to possibly find a solution to the issue. Although there is not an exact solution that fits every aspect of the privacy concern that exists in IoT today, the technology continues to develop and so should the research and discussions about the issues that exist in IoT.

The collection of information performed by the IoT-devices creates a great potential of privacy in terms of the usage of the data and its access. The challenges with the access of the collected information is based on that there are several actors involved in both the collection, storage and analysis of data, therefore, it is difficult for the users to have knowledge of who has access to their data. As a disclaimer, it is necessary to mention that despite the literature provided by Weber was written in 2015, some of the issues that the society was faced with at that time, are still issues that exist today. Consent forms are still difficult to understand and read, therefore, are often agreed to without a clear understanding of what users are accepting and of what rights they are giving up. Additionally, legal regulations are still not adequate or defined with sufficient precision to fully protect users of IoT due to the many different definitions of data, personal and non-personal information. The distinction of these will as stated previously, be elaborated in more depth further on. Despite the issues concerning IoT, and the inadequate regulations, there have been research and studies to find possible solutions to the issues users and producers are faced with in their production and interaction with IoT-devices. The next section will highlight some of the efforts deployed to find solutions that may better secure the privacy and personal information of IoT users.

5.4. Bringing solution to the dilemma

There is an extensive amount of literature about the challenges of privacy, and about the possible solutions that may contribute to reducing the privacy concern. In the context of this thesis, two possible solutions have been selected as they could potentially contribute to solve some of the issues concerning privacy in the Internet of Things.

5.4.1. Four Key Elements in Rule-making Process

Regarding developing new rules and regulations for protecting and securing the privacy of users in the IoT, Weber suggests that certain key elements should be involved in the rule-making process. Firstly, it is suggested that the technology that is used, should be "global" (Weber, 3, 2015). Specifically, a global RFID technology is emphasized by Weber (3, 2015). By applying the same technical processes such as RFID technology globally, it can contribute to ensure interoperability and security. Currently, only passive ultra-high frequency (UHF) RFID is regulated by a single global standard. The global standard should additionally

deal with the regulatory efforts as well. With many international internal and external entities, it creates difficulties in correctly implementing legal regulations as there are different views on privacy rights and issues around the globe. With a common agreement around the world, a global standard would be followed by most of the countries in the world, and thus creating a safer environment regardless of the policies practiced by legal authorities and IoT-producers. The security guideline for one technical process may not be suited for all of them collectively due to a lack of interoperability and difficulties in securing each device.

Furthermore, Weber refers to ubiquity which he defines as the extension (scope) of the technological environment. The rules that should be applied to IoT including data protection, privacy laws and technology standards must be designed to ubiquitously encompass persons, things, plants, and animals (Weber, 3, 2015). According to Weber, this element is important as IoT can adjust to many forms and impact many spheres of human life. As it has been stated, the technology and advancement in the IoT have surpassed the virtual world and into the physical world, creating new challenges that require new solutions.

As a third key element, Weber directs attention to verticality (3, 2015). The meaning of the word verticality is described as "the potential durability of the technical environment"; an important aspect that the duration of the lifetime of IoT-devices is that technical measures have a long enough life extension to not enable its use in the supply chain until it has reached its final customer (Weber, 3, 2015).

And the final key element suggested by Weber is technicity. The focus on technicity lays on the fact that it is an important basis for the development of rules protecting privacy objectives as several differentiations must be taken into account; "the complexity of the techniques (active and passive, rewritable, processing and sensors provided products), the complexity of background devices (reader or other linked media), and the maximum reading range which is designed to cover transparency demands" (Weber, 3, 2015).

5.4.2. Privacy by Design

The privacy solution that is provided by Perera et al is a privacy by design (PbD) framework. It can be used to assess both IoT-applications and middleware platforms without any changes

and agnostic to their differences (1, 2016). The background for Perera et al´s research has ground in the lack of privacy protection features in both IoT-applications and middleware platforms (1, 2016). There are some existing privacy-by-design, among them, is a framework proposed by Cavukian which have identified seven foundational principles that are guidelines while developing privacy sensitive applications (Perera et al, 1, 2016). The seven foundational principles are as following, (1) proactive not reactive; preventative not remedial, (2) privacy as the default setting, (3) privacy embedded into design, (4) full functionality positive-sum, not zero-sum, (5) end-to-end security; full life-cycle protection, (6) visibility and transparency- keep it open, and lastly (7) respect for user privacy, keep it user-centric (Perera et al, 2, 2016). Additionally, Jaap-Henk Hoepman have proposed an approach based on previous work performed by Spiekerman and Cranor that identifies eight specific privacy design strategies which are based on minimize, hide, separate, aggregate, inform, control, enforce and demonstrate (Perera et al, 2, 2016). Lastly, LINDDUN have proposed a third privacy-by-design framework which is developed as a method of analyzing privacy threats with the use of data flow diagrams (DFD) which consist of six specific methodological steps (Perera et al, 2, 2016). The methodological steps in the framework proposed by LINDDUN, are as follows, define the DFD, map privacy threats to DFD elements, identify threat scenarios, priorities threats, elicit mitigation strategies, and select corresponding privacy enhancing technologies (Perera et al, 2, 2016). However, despite the existence of privacy-by-design framework, Perera et al states that they are not able to provide specific guidance that are useful for software engineers in the process of designing IoT-applications and middleware platforms (1, 2016). These principles are proposed for computer systems in general, however, they do not contain enough information to be adopted by software engineers in their process of designing and developing IoT-applications (2, 2016). Based on that, the authors focused on a privacy-by-design framework that could systematically help to guide software engineers “to assess (and potentially design new) IoT-applications and middleware platforms” (2, 2016). Additionally, the authors assume that such systematic guidelines may generate consistent results irrelevant of who is carrying out a given assessment (2, 2016).

The guidelines Perera et al have chosen for their privacy-by-design framework is based on Hoepman´s approach (1, 2016). By using the Hoepman´s approach, it contributes to a better

organization and structure of Perera et al´s privacy-by-design framework. It is noted by the authors that the primary use of the framework is designed to serve a specific purpose or category of application (3, 2016). As it was mentioned before, Perera et al have identified two major privacy risks as secondary usage and unauthorized process. These two risks are primary focuses for the privacy-by-design framework as they may arise as consequences of not following the guidelines of the framework (Perera et al, 3, 2016). The guidelines of the framework emphasize the minimization of data acquisition, number of data sources, raw data intake, knowledge discovery, data storage, and data retention period (Perera et al, 3, 2016). Additionally, it focuses on hidden data routing, data anonymization, encrypted data communication, encrypted data processing, encrypted data storage, reduction of data granularity, query answering, repeated query blocking, distribution of data processing and data storage, knowledge discovery based aggregation, geography based aggregation, chain aggregation, time-period based aggregation, category based aggregation, information disclosure, control, logging, auditing, open source, data flow, certification, standardization, and compliance (Perera et al, 6, 2016). As it is possible to judge from the list above, the guidelines for the privacy-by-design framework have a wide focus on many different aspects of the data collection, distribution and access control. With the elements that are highlighted by Perera et al, it shows a set of guidelines that should guide software engineers in their design process of IoT-applications and platforms. Although there are many elements that should be considered to protect privacy by incorporating the guidelines in the design-process, the mentioned guidelines are necessary to ensure the protection of the privacy of the IoT-users.

The discussion about the possible solutions for preserving the privacy of the IoT-users is solely meant as a style for a continuous process of evaluating and researching such privacy solutions. Throughout the suggested solutions, one method may be to incorporate several of the solutions that have been discussed. Such as incorporating a privacy-by-design framework with accurate and defined regulations. However, it is necessary for the regulations to function in a globalized and standardized way, in the meaning that the regulations are qualified enough to fit globally. The usage of such methods could potentially contribute to solving some of the privacy issues in many different sectors of securing privacy in IoT-devices. As stated in 4.5, privacy issues have not recently appeared but in the context of the Internet of Things, they are

more challenging as they have a more intrusive presence in the human sphere as for data about users´ physical bodies, patterns and surroundings. The quantified self show that the interest and motivation behind the usage of smart objects will most likely not decrease as they are a tool for self-monitoring and optimization, thus increasing the importance of the continuous research into possible solutions to increase the protection of users in their interactions with technical systems such as the technology of the Internet of Things. Through an integrated environment, the privacy mechanisms within various devices may be efficient, hence the possibilities of increasing the protection of users´ privacy.

Although the suggested solutions that have been discussed, have the potential of increasing the protection of users, it is necessary to incorporate solutions for the security issues that exist in IoT as the privacy of the users are dependent on changes that affect the security features in IoT-devices. Secured and safe IoT-devices contribute to maintaining the privacy of the IoT-users as protection of personal data and the vulnerabilities which exist in IoT-devices, will suffer if there are weak security features in the devices. The concerns and issues with security measurements in the Internet of Things and some of the possible solutions for these challenges will be elaborated. It is therefore important to remember that the solutions that will be discussed in the next chapter may affect the privacy of the IoT-users as well. Security issues will be discussed in further detail in the following chapter which will elaborate on issues that are linked to privacy challenges in IoT.

6. Fundamental technological challenges in the wake of IoT

With a rapid speed, the Internet of Things is developing, designing and creating new devices. Alongside the creation and design of existing and new devices, are an increasing amount of security threats and vulnerabilities. Rizvi et al who propose a “security taxonomy” states that security is one of the most “paramount technological research problems that exist today” (2, 2018). Meaning that the security in technological aspects contain the power as it controls how secure and how vulnerable the different technologies are. When looking at the term “security”, it initially means that one should be free from danger or threats. Dan Craigen et al states in the book “Defining Cybersecurity” that the definitions of cybersecurity are quite variable, “often subjective, and at times, uninformative” (1, 2014). A new definition was

suggested by Craigen et al that states “Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights” (1, 2014). By further clarifying the definition of the term cybersecurity, it may contribute to a more enhanced and enriched focus, and thereby influence the different approaches to cybersecurity challenges (Craigen et al, 1, 2014). To grasp the concept of security and its challenges in the Internet of Things technology, a well-defined definition of the term is necessary. With a variation and uninformative definitions of the term, makes it more difficult to research possible solutions to the security challenges users and producers are faced with in their interaction and production of the IoT-devices. Through the deconstruction of the suggested cybersecurity definition proposed by Craigen et al, the authors have broken down the meaning behind the well-defined words that aim at better defining the term. In terms of “the organization”, Craigne et al have defined it as the “multiple, interwoven dimensions” and involves the interactions between humans and systems (5, 2014). The statement “protect cyberspace and cyberspace-enabled systems”, Craigen et al are refering to protection in the broadest sense; threats (intentional, accidental and natural hazards) (5, 2014). Both traditional and non-traditional systems. The meaning behind the phrase “from occurrences” refers to the intention that protection should cover the full range of the different events such as intentional, accidental and natural hazards (Craigen et al, 5, 2014). And as for the last phrase of the definition “...that misalign de jure from de facto property rights” incorporates the two independent notions of ownership and control (Craigen et al, 5, 2014). With the breakdown of the definition suggested by Craigen et al, it shows that the different phrases have been able to capture many elements with well-defined wording which clarifies the term of cybersecurity.

With the focus on security and the Internet of Things, a blogpost on the website “Fortinet” states that IoT Security “is the act of securing Internet of Things devices and the networks they´re connected to” (2020). Additionally, the website states that initially, the IoT-devices were not designed or built with security in mind, and that in most devices, there are limited abilities to implement protective measures on the devices itself (2020). Within the act of securing IoT-devices and connected networks, the protection and security of the data and information that is collected and transmitted through IoT-devices should be a key factor within IoT security. It is important to have more clarification of what is defined within IoT

security as there are many layers within the interaction between devices and users. Is IoT security exclusive for the device or the users that interact with the device?

Through the definition provided by Craigen et al and the statement from “Fortinet” about cybersecurity, they both have in common that the systems, devices and humans that interact alone and with each other should be protected in all events, both intentional and unintentional ones.

The Internet of Things in context of privacy and security have been classified as “a class of devices and associated processes that will lead to sharing and exposing more information and keeping fewer secrets” (Weinberg, 2, 2015). Recent studies have shown that the word “security” is not associated with this category of devices (Shen et al, 1, 2019). The consequence of this above described situation is that the users of IoT might potentially be exposed to massive attacks, both physical and virtual. The ability IoT-devices have of collecting and transmitting high volumes of data from device to device, device to enterprise systems, and in certain situations, device to humans; contributes to creating great risks connected to the Internet of Things (Shen et al, 1, 2019).

6.1. Usability and security

In the discussion about security in the Internet of Things, it is important to elaborate the two concepts of usability and security as they are considered two contrasting system goals. Nurse et al states that usability and security are viewed as two competing system goals (1, 2011). Throughout literature about the two concepts of usability and cybersecurity, security systems have been criticized for its insufficient usability due to its inconvenience for the users. This is possible to see in the context of the emphasis on strong and unique passwords which is suggested should be regularly changed. As for usability, the security requirements for password control may often be a strain on users and the system's usability (Nurse et al, 1, 2011). Within the usability field, there are six categories of studies; authentication, encryption, Public Key Infrastructure (PKI), device pairing, security tools and security systems (Nurse et al, 2, 2011). The result from studies conducted on all six areas show problems that have affected the usability of cybersecurity interfaces and functionality (Nurse

et al, 2, 2011). Despite system usability remaining a problem for users in such that they become frustrated and confused due to its insufficiency, poor usability in the context of cybersecurity are often a result of "inadequate configurations of security tools and functionality" (Nurse et al, 2, 2011). According to Nurse et al, such can be seen in insufficient access controls, firewalls, encryption mechanisms, and routers (2, 2011). An insufficient usability may cause the users to be displeased with the device, causing the users to not successfully adapt the device into their everyday lives. The adaption of devices into everyday lives is specially an important element within the Internet of Things as IoT-devices in many cases replay the ordinary tool or action prior to the integration of the device. With two systems competing against each other, it creates challenges in terms of both securing and encouraging users to use the device. Security requirements are necessary for IoT-devices in such that users are secure in their interactions and that devices are protected from the different threats that exist against IoT-devices. Such threats will be discussed further in this chapter.

There are many aspects of how security is used and combined with the technology of IoT. Security may be built within the device and contribute to securing data transmission and data storage both within the system and its application (Rizvi et al, 2, 2018). The authors also state that security and trust are key requirements to have the ability to handle different kinds of attacks, threats, malfunctions and devastating impacts to society (Rizvi et al, 2, 2018). The responsibility of securing IoT-devices lies with the device manufacturing companies and the companies that use the devices for personal use, production, distribution and commercial. Alongside the development of IoT, there are increased risks such as identity and data theft, device manipulation, data falsification, server/network manipulation and subsequent impact to application platforms (Shen et al, 2, 2018).

Regarding data security and privacy, there are several reasons why the Internet of Things systems are at a high risk; they lack well-defined perimeters, highly dynamic and are continuously changing because of its mobility (Bertino,1, 2016). Additionally, they are highly heterogeneous due to their communication medium and protocols, platforms and devices, and the fact that many of the IoT-devices that are connected to the Internet may not be designed to do so (Bertino, 1, 2016). An number of IoT-devices are physically unprotected and are

controlled by different parties. Unlike other technologies, due to its information systems and mobile environments, IoT is more difficult to protect, and by extension, the users.

6.2. Vulnerabilities in each layer

The technical components of the Internet of Things which have previously been discussed, show that due to the core technologies that support the Internet of Things networks, it is challenging to ensure that they communicate safely and securely. Additionally, the abilities that are created by the dynamic environment of IoT, are contributing to complicating the tasks of identifying, assessing and monitoring these components to secure the IoT-users, and "ensure compliance with security politics" (Alhalafi et al, 3, 2019). Shen et al emphasize that most IoT-devices are closed in terms of its software and hardware design, due to the proprietary design (1, 2019). Since most IoT-devices have limited processing capabilities and storage capacities, it contributes to a lower level of security in these devices. The factors mentioned above may affect how the security measurements are weighted in terms of design process, as efficient protective measures may induce more technical overhead and added development costs.

The history of the Internet of Things has been discussed in Chapter 3 and the important elements that contributed to the development of IoT have been highlighted, in addition to the technological developments that have made it possible to evolve the technology of IoT. However, to gain a better understanding of the security issues and challenges with IoT, an understanding of the specific technical components that contribute to the vulnerabilities in the technology, is necessary. In the process of elaborating those technical components, an IoT taxonomy compiled by Syed Rizvi et al in "Securing the Internet of Things (IoT): A Security Taxonomy for IoT" is used as a foundation (2018).

Rizvi et al states that the aim of the proposed taxonomy has been to create a method that, with the use of the security controls of the top-level security divisions, may contribute to create an IoT security dashboard for the different types of IoT-devices (7, 2018). Hence providing a method allowing one to identify the security architecture of IoT that may contribute to protect the individuals, companies and entities which utilize them (Rizvi et al, 3, 2018). Considering

the interactions between layers such as perception, application and network, it is plausible to say that IoT comprises a type of open network (Rizvi et al, 3, 2018). Within IoT, there are several properties such as mobility, wireless, embedded use, diversity, and scale that continuously challenges the security issue in IoT.

The table below is reproduced from Rizvi et al. (2018, 3) The content in the table is elaborated and discussed with explanations of the taxonomy. The table shows the top-level security domains with their sub-domains. Rizvi et al have chosen to divide the IoT taxonomy into four top-level security domains where each domain comprises three sub-domains. The four top-level security domains are Architecture, Threat Vector, Trust and Compliance (Rizvi et al, 3, 2018).

Top-Level Security Domain	**Sub-Domains**
Architecture	Perception Layer
	Application Layer
	Network Layer
Threat Vector	Communication Attacks
	Physical Attacks
	Application/Software Attacks
Trust	Privacy
	Availability
	Reliability
Compliance	Policy Control
	Government oversight
	Non-Government Oversight

Illustration 1.2. Source: "Securing the Internet of Things (IoT): A Security Taxonomy for IoT" (Rizvi et al, 3, 2018).

The next step is to discuss the top-level security domains and sub-domains in some detail to have a better understanding of some of the issues that lie within the technology of IoT. The details in each top-level security domains and sub-domains that will be elaborated are provided by Syed Rizvi et al.

6.2.1. Architecture

Within architecture there are three sub-domains; the perception layer, the application layer and the network layer. The intention behind this division into sub-domains is motivated by the unique architecture of IoT-devices which may be defined using a layering approach (Rizvi et al, 3, 2018). IoT-devices are like the TCP/IP protocol as they both are considered to have "three different operational layers" (Rizvi et al, 3, 2018). Within each layer, unique threats may be identified, and possibly addressed and countered. Since the layers are connected and reliant on each other, every layer has to be secure to have the security intact. Meaning that if two of the layers are secure but the third is insufficient, all three becomes vulnerable.

The perception layer is responsible for the collection of data, and each of the IoT-nodes perform a function that requires the collection of data. The perception layer operates with the use of RFID and other various sensors, and the use of such sensors are one of the reasons why it is important to secure this layer from damaged or malicious data (Rizvi et al, 3, 2018).

The application layer is the most diverse and complicated of these three as there are no universal standards for the construction of this layer (Rizvi et al, 3, 2018). This is because of the many different products, devices and manufacturers involved. Some of the concerns associated with this layer are data access permissions and identity authentication (Rizvi et al, 3, 2018). As explained, with many different types of applications and users, it becomes more difficult to manage such access. Other challenges are the data protection and recovery, and the massive amounts of data and information transactions.

The network layer is involved with the transmission of data and this layer does also operate the same network layer as TCP/IP, and therefore, faces traditional security problems that previously have been encountered with the TCP/IP model (Rizvi et al, 4, 2018). The common security problems with IoT and TCP/IP models are, e.g. illegal access networks,

eavesdropping information, confidentiality damage, integrity damage, DoS attack, man-in-the-middle attack, virus invasion, exploit attacks, and etc. (Rizvi et al, 4, 2018).

The exploration of the three layers within the architecture of IoT is composed and shows the necessity to clarify proper security requirements as one uncertainty makes all three vulnerable. With an understanding of the unique architecture of the Internet of Things, the next phrase is to elaborate on the different types of threats that the IoT-devices may be vulnerable to.

6.2.2. Threat Vector

A threat vector is classified as a method or medium for an attacker to penetrate IoT-devices and execute malicious functions to harm a device or system (Rizvi et al, 4, 2018). Within the IoT-environment, the examples of such threat vectors include identity management, embedded security, storage management, physical threat, dynamic binding and communication attacks (Rizvi et al, 4, 2018). The sub-domains within the threat vector category are based on communication attacks, physical attacks and application attacks (Rizvi et al, 4, 2018). Based on the names of these sub-domains, they give a clear image of what types of attacks and the damage these attacks may cause.

It may come across that the technology of IoT may be the only digital technology that is faced with threats, however, a unique factor is that within IoT, threats may cause more physical harm than previous technologies. Despite a focus on the technical components of how IoT may be vulnerable if security requirements are not met, the security in IoT-devices are also affected by the users´ interaction with devices, and how they handle vulnerabilities. It is therefore important that the users trust the IoT-devices they interact with. Trust is established through different methods.

6.2.3. Trust in IoT

Rizvi et al states that there is a lack of knowledge amongst the individuals in society about the level of security on their connected devices (5, 2018). Earlier events have shown that in the past, the sacrifice of security for a financial added value has become a problem in the IoT-environment (Rizvi et al, 5, 2018). A trust management model has been established to

determine the different elements that are required to establish trust with and between IoT-devices. There are four levels to the model; IoT user, application, network and the physical layers (Rizvi et al, 5, 2018). However, in this IoT taxonomy, trust is divided into three sub-domains; privacy, availability and reliability.

IoT-devices collect information that is necessary for performance of the business application and used to better suit the individual's needs. As stated previously, the collected information is based on physical, medical, communications, and Internet browsing history. In terms of the availability sub-domains, users of IoT-devices should be able to require that the devices are available and powered to complete their tasks (Rizvi et al, 5, 2018). IoT-devices do require many updates, and based on that, there have been some proposed recommendations that there should be a standard available updating platform which would require to be available for all the devices in a certain domain (Rizvi et al, 5, 2018). The users should be certain that information is transmitted and received correctly. The most important aspect is a reliable scheme to communicate with devices with embedded security involving integrity, confidentiality, and availability (Rizvi et al, 5, 2018). It is therefore necessary with efficient and reliable communication for day-to-day operations in the IoT-environment.

6.2.4. Compliance

Compliance is necessary for security and security operations, and without proper compliance, policy and procedure controls, it becomes more difficult for companies to organize their security operations to accomplish a better security lifetime (Rizvi et al, 5, 2018). In terms of the organizational management, it has been defined into three classes within compliance; policy control, government oversight and non-government oversight (Rizvi et al, 5, 2018).

As a conclusion to the walk-through of the taxonomy suggested by Rizvi et al, there are several components that must cooperate to ensure the protection of IoT and its users. One insufficient component may make the other components vulnerable. Hence the importance of ensuring that all the procedures are followed, and the correct security requirements are achieved. Until now, the technical components that may create vulnerabilities for the devices and users have been elaborated. Furthermore, specific challenges of the security in the IoT will be discussed and highlighted, and some potential solutions to these concerns.

6.3. The challenges of securing devices and users in IoT

The available IoT-devices have scarce resources, they cannot use complete security suites which are typically used in networks. This presents a challenge as one must design a unique security framework for IoT or develop existing solutions. Efforts must, however, be made to ensure that lightweight security solutions are used to secure IoT so that devices resources are not depleted on security at the expense of performance (Alhalafi et a, 2, 2019). In the coming pages of this chapter, the discussion of common risks associated with the security concerns in IoT will be based on several authors and their opinions about why IoT-devices are vulnerable due to the lack of security measures in the design and production.

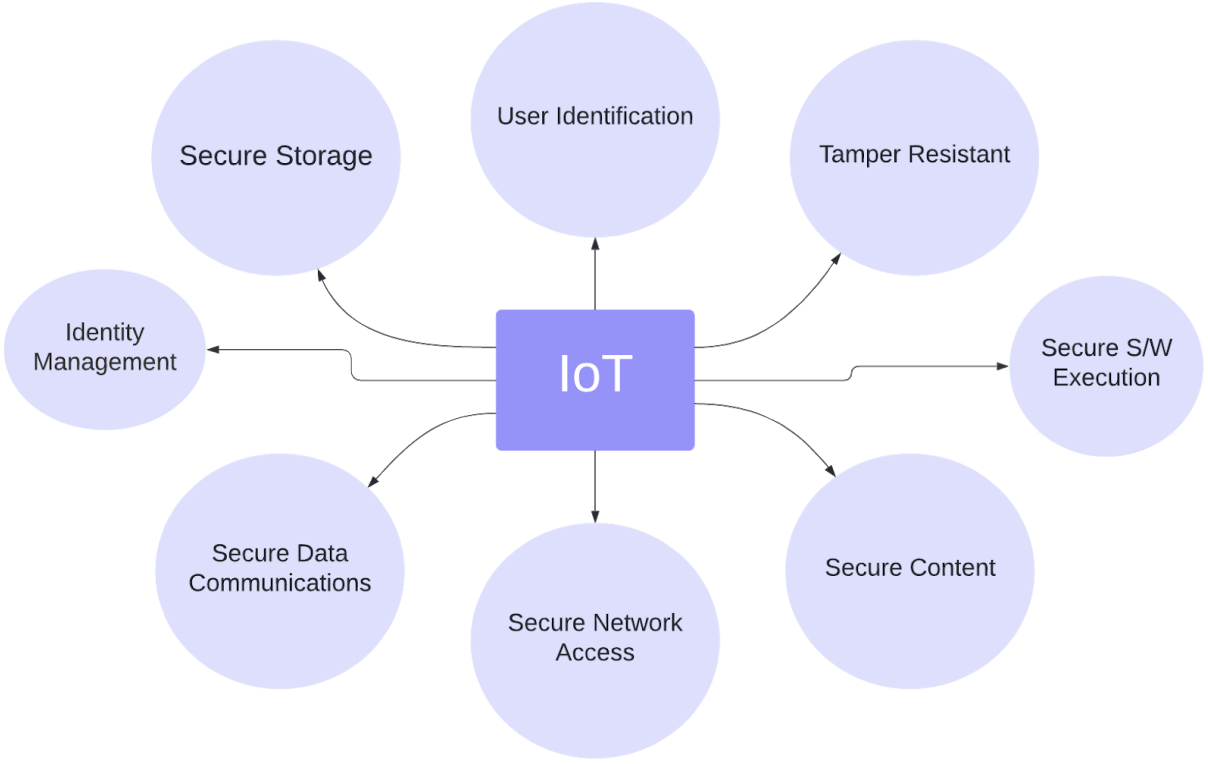

Illustration 1.3. Security Concerns in IoT.

Source: "Proposed Embedded Security Framework for Internet of Things (IoT)" (Babar et al, 2011)

The illustration above illustrates an embedded security framework for Internet of Things exploiting knowledge about major security concerns when it comes to IoT (Babar et al, 2, 2019). As it is possible to see, many of the highlighted security issues are concerned with the ability to secure the different elements and containing an anonymized profile of the IoT-users.

Shen et al argue that the common mistakes within IoT-devices in terms of making them vulnerable are the use of unencrypted network communications, hardcoded username/password, lack of strong authentication mechanism, and etc. (1, 2019). It is inevitable that there will be an increase of attacks on IoT-devices due to the lack of security components and the accelerated growth of Internet-connected smart devices and applications without security by design (Shen et al, 1, 2019).

According to Alhalafi et al, the three common issues with security in IoT are confidentiality, authentication, and access (3, 2019). It is necessary with confidentiality to ensure that personal data are private, and that only authorized users can access it. And cryptography has emerged as the most important technology for IoT to ensure confidentiality. When it comes to authentication, it is the method of verification of data to ensure that there is no tampering with the information and that the transmitted information is delivered by the appointed sender or author. Additionally, it is important to make certain that only authorized users have access to retrieve and obtain the infrastructure, communications, and information, at the same time, it is necessary to secure the access the authorized users should have (Alhalafi et al, 3, 2019).

Recommendations have been made by researchers such as Alhalafi et al and Brumfit et al show that other views besides the traditional approach should be studied (3, 2019). The security issues according to Alhalafi et al have been divided into three parts; identification and localizing and tracking, profiling and authentication, and lifecycle transitions and inventory attacks (4, 2019).

The identification challenges with IoT involves the risk of associating a specific identifier to an individual and related data (Alhalafi et al, 4, 2019). With the possibility of potentially associating information that could identify certain aspects of an individual may violate the individual's privacy by providing the identifying information to entities outside the user's personal sphere, and therefore, increasing the possible cyber-attack vectors (Alhalafi et al, 4, 2019). In context of localizing and tracking, the issue is related to the ability to record and establish an individual's location across space and time with the use of the technical components of IoT. As a disclaimer, it is necessary to mention that other technologies such as Internet traffic and mobile GPS location can localization and track individuals already. The

ability to localize and track IoT-users may be viewed as a violation of privacy, which is based on the uncertainty of the usage of the collected data and the lack of control over the sharing of their location data (Alhalafi et al, 4, 2019). Therefore, in context of IoT, there is a challenge in ensuring the awareness of tracking and control over the localization data (Alhalafi et al, 4, 2019).

The second issue that Alhalafi et al have mentioned is profiling and authentication. The uncertainty with IoT in terms of profiling is the compilation of personal data about the users as a method of determining their interests through linkability in such a way that other sources of data and profiles are linked together (Alhalafi et al, 4, 2019). Thus, creating information power of the IoT-users. The linkability with other sources and profiles show the interaction between IoT-devices and how they communicate, and the dynamic environment that is the Internet of Things. Profiling methods are used as a method of personalization for the consumers and internal targeting (Alhalafi et al, 4, 2019). Although profiling methods are mostly used in e-commerce and as a tool for personalizing the content for the consumers, it may progress into an issue if the collected data is used for “unsolicited ads, price discrimination, and social engineering” (Alhalafi et al, 4, 2019). The gathering and sale of user profiles in the data marketplace without the individual's consent is considered as a privacy violation (Alhalafi et al, 4, 2019). Despite violation of privacy, such actions are conducted by companies and actors.

Different applications such as healthcare, transportation, and retail are reliant on significant user interactions, and a great number of the mechanisms that are used to interact with the user and present feedback information are inherently public in nature, which pose a threat to the individual's privacy if other people can observe the data (Alhalafi et al, 4, 2019).

The lifecycle transitions and inventory attacks are according to Alhalafi et al, the personal information that is collected through the users´ interaction with IoT-devices and has a possibility of being disclosed due to changes that may occur with a device’s “control spheres” during its lifecycle (4, 2019). Communication and interactions are saved on the IoT-devices´ history logs. This creates a potential danger associated with sale or sharing of these devices. In most cases, IoT-devices are produced with the intent that the user who bought the device,

owns it throughout its lifecycle but in reality, there is a high possibility that it may be sold or shared between several users. This may cause a threat to the initial user as the second or third user of the device may have the opportunity to access sensitive information about the previous owner.

In terms of inventory attacks, alongside "the development of end-to-end vision" the capabilities of interconnection in IoT-devices continues to evolve which creates opportunities for both legitimate and non-legitimate parties to query the IoT-devices over the Internet (Alhalafi et al, 4, 2019). Meaning that non-legitimate entities may exploit the IoT-devices in order to collect unauthorized information about the characteristics and patterns of users' personal habits. With non-legitimate parties accessing IoT-devices, and the IoT-devices allow them access leads to the opportunity of exposing extensive data about the IoT-users and their belongings. This may pose a threat to the IoT-users´ security and privacy (Alhalafi et al, 4, 2019).

There is a consensus amongst researchers of IoT, as reviewed by the present author, that the features and technologies of IoT together with emerging patterns of IoT interaction have contributed to amplify existing serious privacy and security challenges. The common security threats and risks associated with IoT-devices have been discussed above without addressing possible solutions to those risks and threats. The following will discuss such possible solutions which several researchers have proposed.

6.4. Possible solutions to security risks in the Internet of Things

Many researchers have suggested different proposals as methods and solutions for securing IoT-devices and their users. However, in this thesis, as it is not possible to discuss in-depth and in detail each proposed solution, the focus will be set on highlighting a common element in these proposals which is the method of incorporating security into the design process. The thesis will therefore elaborate on one of the proposed "Security by Design" approaches as a possible solution for the security threats IoT-devices face. Additionally, researchers have agreed that if appropriate measures are adopted and enforced while developing the device, it

may minimize the possibilities of an attacker taking advantage of a weak design to bypass the authentication or the security methods that are used in the IoT-device. Therefore, by allowing and considering the security regulation while designing the product may be a better method of securing the information rather than incorporating security regulations as add-ons.

It is necessary to mention that a possible solution as a tool and a foundation for a desktop method has been discussed earlier; the IoT taxonomy. However, the taxonomy discussed above is intended to serve as a diagnostic tool and a guideline of best practices for researchers, designers and hardware/software programmers in the design process as a method of exploring how each component in the IoT-technology may be identified as vulnerable. By obtaining an awareness of the vulnerabilities and how attackers may harm the technology and the users, it may contribute to advancing how the devices and technologies are created. If appropriate measures are taken throughout the process of designing IoT-devices, it may contribute to minimizing the possibilities of attackers taking advantage of weak design or the security methods that are used in IoT-devices.

“Security by design” is based on that security measurements often are described as an add-on and not as a constitutive part of the design process of the IoT-devices. Shen et al and Alhalafi et al suggest that by incorporating “security by design” might be an approach of strengthening the security in IoT-device due to that they will be secured at various system levels (3, 2019). In most articles and papers concerning the security risks and vulnerabilities in the Internet of Things, there are suggestions related to incorporating security measurements into the design and production process of the devices and objects. And because of the several suggested methods of how to incorporate security measurements into the design-cycle, it has been chosen for this thesis to elaborate one of these suggestions. The thesis will elaborate more on the suggestion proposed by Babar et al which is labelled “Embedded Security Framework for Internet of Things”.

6.4.1. Embedded Security Framework for Internet of Things

Babar et al states that research on existing solutions for the security concerns in IoT is divided into two main topics which are “optimization of the basic security functions” and “countermeasures against security attacks” (3, 2019). Babar et al claims also that solutions

within these two topics have not provided solutions against most of the security attacks but have focused on increasing the basic security functions (3, 2019). Furthermore, the authors insist that there is a continuous need for "an embedded security framework and architecture" (Babar et al, 3, 2019). To find possible solutions that may solve the majority of the security attacks, it is suggested by the authors that the focus have to shift the security considerations from "a function-centric perspective" to a "system architecture (HW-SW) design issue" (Babar et al, 3, 2019). Furthermore, Babar et al state that an embedded security measurement may contribute to better secure IoT-devices as that means to build the security features in at the start phase. In other words, security features are built and designed into the IoT-devices in the starting phase. To be able to build security features into the devices at the starting phase of the design-process, it is necessary with solid building foundations for the embedded security. Babar et al have listed five major building foundations for such (4, 2019). These are as followed; Cryptographic Algorithms, Secure Storage, Secure Boot, Secure JTAG and Secure Execution Environment (SEE) (Babar et al, 4, 2019). The foundation for creating a framework for the security architecture for IoT is "utilizing security mechanisms and protocols effectively, to start off with a design that takes security into consideration from the requirements gathering to maintenance, following the software development life cycle" (Babar et al, 4, 2019). Below is an illustration that shows the design-cycle of an embedded security architecture.

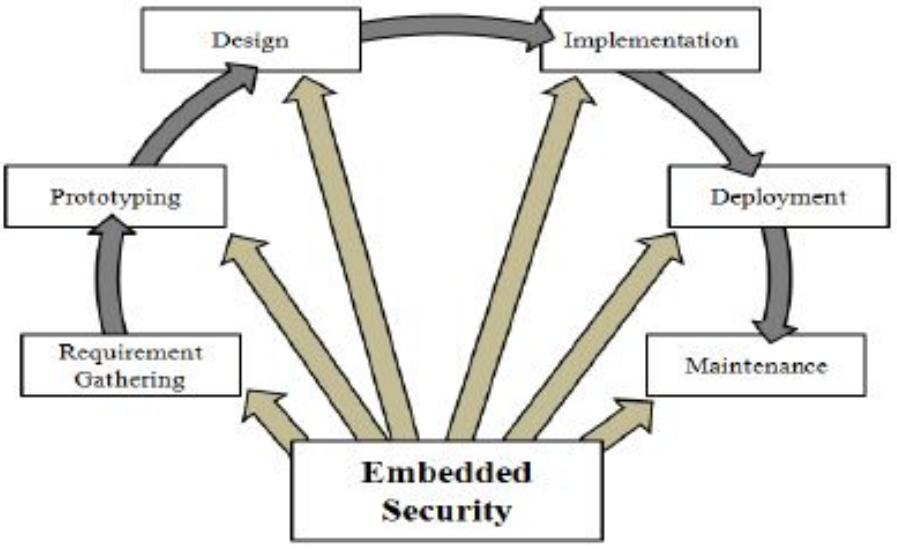

Illustration 1.4. The design steps of an embedded security architecture. Source: "Proposed Embedded Security Framework for Internet of Things (IoT)" (Babar et al, 2011)

Although Babar et al have suggested methods and steps for building a solid foundation for designing security measurements into the design from the starting phase, there are some issues related to the actual creation of such a framework. In order to design a framework for embedded security, three concepts must be considered; performance, cost, and security (Babar et al, 4, 2019). The concepts are almost directly at “odds with one another”. Babar et al states that “more performance means the cost goes up, lowering the cost means lowering security and performance, and implementing higher security means performance will decrease” (4, 2019). However, solutions to these issues have been proposed; a hardware and software-based security architecture; a mixture of hardware and software that may accomplish overall security goals as it provides enough motivation for attempting a synthesis-oriented approach to achieve security system implementations having both hardware and software components. Such an approach would benefit from a “systematic analysis of design trade-offs that is common in synthesis while also creating cost effective systems” (Babar et al, 4, 2019). Babar et al have specified the key features of the security framework and architecture, e.g., mechanisms implementing lightweight cryptography, physical security, standardized security, secure operating systems, future application areas, and secure storage (5, 2019). These key features show possible solutions to the major concerns related to security in IoT which is shown in the illustration 1.4. above.

The illustration 1.5 below shows a suggested figure to an embedded security architecture.

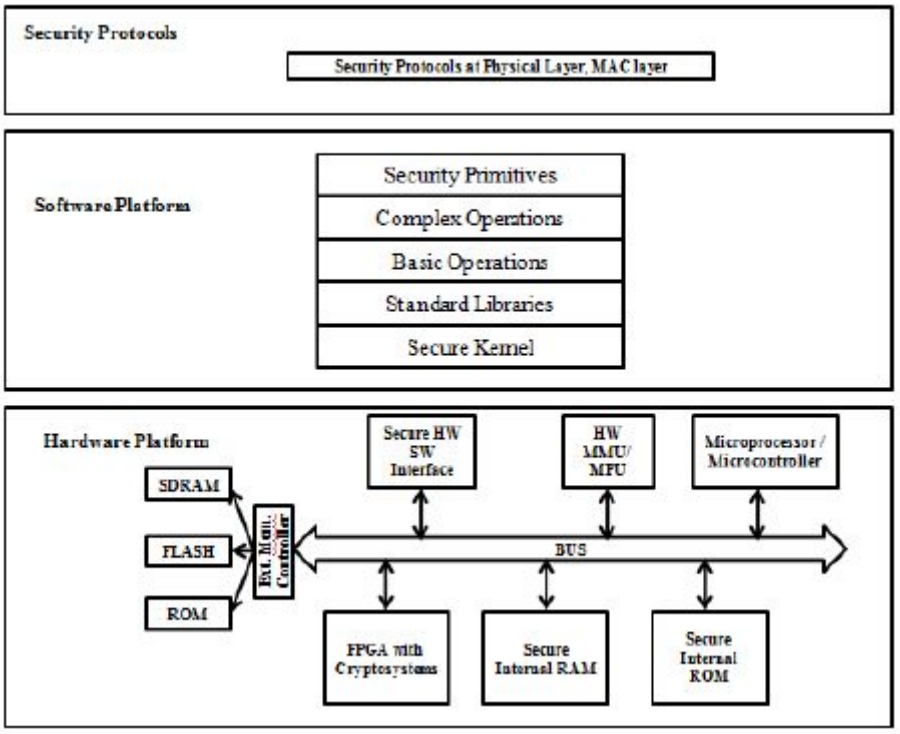

Illustration 1.5. An embedded security framework and architecture figure.
Source: "Proposed Embedded Security Framework for Internet of Things (IoT)" (Babar et al, 2019).

As it is possible to see in the suggested solutions for the security issues in IoT, there is an emphasis on the integration of security features into the design and design-process. In such a way that the security measurements are not designed at the final stages nor designed as an add-on which previously have contributed to vulnerabilities in IoT-devices as the countermeasures for security are not embedded in the devices. The website "Fortinet" has stated that the only method for securing the users and protecting the IoT-devices is with "an integrated solution that delivers visibility, segmentation, and protection throughout the entire network infrastructure" (2020). This approach can also be referred to as a holistic security fabric (2020). This method supports the statement regarding convergence that was discussed in chapter 4, that an integrated environment will contribute to an increased effectiveness, efficient security, and privacy mechanisms into various devices, architectures, platforms, and protocols (Fantana et al, 20, 2017). The increased interactions between smart objects, humans and technologies must ensure that security features together with privacy regulations must be combined throughout the process of designing and creating IoT-devices. In context of this statement and suggested approach, it shows that to reduce the security risks with IoT and IoT-devices, the entire device including both hardware and software, must be secure and

therefore have some sort of security layer throughout the device. However, some of the vulnerabilities the IoT-devices are challenged with, are consequences of its ability to interconnect and interaction with objects and humans**.** Hence the complex interaction between humans and technical systems that Hayles have outlined, and the integration of the human aspect into the nonconscious cognitive assemblages within technical systems.

The regulations of all assorted IoT-devices should be standardized as it affects the chain of interconnected devices and objects which entails that if there is one weak layer that does not have the sufficient security protection layers and protocols, the other layers become vulnerable as well. The scarce resources of the IoT-devices cause the traditional security suits to be a misfit for smart objects. With a potentially higher cost of ensuring safe IoT-devices, it may affect their performance and price. Hence, the importance of awareness of the transaction between IoT-users and IoT-producers in which the users of IoT have a transaction with the producers of IoT in terms of personal data which are exchanged for the services of IoT-devices. The cheaper the devices, the possibility of being more vulnerable than with a more expensive device.

7. Framing the ethical use of personal and physical data in IoT

In the book “Ethics in Information Technology”, Reynolds defines ethics as a set of beliefs about right and wrong behaviour within a society (25, 2014). Reynolds emphasizes the differences between morals, ethics and laws as they may be interpreted similarly. Morals is defined as one's personal beliefs about what is right and wrong while ethics describes standards or codes of behaviour which would be expected by an individual by a group (nation, organization or/and profession) (Reynolds, 26, 2014). A law is referred to as “a system of rules that tells us what we can and cannot do”, and they are enforced by a set of institutions such as the police and courts (Reynolds, 26, 2014). According to Tzafestas, the concept of ethics provides standards of obtaining good human behaviour beyond the legal minimum (1, 2018). Although some standards of good human behavior in the deciding of what is right and wrong, how to act and behave, and how to maintain social order is decided by the law, and some by ethics and morals, they should be equally respected (Tzafestas, 1, 2018). Within the concept of ethics, a new branch called data ethics have been developed. This thesis will rely

on the definition provided by Luciano et al which describes data ethics as an aspect of ethics completely devoted to researching and studying moral dilemmas connected to data, algorithms, and corresponding practices to obtain a better method of formulating and supporting morally good solutions (5, 2016). As an element of the research on data ethics, the dilemma and continuous discussion about data ownership is important to address as it is directly connected to issues regarding the ethical use of data within the Internet of Things. As part of protecting the users´ privacy, the regulation and laws regarding this topic, must be accurate to provide the correct protection but an ethical viewpoint of the dilemma may contribute positively to the concerns regarding data ownership and privacy.

The statements that have been highlighted and emphasized by several researchers and authors show that with a lack of clarity surrounding the definitions of data and information, personal and non-personal, there are several difficulties in finding a solution to the debate of data ownership. Additionally, as it aims to find solutions to the privacy issue, there must be regulations and access control when it comes to collected data and information. If there are limited regulations to control who has access to collected data or who can use the collected data, the privacy of the IoT-users is at risk. With the technology of IoT, information and data that have been viewed as non-personal may, with the use of analytical and technological advancements, be viewed as personal. The dynamic environment of IoT creates new possibilities of linkability and methods of connecting data and information about IoT-users. Data is collected through many different aspects, and many of them may be without consent from the citizens (Janeček, 4, 2019).

The ethical aspect will be discussed in context of the Internet of Things. Guidelines of ethical conduct will be presented alongside an example of the importance of clarification and sufficient legal regulations, security features and ethical conduct in IoT.

7.1. Ethics and the Internet of Things

Tzafestas states that with the technology of the Internet of things, it creates “a new social, economic, political, and ethical landscape that needs new enhanced legal and ethical measures for privacy protection, data security, ownership protection, trust improvement, and the

development of proper standards" (1, 2018). Since IoT does not solely involve objects but also the interrelations between objects and humans, the philosophical, ethical, and legal issues of IoT, must be considered (2, 2018). Janeček writes that through users´ interactions with IoT-devices, a massive amount of data is generated and collected which leads to serious ethical and legal questions regarding management (1, 2019). Furthermore, ownership of personal data has constructed the issues with data management and control in terms of privacy, trust and security (Janeček, 1, 2019). The dilemma of ownership of personal data may have important implications for the future of the "digital" economy and trade in data.

Personal data have been recognized as one of the key economic assets, and by failing to explore and clarify the debate may be problematic due to these economic trends (Janeček, 4, 2019). The use of personal data and the ownership of them are starting to imply severe implications for social discrimination and justice issues as actors and agencies other than the individual who generated the data, have access (Lupton, 17, 2016). Software coders construct algorithms that connect digital data in certain ways that produce "algorithmic identities". The usage of personal data may be undertaken beyond the user´s control and knowledge about how the data are analyzed or employed (Lupton, 17, 2016). Lupton emphasizes "algorithmic authority" which states that the decisions made by software programmers have a dominant role in displaying or sharing the individual's life based on the collected data through self-tracking (17, 2016). Although collected data may be originally anonymized, it is possible for data experts to re-identify some of the data. Lupton states that it is estimated that particularly health and medical information is one of the most valuable commodities for hackers (13, 2016).

7.1.1. The debate about data ownership in IoT

Janeček states that the limitations in ownership of personal data should precede discussions and debates on ownership of purely non-personal data (2, 2019). Since data is classified as non-personal, it may identify an individual, thus increasing the importance of clarification and exploration of the limits of ownership of the classified personal data to be better secure individuals, and increase the protection of users of IoT in their interactions with IoT-devices (Janeček, 2, 2019). The generated and collection of huge amounts of data in IoT leads to the distinction between personal and non-personal data, as the line between them is continuously

in movement and blurry. Data that may be viewed as non-personal, can be viewed as personal with the use of analytical and technological advancements (Janeček, 4, 2019).

How the data is produced and collected lays the foundation of the questions Mashhadi et al have researched (1, 2014). The authors have researched the questions “who owns this data and who should have access to it?” (1, 2014). The questions raised by the authors have contributed to the emergent of the topic of Human Data Interaction (HDI) which refers to “the broad topic of providing access and understanding of data that is about individuals and information on how their collected data affects them, by placing human at the center of the data driven applications” (Mashhadi et al, 1, 2014). HDI is classified as an interdisciplinary field which is combined of several different fields such as domains of databases, computer science, visualization, interaction design, law, psychology and behavioural economics. By combining such different fields together, the aim is to try to define “a human centred framework and design guidelines for future data driven applications” (Mashhadi et al, 1, 2014). Through different studies, new insights about data, users and IoT have been discovered. Examples of these insights refer to observations of the users´ lack of awareness about who can access their devices and/or data (Mashhadi et al, 1, 2014). According to Mashhadi et al, data collected through either IoT-devices such as fitbits, smart-thermometer or smart cities, are sold to or shared with a third-party company “that operates as state agents” (2, 2014). These smart objects in addition to devices and environments equipped with digital sensors show a variety of methods of how the act of self-tracking may obtain data that may not be clear to the users as it collects data in various ways. Although the recent digital technologies, e.g. IoT networked sensor capabilities, augmented self-tracking opportunities, e.g., allowing users (and producers, as well as third party actors) to collect, analyses, search, aggregate, visualize and compare data more rapidly. These developments do raise new issues concerning the use of people's personal information as the networked sensing capacity of IoT lives, practices, location, and even, physiological functions and physical bodies. In particular, the various ways collected information is purposed and repurposed as part of the global digital knowledge economy, data privacy and security issues, and additionally, the implications for concepts of selfhood and citizenship (Lupton, 3, 2016).

7.2. Legal definitions and regulatory framework unstrained

In the context of GDPR, personal data is legally defined as “any information relating to an identified or identifiable natural person” (Janeček, 6, 2019). By referring to personal data as information that is related to a natural person, it overlooks the distinction between data and information and therefore, the ownership of personal data as opposed to ownership of personal information (Janeček, 6, 2019). This distinction is based on that data and information is, according to Janeček, “two distinct concepts” (7, 2019). Data can be defined as “putative facts regarding some difference or lack of uniformity within some context”, and that data are the source of information, depending on the interpretation of them (Janeček, 7, 2019). Hence no data - less information. With other words, it is not necessary to understand the information that any data may convey to be able to use the data as an asset from which “valuable information may be extracted in the future” (Janeček, 7, 2019). Based on that data and information are two different concepts, a clear distinction between data and information is needed. That is why there is a continuous debate about data ownership as there is a distinct differentiation between the form in which information is embodied and the meaning contained in that form such as the information itself. According to Janeček, the difference is described as a distinction between “the syntactic level of information (the form) and the semantic level of information (the meaning)” (7, 2019). Furthermore, a confusion between the formal representation of information and the source of identical information, also called information and data, is created based on an information-centred starting point (Janeček, 7, 2019). The original questions of the debate of data ownership was initially based on how data can be protected and what type of information can be extracted from data. Since collected data in an IoT-environment can be analyzed in indefinite ways, it raises concerns that the data may reveal sensitive information about an individual (Janeček, 7, 2019). There have been statements from researchers that the same fragment of data may be understood as both personal and non-personal information (Janeček, 8, 2019). Thus, depending on the context and purpose of its use. However, it is in Janeček´s opinion that the root of the issue regarding data ownership is the definition of personal data set by the EU law (8, 2019). Data is the source of information which implies that if the data can be viewed as personal, the original data is personal data. Furthermore, Janeček claims that the definition set by the EU law

creates “a paradoxical situation in which no data are personal from the outset and all data can become personal from the outset” (7, 2019).

Besides the debate about data ownership in IoT and unclear distinctions between personal and non-personal data, there are several other serious ethical and legal concerns. These issues are in relation to protection of privacy, data security, data usability, data user experience, trust, safety, and etc. (Tzafestas, 9, 2018). According to Tzafestas, the huge amount of data that is generated and analyzed in the IoT contributes to more complex and demanding ethical and responsibility aspects than those of “pure Internet” (9, 2018). The debate about data ownership dwells on whether or not the users, the producers or external entities own the collected data, and based on that debate, discussions are now about whether or not the concept of data ownership as a legal right should be introduced (Janeček, 2, 2019). Until the issue is resolved in terms of determining whether data ownership as a legal right should be imposed, ethical guidelines should be followed.

By applying an awareness of the ethical issues in IoT, it may contribute to a better foundation of assessing the correct methods of enhancing the positive elements of IoT than the negative elements. Additionally, when designing and building IoT-devices, it is necessary to have information and decisions about questions such as who is responsible and who is accountable in case of harm (Tzafestas, 9, 2018). The ethics of IoT is important both for the private and the public life. Questions surrounding ethical dilemmas such as data ownership in the Internet of things are increasing. There is no clear answer as to who owns the generated data. Is it the users that generated the data, the producers that designed the devices, or is it the third actors that analyze and illustrate the collected data in graphs and statistics? According to Janeček, the concept of data ownership is not defined at the EU-law level, and national legal systems are defining the concept differently (1, 2019). To clarify the definition of data ownership in IoT, there are several elements within the dilemmas such as property and personal information that must be defined. Without a clarification of the definition of data ownership, the uncertainty in the ownership of the collected data through interactions with IoT-devices continues to increase.

The ethical issues that have evolved in the context of IoT may be caused by the characteristics that are distinctions for the technology. The ability of ubiquity, miniaturization, ambiguity, difficult identification, autonomous and unpredictable behavior, incorporated intelligence, incorporated intelligence, etc. (Tzafestas, 13, 2018). With these characteristics, IoT is everywhere, and users are intrigued by the many possibilities of the technology. The devices are smaller than other technologies which gives the illusion that they are more practical in everyday life. Each object or thing must have an identity to be able to connect to IoT, and due to access and management of these identities; security and control issues may arise. Additionally, with an interconnected environment such as IoT, objects interact autonomously and create emerging behaviours that IoT-users may not be aware of or fully understand. Based on these ethical issues regarding the characteristics of IoT, there are several ethical questions that must be addressed within IoT. Questions related to lack of Internet connection, liability of patching IoT-devices, routers, and cloud connections, assurances of the vulnerabilities in case of hacking, risks in context of downtime for critical life-supporting devices, ownership of data, situations where IoT-devices may act without user's consent, and digital divide (Tzafestas, 13, 2018). According to Tzafestas, with all the activities involving collection of personal data, it is expected that it complies with the applicable data-protection legislation (13, 2018). Beyond the legal compliance, it is suggested or demanded that IoT-activities should respect the ethical principles that are relevant in each case. There are therefore compiled a set of general ethical rules that are applicable to IoT-activities (Tzafestas, 14, 2018). The set of general ethical rules are as following; “In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity. Individuals should not suffer physical or mental harm from IoT-activities. Benefits from the application of IoT should be added to the common good. The necessity and proportionality of an IoT process should be considered and capable of being demonstrated. IoT-applications should be performed with maximum transparency and accountability via explicit and auditable procedures. There should be equal access to the benefits of IoT accruing to individuals (social justice). IoT-activities should have a minimum negative impact to all facets of the natural environment. IoT-activities should aim to lighten the adverse consequences that data processing may have on personal privacy and other personal and social values. And, as the last principle, adverse effects beyond the individual (groups, communities, societies) should be avoided or minimized or mitigated” (Tzafestas, 14, 2018).

7.3. Implemented Medical Devices (IMD)

A set of general ethical rules should act as a method for protecting users of IoT in situations where the legal definitions and regulations are not enough to ensure protection for users. With the ongoing debate about the distinction between personal and non-personal data, accessibility, privacy and ownership of the generated data in the Internet of Things, users are the vulnerable element that continues to be at risk in their interactions with IoT-devices. Many concerns related to the technology of IoT have been emphasized throughout this thesis but as of this moment, there are no clear solutions to either definitions or legal regulations that are enough to ensure protection of users nor devices. With the emergence of the virtual and physical world, Lupton and several other researchers have stated that health and medical information are particularly one of the most valuable commodities for hackers. The development of IoT has contributed to the advancements in medical care. Implemented medical devices (IMD) are through surgical procedures operated into the patients´ bodies. They are used as a method for improving life quality for many patients. Camara et al states that IMD are electronic devices which are implanted into bodies to either treat a medical condition, monitor or improve the functions of different body parts (1, 2015). Examples of IMDs include pacemakers, defibrillators, neurostimulators, drug delivery systems in the form of infusion pumps and a variety of biosystems (Camara et al, 1, 2015).

Camara et al states that several of the newest IMDs have incorporated communication and networking functions which are known as “telemetry” (1, 2015). Telemetry increases the sophisticated computing capabilities in such a way that the devices have an increased intelligence and offers the ability of medical personnel accessing the IMDs from a remote location (Camara et al, 1, 2015). These devices can contribute to the reduction in time spent in hospitals, and therefore, increase the patients´ independence despite the medical conditions they might have. Although there are many advantages in this development such as reduction in cost, time and an increase in independence, there are several risks connected to these developments. Particularly the debate about accessibility, data ownership, privacy and security. Threats and attacks against IMDs may result in fatal consequences (Camara et al, 1, 2015). The privacy risks include the transmission of data through eavesdroppers that may have access to listen to the channel which would lead to a severe privacy breach. Storage of

sensitive information in IMDs is of great size. As IMDs are part of the collection of IoT-devices, the same security protection layers and lack of clarification of definitions surrounding the technology exist in these devices as well. One weak link lead to the vulnerability of the device and the user. As the technology continues to develop in such terms that it is emerging into the physical world and body, legal regulations are utmost important to address but currently, neither legal regulations or safety measurements are adequate to ensure protection of IoT-devices nor IoT-users. Especially, breach in security or privacy in such devices may be fatale but as mentioned, users may not be aware of the risks they are exposing themselves to. Therefore, the debate about data ownership is crucial to establish and address but as for the insufficient legal regulations that exist today, the set of ethical guidelines that was provided earlier in this chapter, should be mandatory to follow. The guidelines may increase the awareness to ensure that treatment and protection of users and devices are adequate and executed in the best interest of the users of IoT. This suggests that despite the limitations within control and regulations by legal compliance, there should be a demand that ensures that general ethical rules should be followed during the design, production and usage of the IoT-devices.

8. Assessing the complex interaction between users and smart things

Nancy K. Baym states in “Personal Connections in the Digital Age” that “people are adaptive, innovative, and influential in determining what technology is and will become” (151, 2010). It is important to understand this statement in such a way that without users of technology, the technology will not succeed. Without integration of the technology, the technology will not develop as there is no usage for it without the human aspect. Especially in the context of the Internet of Things, without active users of smart objects, the technological developments will decrease as it is not beneficial for neither users nor producers of the technology, to continue. Hayles has stated that nonconscious cognitive assemblages include technical and human cognizers, and the power of these assemblages are maximized when all functions of a system are well-defined and working together (2, 2017). In terms of the Internet of Things, programmers and designers challenge themselves to discover and create new aspects within

the technology, and in some cases, the technology is developed to simplify tasks that were primarily performed by humans. In some situations, the result of reducing the human aspect may give a different conclusion than if the human were to perform the same task. The technology would solely focus on the details and script that were programmed into their code, however, through an interaction with humans, the result will be affected by the human aspect. The result provided by the technology would be clearer and more factual, depending on the information that was programmed into the technology. If a human performed the same task, the result might be more diverse and be built on more than just the factual data. Studies have shown that neither humans nor technology give the best result, but a combination of the technological and human aspect will be closer to a perfect score. Thus, suggesting that digital technology is important to integrate into human lives but not at any cost.

In the book "From AI to Robotics: Mobile, Social and Sentient Robots", Bhaumik writes that modern-day medicine has contributed to developing embedded devices and wearables such as pacemakers, heartbeat and pulse rate monitors (340, 2018). The implemented medical devices discussed in chapter 7 are perfect examples of the developed embedded devices and wearables Bhaumik is referring to. Research suggests that soon, humans and computers will be connected through "direct neural interfaces" (Bhaumi, 340, 2018). "...from mind to the computer to the internet, where instead of using senses as touch and vision, there is direct neural interface in both directions", suggesting that the level of interactions between technology and humans that are available today will expand further (Bhaumik, 340, 2018). This leads to the utter importance of sketching out legal regulations and clarifications throughout the interaction between digital technology and humans. As stated, the development of digital technology will only continue, thus enhancing the importance of both maintaining and increasing the continuous attention on users. Furthermore, Bhaumik states that an emergence of developed technology will continuously invite users to incorporate embedded electronics into our biological systems "as means to monitor and enrich our metabolic processes, extending our longevity and add to more mind power" (340, 2018). The concept of quantified self supports this statement. The increase of opportunities in the process of operating smart devices into the physical body, have given patients that were dependent on regular appointments at hospitals, a more independent everyday life where they are no longer

defined to regular check-ups. Thus, the many positive aspects of the development of the Internet of Things.

Hayles´s statements about unconsciousness is supported by Bhaumik´s claim that "unknowingly, we already use our minds as extensions of the internet, with resources such as Wikipedia and other online databases, we consider clicking our phones rather than relying on our retention of information or extending our thoughts, and with embedded electronics in our body, this process of checking an online database will become ubiquitous" (340, 2018). Technology does not reflect "neither human values nor adhere to human virtues" (Bhaumik, 340, 2018).

8.1. Key principle in both self-monitoring and IoT is data collection

The human aspect including the human values and virtues are crucial to assess in terms of the complex interactions with technical systems as it may provide intel to understand more about the motive and desire for the usage of digital technologies. Specifically, with the Internet of Things, users generate data through their interactions with smart objects which collects the generated data. As the number of smart objects increases so does the possibilities of how users are able to self-monitor themselves. The abilities IoT-devices have to collect information about users, their activities and their behaviour through its technical components, makes them great tools for monitoring and tracking specific elements about the users, which leads to the availability of the generated data for internal and external entities. However, the tools they use for self-monitoring may create more challenges for them than they are aware of. With all the smart things that are available today to monitor activities, physical bodies and patterns, a linkability among the smart objects may have the opportunity to create concerns regarding privacy and data ownership. The linkability among smart objects are optimized when an IoT-user is interacting with several smart objects as they communicate with each other and transmit data between them. Although the actions of those that desire to self-track are motivated by themselves, the knowledge about which smart objects they use to achieve the act of self-tracking may affect how vulnerable they are in their interactions with IoT-devices. As a disclaimer, it is necessary to mention that the use of IoT-devices may not be solely or primarily aimed at self-tracking, but the use of IoT-devices do show that through

users´ interaction with the devices, they do self-monitor. This is possible to see with the use of implemented medical devices as health professionals can monitor vital signs wireless from a remote location. Additionally, the use of smart vehicles, the self-monitoring can be seen through this usage as well. The opportunity of remotely accessing the car through their smartphone to start the car, check its battery status (electrical cars), its location and to heat up the car in advance. Although the aim of owning a smart vehicle may not primarily be the ability to remotely access the car, it does create opportunities for such an act. Therefore, it becomes an action that is like those that actively self-monitor themselves through smart objects. The use of digital technology contributes to a configuration of selfhood, embodiment and social relations. And the digitization of bodies and selves are increasing in many different aspects, and therefore, the use of smart objects becomes an element of the process of digitization of the physical body and the self.

Majumdar suggests that the primary aims of both quantified self and the Internet of Things are not very different as the key principle in both, is data collection (2015). Majumdar emphasizes that the three major factors which are involved in the ecosystems include sensors, data and processing (by applications). In both quantified self and IoT, there are similarities in the visualizations of the occurring events. These similarities are local sensing, data integration, analysis of things and cognitive action (Majumdar, 2015). It is suggested that if these two concepts are merged together, the outcome will provide a more instant collection of information, therefore, increasing the optimization, efficiency, effectiveness, the collaboration between developers, designers and the target audience, prevention of chronic conditions and research (Majumdar, 2015).

The earlier examples of the Internet of Things suggest that the motive behind the design and creation of smart devices is convenience. It was more beneficial for the programmers that developed the vending machine to create a program that they could use prior to physically walking to the soda machine to either purchase warm sodas, cold sodas or find an empty machine. The motivation show that they would rather push themselves into creating something new and innovative than walking a longer distance in hopes to find a cold beverage. This major event and the history behind the creation of the vending machine lays a foundation in which factors that motivate IoT-producers in their quest of developing and

creating IoT-devices. However, it is important to remember that the development that has followed the vending machine, has been massive and steep, and that the possibilities that exist today are far more than at the time of the development of the vending machine. At the same time, it is important to be aware of the factors and elements that have supported and contributed to the development. The history of IoT show that the development of the technology was depended on other components such as RFID, GPS, etc. to be developed. Which entails that the technology did not have the capabilities to be developed or progress further without these components.

8.2. The emergent of the physical and virtual world

Through the process of establishing key characteristics for the Internet of Things, it contributes to maintain a consistent view of IoT which distinguishes it from other digital technologies. One of the most agreed upon definitions of IoT is that it is a method of increasing information sharing in such a way that leads to a better world for all human beings. Basically, the Internet of Things connects humans and smart objects, emerging in the virtual and physical world. Atlam et al states that the technology of the Internet of Things aims at improving the quality of people's lives by generating new applications that facilitate daily activities (4, 2019). Smart objects are meant as a tool of optimization and efficiency. An approach to simplify ordinary assignments. Additionally, the ability of the dynamic IoT-environment creates more opportunities of simplifying the lives of users. However, as an approach to simplify and optimize their everyday lives, users are more vulnerable to risks and threats than they are aware about. Despite what may seem convenient, the amount of data that are given up may be more than they are gaining through the transactions. The communication among smart objects give more opportunities of exchanging and sharing data with each other, this may lead to more interconnected information about the users. The ability to connect the IoT-devices to a focal point may seem as a method of efficiency but in regards to the concerns of IoT and the challenges users are faced with, it means that more information about the users are linked together which leads to information that initially were non-personal becomes personal information. It becomes personal information in that sense that more information is linked together, creating a more complete image of the user, personal habits and behaviour. With all the smart objects communicating and sharing information, it becomes difficult for the

users of smart objects to maintain control about who has access, storage, external and internal entities´ knowledge about users, and the usage of the information.

For the Internet of Things, Atlam et al has mentioned a set of essential characteristics to better classify the technology; large scale, intelligence, sensing, complex system, dynamic environment, massive amount of data, heterogeneity, limited energy, connectivity, self-configuring, unique identity and context awareness (4, 2019). The combination of these essential characteristics are parts of the foundation that makes the technology of IoT unique, and that legal regulations and measurements are not adequate to protect users and their personal data through their interactions with IoT. Traditional measurements have stated to not be enough to protect users in their interactions with smart devices, especially due to the characteristics of IoT. The emergent of the physical and virtual world that have occurred because of the development of the Internet of Things have created new issues and challenges that are beyond those that have previously existed.

As IoT-producers and third actors have access to the users' personal information, the data becomes enfolded within networks and economies. Lupton states that the configuration of data assemblages is through “systems of thought, forms of knowledge, business or government models, human users, practices, devices and software, and sometimes by networks of other users and agents other than the self-tracker himself” (15, 2016). Lupton states that the data assemblages which are produced through data practices are split into two parts; active and passive data practices (15, 2016). Active data practices consist of the outcome of self-tracking while passive data practices are different forms of personal data collection which may be viewed as characteristics of other forms of transactional user interaction with online technologies (Lupton, 15, 2016). Lupton has described data assemblages as a complex socio-technical system composed of many actors that are mainly interested in data production (15, 2016). The interesting part with data assemblages is that they are always alterable, effective, and conscious to new inputs and interpretations. Through configuration of them, detailed profiles about users are formed by leveling out the heterogeneity of the information. Although the intention for most of the generated data may be for the users, there is little to no knowledge about who can access the users´ data or use it (Lupton, 15, 2016). Which leads to the continuous debate about data ownership. The lack of

knowledge about accessibility and usage of collected personal data, have forced some users of smart objects to attempt to regain some of the control over their own personal data. Their attempts are responses to a "growing awareness of the ways in which personal data are structured, archived and appropriated by commercial, criminal, government or surveillance agencies" (Lupton, 18, 2016). The response show that there is some knowledge about how data is stored, used and collected. With an increasing knowledge about security, privacy and data ownership in the Internet of Things and its devices, some users are attempting to restrain the usage of IoT-devices. Different studies that Lupton has performed, have shown results indicating that users of digital technology have a vague idea about the usage, storage and accessibility of their personal data, however, an uncertainty remains about the details of the matter and the available options they have to protect themselves and their personal data (18, 2016). Despite a small growth in awareness of the challenges with privacy in IoT-devices, there is little knowledge about how to protect themselves in their interaction with the devices. And because of that, it is difficult to find solutions to how to continue to use the device while protecting themselves. The protection of users of IoT needs to start with the producers and the legal authorities. Without the correct measurements, it becomes difficult, almost impossible for IoT-users to protect themselves. In most cases, there is an informed consent that the users must agree to in order to use the device. As with many other digital technologies, the language of such a consent is difficult to understand for the regular population as it is necessary with knowledge about the elements to fully grasp the extent of what they are consenting to. According to Tzafestas, the "principle of informed consent" is of utmost importance in contracts between IoT-providers and IoT-users (2, 2018). Users must sign an informed consent in many situations, prior to using the devices. These informed consents are service contracts with "terms of use" which typically is difficult for most IoT-users to fully understand the depth of (Tzafestas, 2, 2018). It is plausible to presume that if the users had comprehended the risks and harms that these terms could cause, they would never have agreed and signed them. To be able to provide precise recommendations for maximizing good and minimizing harm, it is important to review IoT and to understand the limitations of protective legal and regulatory frameworks (Tzafestas, 2, 2018).

8.3. The optimization of integration

Hayles states that computational media have a noticeable advantage over other invented technologies as they have a “stronger evolutionary potential than any other technology” (33, 2017). This is due to their cognitive capabilities which allows them to enable these capabilities to simulate any other system (Hayles, 33, 2017). This can be seen in the context of humans, as they are not the largest nor the strongest. Their superior cognitive capabilities contribute to achieve “planetary dominance with their ecological niche” (Hayles, 34, 2017). These “smart” capabilities that are swiftly transforming technological infrastructure, are incorporating themselves into every other technology (Hayles, 34, 2017). Hayles defines computational media as the “quintessentially cognitive technology”, thus establishing a special relationship with “the quintessentially cognitive species, Homo sapiens” (34, 2017). Since both humans and computational media are “quintessentially cognitive” within their own field, the interaction between them is complex. Thus, increasing the need to study and research the complex interaction and what arises from these communications. Hayles emphasizes that the bigger the cognitive components of a technological system, the more unpredictable are their specific developments due to the cognition within flexibility, adaptability and evolvability, hence the Internet of Things.

Through the socio-technical perspective, the aim is to optimize the interaction between technology and social subsystems which entails that with the use of socio-technical perspective, systems are designed with the ability to adapt to the needs of humans and complex social environment requirements. Many IoT-devices are designed and produced as tools for optimizing normal practices forms such as adjusting temperature, opening and locking doors, tracking physical activity, and more complex actions with industrial and inventory processes. By following the socio-technical perspective and thereby, developing devices that can integrate into the users´ everyday lives, the Internet of Things have succeeded in such a way. For instance, the use of wearable fitness trackers may motivate users to be more physically active as they are able to track their activity and receive statistics based on their data. The wearable fitness trackers are easier tools to incorporate into the users´ everyday life, both as a motivation and as a method of self-tracking themselves. Which leads

to a study conducted by Michel Foucault that focused on how humans obtain knowledge about themselves.

8.4. The digitalization of the body and the self

In Foucault's study of the technologies of the self, his objective has been focused on the different methods in how humans develop knowledge about themselves, such as economics, biology, psychiatry, medicine and penology (1988). Foucault has distinguished between four major types of technologies; production, sign systems, power, and the self. Within the technologies of production, Foucault refers to what "permits us to produce, transform or manipulate things", technologies of sign systems allow humans to use "signs, meanings, symbols, or signification" (1988). For the technologies of power, Foucault distinguishes as the determination of human conduct and thereby, submits them to "certain ends or domination, an objectivizing of the subject" (1988). In relation to the technologies of the self, Foucault refers to the authorization of the individual to be affected by "their own means or with the help of others a certain number of operations on their own bodies and souls, thoughts, conduct, and way of being, so as to transform themselves in order to attain a certain state of happiness, purity, wisdom, perfection or immortality" (1988). Meaning "the constitution of the self through various discourses; operations on bodies, souls, thoughts and conducts" (Foucault, 1988). Within the technologies of the self, it is defined as various forms of "self-care" both in historical and cultural settings. Claiming that social media is the new technologies of the self as users portray themselves through sharing or not sharing on different social platforms. Creating a persona through the content of what is shared on different social media. However, with digital technologies, the online and offline personas are becoming closer than before as the virtual and physical world are emerging.

Ramírez states that self-modification can be viewed as an ancient human practice but with the use of technology, it enables us to modify our lives on existential, experiential and informational level (1, 2016). With the use of informational technologies, new dimensions for humans have been discovered to transform bodies, minds and the self-conception (Ramírez, 1, 2016). Digital technologies contribute to different methods of alternating contexts and practices in how humans shape their personal identities, and therefore, how they relate to

groups, societies, cultures and environments (Ramírez, 1, 2016). As a disclaimer, such practices have existed prior to the development of digital technologies, however, with the increased use of digital technologies, new forms of conducting such acts have occurred. In terms of the technological shifts that are occurring, is due to “the availability, range of action, and power of our self-modification tools” (Ramírez, 1, 2016). Thus, blurring out the lines between the virtual and physical world. Again, pointing towards the socio-technical systems whereas the human practices and technologies form complex socio-technical systems. Ramírez states that the thought of technological systems and human beings analyzed independently from each other is “a crucial step towards developing a much-needed contemporary humanistic critique of how technologies are shaping our sense of self”. (2, 2016). With the use of all socio-technical systems, it contributes to impact human self-understanding, and thus expanding the capabilities of the usage of self-modifying tools (Ramírez, 2, 2016). How individuals self-modify and self-explore, thus empowering their own self-understanding is supported by the opportunities and availability of the IoT-devices. Ramírez supports his statement about the impact of socio-technical systems on individuals' self-understanding by describing the exposition of users by digital technologies to “potent and inconspicuous forms of ontological tinkering” with and without awareness of such. This leads to an increasing number of aspects in our lives, specifically the development of users´ social selves and the self-understanding, becoming “matters of design” (Ramírez, 2, 2016). What can be seen from Ramírez´s statement of “potent and inconspicuous forms of ontological tinkering”, is a reference to the impact digital technologies may have on users without their awareness of the situation. This can be related to the statements provided by Hayles in terms of the powers of unconsciousness. Digital technologies can therefore contribute to an alternation of the users´ self-understanding which leads to an impact on their social selves. Due to the socio-technical systems, the distinction between online and offline are becoming smaller as the virtual and physical world are emerging (Ramírez, 2, 2016). Thus, not solely enhancing the reality but contributing to re-engineer it (Ramírez, 2, 2016). This is possible to see in terms of extimacy and intimacy as users of digital technologies may shift their limits between private and public depending on the situation. Intimacy is defined equally to privacy as it involves several aspects of isolation, solitude, anonymity, secrecy, and reserve. Closely related to the notion of being a person and identity. Elements that support the notion of intimacy can be seen through protection of relationship, strong emotional bonding,

vulnerability and caring. As for digital technologies, it contributes to the exposure of a greater amount of a user´s intimacy. As the digital technologies increase with more opportunities of sharing, various forms of self-disclosure are evolving, thus creating a constant tension between the desire of exposing oneself and the fear of being displayed, objectified and exploited. Through the act of sharing personal information, users make a choice whether to share. Users may share private information on their social media, however, if that same information is shared without their consent, it may affect their opinion on boundaries between public and private. Sensitive information published by the users themselves is referred to as extimacy as the personal information may be equal to information published by other entities but if users are in control of what is shared in intimate situations, it contributes to the divide between extimacy and intimacy[4].

8.5. The transactions between risks and benefits

The results from the study conducted by Zheng et al indicate that users of IoT-devices are inclined to disregard their concerns about personal privacy risks for the convenient features of IoT-devices. This reason was, according to the interviews, the most frequently cited reason for the adaption of the IoT technology (Zheng et al, 2, 2018). According to Zheng et al, these opinions are supported by previous work conducted on users' behaviours towards earlier technologies and show that convenience continues to be a primary justification for the scarification of privacy for the users of IoT-devices (2, 2018). Furthermore, the study shows that users are more willing to share their data with external entities if it is in their beliefs that the exchange will provide benefits for them and their families (Zheng et al, 3, 2018). These benefits are in terms of automatic software updates and new features. The users´ attitude towards the sharing of information may be seen in terms of the differences between intimacy and extimacy as they are formed by the lack of control over published information. However, by choosing to share personal information in order to gain benefits, it may offer a certain feeling of control. Information that users would not typically share, might be shared if there are possibilities of receiving benefits in return.

[4] References are drawn from conversation with supervisor and an unpublished powerpoint presentation.

Participants of the study reveal that they were more cautious of sharing data with advertisers and government entities. Their opinions were mixed in terms of benefits with personalized advertisement and eventual opportunities for local governments to improve services based on the collected data and analysis of the data provided by smart homeowners (Zheng et al, 3, 2018). Through the process of purchasing an IoT-device, some of the key factors that contributed to the choice of brand, is brand familiarity and reputation. The participants of the study were more inclined to believe that well-known companies, both traditional technology companies and home appliance companies, were more successful in protecting the users´ privacy throughout the interaction with known IoT-devices (Zheng et al, 3, 2018). Within the trust-based purchasing decisions, the interviewees were more convinced that the IoT-devices that they purchased, had adequate privacy protection without any additional actions to preserve their privacy (Zheng et al, 3, 2018). For the last key element of the study conducted by Zheng et al, was the users´ awareness of privacy risks in relation to inference algorithms that collect data from non-audio and visual devices. The results concerning the users´ awareness of such algorithms, show that users are skeptical of the privacy risks with devices that do not record audio or video (Zheng et al, 3, 2018). And that there is a lack of awareness of the possibilities of using machine learning algorithms with the use of non-A/V data to interpret more sensitive information. For this type of sensitive information, Zheng et al have highlighted sleep patterns and home occupancy, which is data that can be collected from non-audio and visual devices (3, 2018). The other three key elements that were focused on in this study, have shown results that can be supported by earlier research on the fields but the results discovered from questions in regards to non-audio and visual devices have not been found in prior research (Zheng et al, 3, 2018). Based on these results, Zheng et al have suggested that designers of IoT-devices should explore the opportunities of improving the convenience of privacy control on IoT-devices and associated mobile applications (3, 2018). Additionally, further research should focus on “developing mechanisms for centralized privacy control in smart homes which have the potential of seamlessly integrating into home life and meet the users´ privacy needs with minimal effort” (Zheng et al, 3, 2018). The study shows that IoT-users are more willing to sacrifice their privacy if there are benefits through the interaction. Additionally, convenience and the ability to be connected are in users´ opinion, a bigger advantage than having control over their personal information. It is possible to see some indications towards a lack of awareness and knowledge about the privacy risks

with IoT-devices, may have contributed to a form of naivety in users. The reasoning behind that, is that users trust producers of IoT to protect them and their personal data. The answers from the participants in the study builds up this assumption. Especially brand familiarity. Without a proper understanding and awareness of privacy and security risks with IoT-devices, users are vulnerable in their interactions with smart objects. However, despite having an understanding and awareness of privacy and security risks may not adjust their level of vulnerability. In fact, through interaction with smart objects with the abilities and security measures that exist today, IoT-users are vulnerable. If producers of IoT-devices have not designed and programmed sufficient privacy protection layers in their products, and with a trust in them to do so, users are not only very vulnerable, but more taken advantage of than they realize.

Participants in the study performed by Zheng et al, state that if there are promises of benefits for them and their family, they are more willing to jeopardize their privacy. Although, their thoughts might be solely focused on one of the devices, but the reality is that all these smart devices such as thermostat, vehicle, coffeemaker, light bulbs, refrigerator, pacemaker, and so on, communicate with each other. The combination of all these devices connected and communicating, creates a whole network and interconnected links about users and their habits and preferences. Convenience is the key factor in the act of integrating IoT-devices into users´ everyday life. And the human body is becoming a rich source of data and information for producers and third actors of the Internet of Things. Generated data creates a massive source of information about the users´ bodies, surroundings, patterns and behaviours. The collection of all these devices communicating with each other and the servers of their producers contribute to a huge amount of information about the users of IoT-devices are available for several actors to access, with or without both the consent and knowledge of the IoT-users. And as stated, data is an economic asset. External and internal entities are earning a profit of users of IoT.

The different chapters and subjects that have been presented throughout the thesis have a common element among them which show an unawareness of the characteristics and capabilities in the IoT-devices, hence the transmission and communication methods. The users´ unawareness are jeopardizing much more than they may realize.

8.6. Security is not associated with IoT-devices

As with many of the issues surrounding the technology of IoT, the core of the issues is unclear and imprecise definitions which complicates the process of researching and finding possible solutions that protect devices and users. Within these challenges, are the security concern and the potential security threats devices and users may face. In terms of the definition of cybersecurity, the definition provided by Craigen et al was discussed in chapter 6, and is as follows, "cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (1, 2014). It has been attempted through this definition to cover the essential characteristics of what lays within the term of cybersecurity and its aim. Rizvi et al have stated that security is one of the most "paramount technological research problems that exist today" (2, 2018). This can be seen in context of how security breaches affect devices and users, and especially, with IoT, security breaches can be more severe and, in some cases, fatal as the technology has emerged into the physical world. Security in technological aspects contain the power to control the level of security and vulnerability the different technologies have. Furthermore, as stated previously, privacy and security aspects in terms of IoT, have been classified as "a class of devices and associated processes that will lead to sharing and exposing more information and keeping fewer secrets" (Weinberg, 2, 2015). Thus, exponentially increasing the importance of well-functioning security measurements to ensure the protection of both IoT-devices and users. It is concerning that research and studies on security in IoT show that the word "security" is not associated with this category of devices (Shen et al, 1, 2019). IoT has stretched the boundaries between the virtual and physical world, and thus increases the necessity to have a well-function security regulation provided by both legal authorities and IoT-producers. The situation that arises when security is not associated with IoT-devices, is that IoT-users might be exposed to massive attacks, both physical and virtual.

The methods of incorporating security into the technology of IoT are through built-in designs, which offer the potential of securing the data transmissions and data storage, both within the systems and its application (Rizvi et al, 2, 2018). Furthermore, the responsibility of ensuring

that IoT-devices are secure and safe to use, lies with the manufacturing companies and the companies that use the devices for personal use, production, distribution and commercial. The security threats that devices and users are facing, are risks such as identity and data theft, device manipulation, data falsification, server/network manipulation and subsequent impact to application platforms, (Rizvi et al, 2, 2018). The background for the data security concerns of IoT systems are due to the lack of well-defined perimeters, they are highly dynamic and continuously changing due to its mobility (Bertino, 1, 2016). As well as its highly heterogeneous abilities due to its communication medium and protocols, platforms and devices. Several authorities have stated that it is difficult to secure IoT-devices, and as a result, the users. This is due its information systems and mobile environment. Nevertheless, it is necessary to mention that the available IoT-devices have scarce resources, thus meaning that they are not able to use the complete security suites that are typically used in networks. Which leads to new challenges as the design of such security suites must be unique frameworks, compiled especially for IoT. Furthermore, due to its scarce resources, the process of protecting IoT-devices and its users, must not be at the expense of performance, meaning that lightweight security solutions must be used. By incorporating different solutions to secure IoT-devices, higher cost may follow which means that the performance and price of the IoT-devices may suffer. The cheaper the devices, the higher the possibilities of being more vulnerable than with a more expensive device. It should be desirable to buy IoT-devices at a higher price if that entails that users and their devices are better secured and protected throughout their interaction. However, in many cases, users often tend to lean towards the cheaper alternatives. The cheaper alternatives imply weaker security features.

If the interaction and usage of IoT-devices are seen in terms of transactions between users and producers of IoT, goods as exchanged between users and producers of IoT. Users of IoT-devices obtain the ability to use and interacting with IoT-devices. Goods in terms of the usage of IoT-devices are transacted in the access producers and third parties which are companies that provide the statistics and analysis the information, to the user's personal data. Data that initially is not considered personal information in terms of laws concerning privacy but if linked with other data about the same user may become personal information about the user. Without proper regulations that are specifically aimed at data collection through interaction with IoT-devices, there may be loopholes that may make IoT-users vulnerable.

8.7. Failure to distinguish between personal and non-personal data

The motives and interest of integrating IoT-devices into everyday lives are supported by many different elements. IoT give opportunities for simplifying activities that previously were a routine, e.g. boiling coffee in the morning. And although users of IoT may not have enough knowledge of how IoT-devices collect, store and use their generated data, measurements must be taken to protect users in their interaction with these devices. It has been mentioned previously in this thesis that definitions of privacy, data and personal information are not adequate to ensure that users and their personal information are protected. And in the context of data ownership, the lack of definitions and clear lines contribute to a more challenging concern about who owns and has access to the collected data. Based on that, a clarification of data, non-personal and personal information is necessary. As stated earlier, the line between personal and non-personal data is blurry. Which means that with the use of analytical and technological advancements, data that previously would be defined as non-personal can be defined as personal (Janeček, 4, 2019). As the usage of such tools may increase, definitions provided by GDPR and the guidelines they follow, should be sufficient to protect users and their data. However, with insufficient guidelines and regulations such as clear and adequate definitions, the IoT-users are at risk. Janeček has stated that through the definition of personal data as "any information relating to an identified or identifiable natural personal" provided by GDPR, it disregards the distinction between data and information (6, 2019). The dilemma about data ownership turns into the ownership of personal data rather than the ownership of personal information. Definitions defined by legal authorities have distinguished data and information as two concepts which implies that it is necessary with a more clarified distinction between data and information. Janeček states that the distinction between data and information may have been one of the reasons why the debate on data ownership in IoT continues without a solution (7, 2019). With an information-centred starting point, the formal representation of information and the source of identical information becomes confused. To be able to define certain solutions to the debate about data ownership in IoT, it is necessary with clear differences between data, non-personal and personal information. Furthermore, an understanding of how personal information can be obtained through non-personal data and information with the use of analytical and technological advancement is necessary. IoT-users

should be certain that their generated data are secure in their interactions, however, that becomes difficult when the lines between personal and non-personal information are blurred. The statement by Bertino that was previously mentioned, “the human body is becoming a rich source of information”, suggests that collected information from interactive IoT-devices are fine-grained data provided by the human body, and the users´ activity and habits (2, 2016). Bertino states that the collected data from IoT-devices are typically very rich and often contain metadata such as location, time and context (2, 2016). Due to the collection of metadata and fine-grained data, it becomes easier to interpret personal habits, behaviours, and preferences of the users. Thus, studying the statement by Bertino about the human body as a rich source of information supports the blurred line between the physical and virtual world. Although the intention of IoT-devices is creating more efficient methods of achieving certain goals, the producers and external entities are collecting a massive amount of information from the users´ physical bodies. Despite, the motive behind the data collections are explained as personalizing the user's experience of the IoT-device, and making them better suited for each individual, much of the collected data are not necessary to personalize the user's experience of smart objects. More information about each individual is collected due to the generated data from interactions with these devices. With such a massive amount of information collected by the IoT-users, it is alarming not knowing the type of information internal and external entities are interested in, and whether, some types of data are unavailable for them to collect and transmit further. The unknown about external and internal entities´ accessibility of collected data, is dangerous. The smartphone creates more connections than users of IoT-devices may be aware of. Without the knowledge about the amount of information and the types of information that are collected, the users are deprived of the rights to determine what it is private information and what they are willing to share in order to receive the benefits of such a transaction between information and services. This leads to the determination of extimacy and intimacy. Some information users may choose to share themselves, however, if the choice is out of their control, they may be more reserved as to sharing these types of information about themselves, and their personal habits and preferences.

Without clear guidelines and regulations to ensure the protection of the collected data that is generated through interactions with IoT-devices, the users´ privacy is vulnerable. In the constitutional law of countries around the world, privacy is preserved as a fundamental right

(Solove, 13, 2018). And with the development of the new information technology, it has become more difficult to preserve the privacy of the users. As stated, privacy is a broad concept and difficult to precisely define. With a concept that broadly covers many different elements surrounding an individual, privacy becomes an essential issue for freedom and democracy (Solove, 13, 2008). To integrate new information technology, and take advantage of technological development, it is necessary to preserve the fundamental rights users have. A fundamental right to control your own physical body, home, personal information, freedom from surveillance and protection from interrogations. Without a clear definition and a guideline of how to protect the users´ privacy, it becomes difficult to solve the privacy issue in relation to both IoT and other digital technologies. Solove claims that the difficulties in defining the concept of privacy and its importance are related to insufficient privacy laws (13, 2008). This increases the need for more awareness and knowledge about issues in IoT as it may be a key factor in finding solutions and preserving both the technological development of IoT and users. Despite numerous statements claiming that privacy is under “attack”, people's actions do not support these statements. Additionally, it may seem as though privacy is not an important factor in users´ interaction with digital technologies. This statement is supported by the results shown in the study conducted by Zheng et al. The benefits users may be given through their interactions with IoT-devices are more important for them in terms of what they see as more valuable. And in many cases, privacy is what becomes less valuable. It is understandable that benefits for users and their families are viewed as more important than their privacy if there is a lack of awareness and knowledge about how users´ privacy is being taken advantage of by IoT-users and external entities.

The question remains about how the abilities of IoT and other digital technologies develop at the same time as persevering the users and their personal data. It continues to circle back to the unclear definitions of data, non-personal and personal information, privacy, data ownership and security. The starting point to finding possible solutions to these issues concerning IoT, is clarification of legal regulations and definitions. Without clear guidelines for both legal authorities and IoT-producers, it is difficult to ensure protection of IoT-users and IoT-devices. And without secure IoT-devices, the IoT-users are still vulnerable, with or without sufficient regulations and guidelines.

Privacy issues have not recently appeared, however, with the dynamic environment of IoT and its capabilities of blurring out the boundaries between the physical and virtual world, it becomes thus more important to identify and clarify the issues and find solutions to them. With inadequate regulations and definitions by legal authorities, it is challenging for both producers and users of IoT to ensure the protection of their interactions. Despite somewhat insufficient regulations and measurements by the legal authorities hence the data ownership, there are some guidelines IoT-producers should follow to create a safe environment for users of IoT. These are in relation to the ethical conduct of producers and designers of IoT-devices.

8.8. IoT-producers´ ethical conduct

The concept of ethics contributes to provide standards of obtaining good human behaviour beyond the legal minimum (Tzafestas, 1, 2018). Thus, the importance of having ethical guidelines in the process of designing and producing IoT-devices. In relation to IoT, where there may be a lack of clarified definitions and regulations, by following ethical guidelines throughout the design and production phases, it may provide a method for protecting the users and their personal data when legal authorities and measurements may not be adequate. The set of ethical guidelines that this thesis is referring to, is discussed in chapter 7. Whether or not the standards are decided by the law or ethical and moral guidelines, that should not affect the level of neither respect nor conduct. One of the reasons correct legal and ethical regulations are necessary for the protection of privacy, data ownership, security, trust improvement and the development of proper standards, is due to the new social, economic, political and ethical landscape that is created by the Internet of Things (Tzafestas, 1, 2018). Despite pre-existing ethical concerns and legal challenges with digital technologies, IoT have contributed to new challenges. Tzafestas have argued that due to the high amount of data that is generated and analyzed in the IoT, more complex and demanding ethical and responsibility challenges are occurring than those of the “pure Internet” (9, 2018). And that is why an increased awareness about pre-existing and emerging ethical issues is important in the process of decision-making to enhance the positive elements of the IoT. The concern is that, without sufficient regulations and measurements, the interaction with IoT becomes more alarming than the numerous opportunities that are possible with the technology.

Despite the many challenges and concerns surrounding security and privacy issues addressed by both this thesis and numerous other papers and articles, it is important to consider the many benefits and opportunities with the IoT. The aim is to encourage the development of IoT, and secure IoT-users and their generated data through correct and sufficient legal, software, hardware and ethical measurements. Although the criticism that the IoT has faced is justified due to challenges protecting users of IoT, there are very important attributes that the technology is contributing to society. Specially within health as it is possible to see through the development of implemented medical devices that have been discussed.

The important aspect in the next step towards a more secure interaction with the technology, is creating awareness of the occurring issues and finding solutions for these issues. Although many may give the responsibility of protecting the users of IoT to the legal authorities or the IoT-producers, the users of IoT have a responsibility too. When it comes to your own personal data, data that is generated through your interactions with IoT-devices, why should you not be aware of the risks or the vulnerabilities you are exposing yourself to? In a perfect scenario, legal regulations would have a standardized definition of data, non-personal and personal, privacy, and a clarification to the dilemma of data ownership. At the same time, users of IoT should have a better understanding of what is at stake in their interaction with IoT-devices, and therefore, an awareness of the transaction that goes on between users and producers of IoT. What are the benefits for the users in their interaction with IoT? Are those benefits worth the amount of personal data that is transmitted through these devices? There are numerous questions to be asked to every single user of IoT, and some may provide clear answers to them, but some may not understand the vulnerable situation they are in.

8.9. Pulling all strings together

Throughout the thesis, concerns and issues regarding privacy and security associated with the Internet of Things have been discussed and elaborated. In chapter 5 and chapter 6, individual solutions to the concerns have been studied but to find the best method for solving these challenges, a suggested method might be a combination of several suggested approaches.

For the privacy issue, it has been suggested that the technology should be global. And with the use of the same technical processes, it can contribute to enhance interoperability and security. A global standard would be under the same regulatory efforts as well, thus eliminating cultural differences which may have ground in why data privacy rights are viewed differently. Therefore, the cultural differences would not contribute to complicating the privacy concern further. Additionally, Weber states that the rules that should be applied to the IoT such as data protection, privacy laws and technology standards should be designed to ubiquitously encompass persons, things, plants, and animals (3, 2015). These elements are specifically important in the discussion about IoT as it can adjust to many forms, hence its impact on many spheres on human life.

A solution that has been researched and suggested as a possible method of securing devices and users of IoT, is an approach that incorporates privacy and security measurements into the design of IoT-devices. A common issue regarding the challenges of privacy and security, is the lack of emphasis on the protection of users, personal information and devices throughout the design process. By incorporating safety measurements in the start phase of the production of IoT-devices, it may contribute to ensure that devices are both safe from software and hardware threats, in addition to the conserving of the users´ privacy. The privacy by design method this thesis has relayed on, was provided by Perera et al, and aims to function as a framework that can be used to assess both IoT-applications and middleware platforms without any changes and agnostic to their differences (1, 2016). The framework should function as a tool to help guide software engineers. The guidelines for the framework are as follows, the minimization of data acquisition, number of data sources, raw data intake, knowledge discovery, data storage, and data retention period (Perera et al, 3, 2016). The guidelines have a wide focus on many different aspects of the data collection, distribution and access control.

There is a common agreement among researchers of security in IoT that if appropriate measures are adopted and enforced while developing the devices, it may minimize the possibilities of an attacker taking advantage of a weak design to bypass the authentication or the security methods that may be enforced in the devices. Hence the process of allowing and considering security regulations in the design process may prove to be a more effective method of securing data protection rights. By incorporating security into the design rather

than not considering it a constitutive part of the process of designing the devices, it may serve as an approach to help strengthen the security in IoT-devices in such a way that they are secured at various system levels (Babar et al, 3, 2019). The thesis has focused on a suggestion proposed by Babar et al, called “Embedded Security Framework for Internet of Things” (3, 2019). The embedded security framework for Internet of Things is built on five major building foundations; cryptographic algorithms, secure storage, secure boot, secure JTAG and secure execution environment (SEE) (Babar et al, 4, 2019). The security framework is displayed in illustration 1.2 on page 52. Performance, cost and security are three concepts that must be addressed in the process of alternating how IoT-devices are designed (Babar et al, 2019). Advanced performance means the cost increases, and a reduction in cost equals reduction in the performance and security features. With more advanced security, performance will decrease. Performance, cost and security are reliant on each other which means that a solution to these challenges may be a hardware and software-based security architecture. This security architecture would be a mixture of hardware and software that may accomplish overall security goals as it provides sufficient motivation for attempting a synthesis-oriented approach to achieve security system implementations that involved both hardware and software components (Babar et al, 4, 2019). The security architecture is displayed in illustration 1.3 on page 56.

The suggested method for optimization the security for users and devices is with accurate and well-defined regulations that eliminates grey areas of exploiting users and their desire to engage with IoT-devices. The solutions that have been discussed regarding privacy and security issue in the Internet of Things could give a better outcome if they are combined with sufficient definitions and legal regulations. The ethical guidelines should be followed and respected equally to the legal regulations, and thus be considered in the design and production process of IoT-devices. Therefore, it should be demanded that ethical guidelines are followed in situations where legal regulations are not sufficient. This would hopefully ensure that the practices are performed with the best intention to protect both devices and users. By incorporating privacy by design and security by design, the field of the Internet of Things is collaborating to improve the issues and challenges that exist with the technology today. Improvements within privacy and security may contribute to a further development of the technology as the insecurities and possible vulnerabilities users are exposing themselves to,

are reduced. Thus, increasing the interactions between users and IoT-devices. With an active demand for changes to increase the protection of users and IoT-devices, the risks may include a decrease in the development of IoT as users are becoming very vulnerable in their interaction with digital technology. Despite researchers´ claim that producers of IoT have the full responsibility of protecting smart objects and users, the legal authorities and IoT-users share the responsibility to ensure protection. Without a demand for change and increased protection for data privacy rights, it becomes difficult to assess the potential changes to the issues concerning the Internet of Things. It is necessary to continuously address and research the issues regarding privacy, security, data ownership and ethical aspects in the Internet of Things to increase the awareness of these challenges to find solutions and incorporate these solutions in an optimal matter.

Through the technology of the Internet of Things, the split between the physical and virtual world becomes blurry. And therefore, it creates situations where elements that were primarily physical or primarily virtual, are becoming one. Hence the utmost importance of studying the complex interactions between humans and technical systems to enhance the many opportunities that occur within these interactions but ensuring that accurate and sufficient regulations for the protection of smart objects and users are efficient.

9. Findings and conclusion

The theme of the thesis was to focus on various methods for protecting users´ subjective or objective losses of privacy through their interactions with IoT-devices. The capabilities of the technology of the Internet of Things makes it possible to perform tasks and processes more efficient, effective, reduction in cost and time, optimal and mobile. With these infinite opportunities with the use of smart objects, challenges concerning privacy, security, ethical aspects and data ownership are occurring. These challenges have been elaborated and discussed throughout the thesis. Users´ interaction with IoT-devices make them vulnerable as they lose control over their own personal information. Legal regulations and measurements are insufficient as definitions of privacy, personal and non-personal data are not clear in terms of the data collection that occurs with the Internet of Things. Traditional security measurements are not suited for smart objects due to its heterogeneous ability and the IoT´s dynamic environment. Security and privacy features are incorporated as an add-on rather than

embedded in the devices. By incorporating the features into the device as part of the design process, many issues associated with the Internet of Things may be reduced. Additionally, in situations where legal regulations are not adequate, ethical guidelines should be followed to secure both users and devices of IoT. The thesis has suggested several possible solutions to the issues regarding privacy, security, ethics and data ownership, and a combination of several of the proposed solutions may increase the level of protection for users and their privacy. It is beneficial for both producers and users of the Internet of Things to incorporate more efficient protection features for users and devices because the power is maximized when the interaction between humans and technical systems are functioning as a system.

The well-defined interactions and communication circuits between sensors, actuators, processors, storage media, and distribution networks, clarifies the need to continuously study the power the complex interaction between humans and IoT-devices may achieve. Nevertheless, the observations of these interactions contribute to emphasis the necessity to ensure that users are protected throughout their interactions with smart devices to decrease the potential subjective and objective losses of privacy. As a conclusion to the thesis, without a demand by users for more suited privacy and security features, the producers of the Internet of Things will continue to develop the technology without incorporating these features as part of the design process. The perfect future would explore the opportunities of the power of the interactions between humans and the Internet of Things but incorporate more efficient methods of integrating users in such a way that they regain control over their generated data.
Further research should focus on specific methods for users of the Internet of Things to take some of the responsibility in securing themselves. If adequate privacy and security features are incorporating into IoT-devices, and legal regulations and definitions are reestablished, what are the various methods users can apply to protect themselves and their personal information?

10. Bibliography

All URLs in this thesis have been accessed latest May 2020.

Books

Baym, Nancy K. 2015. Cambridge: Polity Press

Bhaumik, Arkapravo. 2018. *From AI to Robotics*. Boca Raton: CRC Press.

Franzen, Jonathan. 2002. *How to Be Alone.* New York: Farrar, Straus and Giroux.

Hayles, Katherine. 2017. *Unthought*. Chicago and London: University of Chicago Press.

Lupton, Deborah. 2016. *Quantified Self*. Malden: Polity Press.

Rettberg, Jill Walker. 2014. *Seeing Ourselves Through Technology*. Palgrave Macmillan.

Reynolds, George W. 2017. *Ethics in Information Technology*. Boston: Cengage Learning, Inc.

Solove, Daniel. 2008. *Understanding Privacy*. Harvard University Press.

Papers

Alhalafi, N and Prakash Veeraraghavan. 2019. “Privacy and Security Challenges and Solutions in IOT: A review.” IOP Conference Series: Earth and Environmental Science. 322. 012013. 10.1088/1755-1315/322/1/012013.

Atlam, Hany and Gary Wills. 2019. “IoT Security, Privacy, Safety and Ethics”. 10.1007/978-3-030-18732-3_8.

Babar, Sachin, Antonietta Stango, Neeli Prasad, Jaydip Sen, and Ramjee Prasad. 2011. “Proposed Embedded Security Framework for Internet of Things (IoT)”. 10.1109/WIRELESSVITAE.2011.5940923.

Bertino, Elisa. (2016). “Data Security and Privacy in the IoT”. EDBT. 2016. 10.5441/002/edbt.2016.02.

Camara, Carmen, Pedro Peris-Lopez, and Juan E. Tapiador. 2015. “Security and privacy issues in implantable medical devices: A comprehensive survey”. *Journal of Biomedical Informatics*. 55: 272-289. https://doi.org/10.1016/j.jbi.2015.04.007

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 2014. “Defining Cybersecurity”. Technology Innovation Management Review. 4. 13-21. 10.22215/timreview/835.

Eloff, Jhp, Mariki M. Eloff, M. T. Dlamini and M. Zieliński. 2009. “Internet of people, things

and services - the convergence of security, trust and privacy".

Fantana, Nicolaie, Till Riedel, Jochen Schlick, Stefan Ferber, Jürgen Hupp, Stephen Miles, Florian Michahelles, and Stefan Svensson. 2013. "Internet of Things - Converging Technologies for Smart Environments and Integrated Ecosystems".

Floridi, Luciano and Mariarosaria Taddeo. 2016. "What is data ethics?". Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences. 374. 20160360. 10.1098/rsta.2016.0360.

Hoffman, Donna L. and Thomas P. Novak. 2015. "Emergent Experience and the Connected Consumer in the Smart Home Assemblage and the Internet of Things". SSRN Electronic Journal. 10.2139/ssrn.2648786.

IEEE Standard Glossary of Software Engineering Terminology, in IEEE Std 610.12-1990, vol., no., pp.1-84, 31 Dec. 1990, doi: 10.1109/IEEESTD.1990.101064.

Janeček, Václav. 2018. "Ownership of personal data in the Internet of Things". Computer Law & Security Review. 10.1016/j.clsr.2018.04.007.

Mashhadi, Afra, Fahim Kawsar, and Utku Acer. 2014. "Human Data Interaction in IoT: The ownership aspect". 2014 IEEE World Forum on Internet of Things, WF-IoT 2014. 159-162. 10.1109/WF-IoT.2014.6803139.

Medina-Borja, Alexandra. 2015. "Editorial Column—Smart Things as Service Providers: A Call for Convergence of Disciplines to Build a Research Agenda for the Service Systems of the Future". Service Science. 7. ii-v. 10.1287/serv.2014.0090.

Ngowi, Lucas, and Nerey Mvungi. 2018. "Socio-Technical Systems: Transforming Theory into Practice". 10.1999/1307-6892/10008768.

Noura, Mahda, Mohammed Atiquzzaman, and Martin Gaedke. 2018. "Interoperability in Internet of Things Infrastructure: Classification, Challenges, and Future Work". Third International Conference, IoTaaS 2017, Taichung, Taiwan, September 20–22, 2017, Proceedings. 10.1007/978-3-030-00410-1_2.

Nurse, Jason, Sadie Creese, Michael Goldsmith, and Koen Lamberts. 2011. "Guidelines for usable cybersecurity: Past and present". Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, CSS 2011. 21 - 26. 10.1109/CSS.2011.6058566.

Patel, Keyur, Sunil Patel, P. Scholar, Carlos Salazar. 2016. "Internet of Things-IOT:

Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges".

Perera, Charith, Ciaran Mccormick, Arosha Bandara, Blaine Price, Blaine, and Bashar Nuseibeh. 2016. "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms". 10.1145/2991561.2991566.

Ramírez, Rodrigo. 2017. "Technology and Self-modification: Understanding Technologies of the Self After Foucault". Journal of Science and Technology of the Arts. 9. 45. 10.7559/citarj.v9i3.423.

Rizvi, Syed & Kurtz, Andrew & Pfeffer, Joseph & Rizvi, Mohammad. 2018. "Securing the Internet of Things (IoT): A Security Taxonomy for IoT". 163-168. 10.1109/TrustCom/BigDataSE.2018.00034.

Shen Y. and PA Vervier. 2019. "IoT Security and Privacy Labels". In: Naldi M., Italiano G., Rannenberg K., Medina M., Bourka A. (eds) Privacy Technologies and Policy. APF 2019. Lecture Notes in Computer Science, vol 11498. Springer, Cham

Sicari, Sabrina, Alessandra Rizzardi, Luigi Grieco, and Alberto Coen-Porisini. 2015. "Security, privacy and trust in Internet of Things: The road ahead". Computer Networks. 76. 10.1016/j.comnet.2014.11.008.

Tzafestas, Spyros. 2018. "Ethics and Law in the Internet of Things World". Smart Cities. 1: 98-120. 10.3390/smartcities1010006.

Weber, Rolf. 2015. "Internet of things: Privacy issues revisited". Computer Law and Security Review. 31. 618-627. 10.1016/j.clsr.2015.07.002.

Weinberg, Bruce, George Milne, Yana Andonova, and Fatima Hajjat. 2015. "Internet of Things: Convenience vs. privacy and secrecy". Business Horizons. 58. 10.1016/j.bushor.2015.06.005.

Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. "User Perceptions of Smart Home IoT Privacy". Proc. ACM Hum.-Comput. Interact. 2, CSCW, Article 200 (November 2018), 20 pages. DOI: https://doi.org/10.1145/3274469

Articles

Aruba. 2019. "Data Privacy Laws in APAC: What You Need to Know". 06.12.2019. URL:

https://blogs.arubanetworks.com/solutions/data-privacy-laws-in-apac-what-you-need-to-know/

Ashton, Kevin. 2009. “That “Internet of Things” Thing”. RFIDjournal. URL: https://www.rfidjournal.com/that-internet-of-things-thing

Braun, Andrew. 2019. “History of IoT: A Timeline of Development”. IoT Trends. URL: https://www.iottechtrends.com/history-of-iot/

Cook, James. 2016. “A complete history of internet-connected fridges”. Businessinsider. URL:https://www.businessinsider.com/the-complete-history-of-internet-fridges-and-connected-refrigerators-2016-1?r=US&IR=T

Elder, Jeff. 2019. “The Internet´s First Smart Device”. Avast. URL: https://blog.avast.com/the-internets-first-smart-device

Foote, Keith. 2016. “A Brief History of the Internet of Things”. Dataversity. URL: https://www.dataversity.net/brief-history-internet-things/#

Foucault, Michel. 1988. “Technologies of the Self”. Michel Foucault, Info. URL: https://foucault.info/documents/foucault.technologiesOfSelf.en/

Fortinet. “What is IoT Security?”. URL: https://www.fortinet.com/resources/cyberglossary/iot-security.html

GDPR Today. 2019. “Privacy policies for Internet of Things devices must comply with GDPR”. URL: https://www.gdprtoday.org/privacy-policies-for-internet-of-things-devices-must-comply-with-gdpr/

Gurvey, Scott. 2015. “IoT and Intelligent Transportation. Cisco. URL: https://newsroom.cisco.com/feature-content?articleId=1601746

Lord, Nate. 2018. “What is the Data Protection Directive? The Predecessor to the GDPR”. Datainsider. URL: https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr

Majumdar, Nivedit. 2015. “Quantified Self meets the Internet of Things: Market Spotlight”. Emberify. URL: https://emberify.com/blog/quantified-self-meets-iot/

McCabe, Bill. 2016. “Short History of the Fourth Industrial Revolution”. LinkedIn. URL: https://www.linkedin.com/pulse/short-history-fourth-industrial-revolution-bill-mccabe/

Robertson, Jordan and Michael Riley. 2016. Bloomberg. URL:

https://www.bloomberg.com/news/articles/2016-08-25/in-an-unorthodox-move-hacking-firm-teams-up-with-short-sellers

Teicher, Jordan. 2018. “The little- known story of the first IoT device”. IBM. URL: https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/

NHO. “Hva er personvernforordningen (GDPR)”. URL: https://arbinn.nho.no/forretningsdrift/personvern/personopplysningsverktoy/personvernforordningen/

Illustrations

Blakes, Jon. 2017. “Securing Your Internet of Things (IOT)”. Hermish. URL: https://www.hermish.com/securing-internet-things-iot/

Babar, Sachin, Antonietta Stango, Neeli Prasad, Jaydip Sen, and Ramjee Prasad. (2011). “Proposed Embedded Security Framework for Internet of Things (IoT)”. 10.1109/WIRELESSVITAE.2011.5940923.

Rizvi, Syed, Andrew Kurtz, Joseph Pfeffer, and Mohammad Rizvi. 2018. “Securing the Internet of Things (IoT): A Security Taxonomy for IoT”. 163-168. 10.1109/TrustCom/BigDataSE.2018.00034.

Tseng, Henry. 2016. “Multipath Load Balancing Routing for Internet of Things”. Journal of Sensors. 2016. 1-8. 10.1155/2016/4250746.