Haaga-Helia

Privacy in the Internet of Things era

Damien Schorer

Bachelor's Thesis
Degree Programme in Business Information Technology
2016

Haaga-Helia

Abstract

Author Damien Schorer	Year of entry 2016
Title of report Privacy in the Internet of Things era	**Number of report pages and attachment pages** 51
Supervisors Olavi Korhonen, Nathalie Courtine	

The thesis has combined two topical areas of research. On one side, there is the Internet of Things. It is a growing market shifting to the consumer side with a range of products going from smart appliances to health tracking systems. On the other side, there is privacy, a highly mediatised subject especially after a number of revelations over the past few years on how governments may be spying on citizens.

The purpose of this research is to assess how personal information is going to be protected, or not, in this Internet of Things revolution. The goal of this thesis is to create an overview of the privacy landscape of the IoT and in order to do that the report focuses on the relevant policies of technology companies and their IoT working groups.

The research is subdivided into two different parts, one with a theoretical long-term approach and another more factual. The first aspect of the research is based on the multitude of groups, consortia and alliances that are working to facilitate the rise of the Internet of Things. These groups are creating frameworks and standards to help different smart devices to communicate with each other. The latter aspect of the research is based on the devices available for consumers and whether they are advanced in protecting data.

After an analysis of the official documentation of the different groups, the results of the research allow to define three categories of market players. The first category companies who are not mentioning privacy at all in their work. The second is the companies that are taking it into account and explain how they manage it but do not take exceptional measures to prevent data breach. Finally, the third group is composed of companies which are really taking privacy into accounts in their certification program, standard or products and services. The study reveals that even with security protocols and certification company products can still be hacked and that personal data is never entirely secured when digitalised and uploaded on the Internet.

Finally, this thesis ends with ideas for further development. As the Internet of Things is a rapidly moving trend, it could be noteworthy to follow how the standards and frameworks will evolve. The other aspect of the subject - the way privacy is - viewed is also changing rapidly and could modify, for the better or the worst, its online pendant.

Keywords
Internet of Things, Privacy Standard

Table of contents

Terms and Abbreviations

IoT	Internet of Things
M2M	Machine to Machine
IP	Internet Protocol
RFID	Radio Frequency Identification
IT	Information Technology
LAN	Local Area Network
HVAC	Heating, Ventilation and Air Conditioning
API	Application Programming Interface
IEEE	Institute of Electrical and Electronics Engineers
OIC	Open Interconnect Consortium
OCF	Open Connectivity Foundation
IIC	Industrial Internet Consortium
OTA	Online Trust Alliance
ITWG	IoT Trustworthy Working Group – Affiliated with the OTA
CSA	Cloud Security Alliance
WWN	Works with Nest

1 Introduction

20.8 billion connected things by 2020, 13.5 billion in the consumer market only (Gartner, 2015). A predicted spending of 3 trillion dollars in 2020, about the same spending level in overall IT right now. This is the latest estimation made by Gartner, an IT research and advisory company. It means that, statistically (GeoHive, 2012), in 2020 every human being will use about 3 connected things, regardless of the nature of the device. And this is not even the most optimistic estimation, Cisco and DHL estimated in a Trend Research that the number of connected IoT devices by 2020 to be around 50 billion (James Macaulay, 2015). In the book *The Internet of Things* written by Samuel Greengard he describes his current typical day, using no fewer than 8 different IoT devices, without counting his different iPhone's applications. This scenario, not a fictional one, is described by himself as "*a realistic snapshot of a typical day in my home, which hardly qualifies as a state-of-the-art lab for connected devices"*. (Greengard, 2015)

It seems that IoT is big and will be even bigger for the years to come. As with every evolution, or revolution, come new challenges, problems and even a sentiment of fear. Since Edward Snowden revelations in 2013 peoples tend to keep privacy in mind when taking new buying decisions. In a survey concerning IoT devices adoption made in November 2014 by Affinova, a marketing technology firm acquired by Nielsen the global information and measurement company, it was found that 53% of consumers expressed concerns about data sharing and a fear of being hacked (Affinnova, 2015). This was one of the leading obstacles to their adoption, right after the cost. Personal privacy is important but this is still the cost who leads in this survey.

We can also mention the different hacks who have been widely mentioned, even in the mainstream press. For example, the connected car hack, the security problems involving different brands of smart baby monitor, the smart health-care pump used to give medication to patients who were hacked or even the pacemaker hack who made it possible to compromise them at a distance of 10m and possibly kill their host.

There is a vital need for companies to reassure the consumer world that massive security breach is not the new trend coming along the Internet of Things because otherwise the adoption phase will be compromised and the revolution will not take place in our homes.

1.1 Goal of this Thesis project

So let us summarise: The IoT revolution has already begun and it is going to be gigantic in a few years. Then on the other side we have the consumers who seem to think a lot more about privacy than before and do not hesitate to express their concerns about it. Therefore, if we take these two parameters into consideration it seems normal than the different companies building this new era would have our personal information into consideration and protect them. This is the goal of this research project, to get an overview of the situation and assess whether or not privacy will be taken into account when this revolution rises.

1.1.1 Research Questions

This leads us to the different questions that need to be answered, at least partially, by this thesis. The order does not bear any importance here:

- Does the consortium/alliance have guidelines about privacy?
- Is there a universal standard in IoT regarding data protection?
- Regarding the IoT devices already available, how secure are they concerning our information?

The answer to these questions will then be used to create a privacy-orientated overview of the IoT revolution. It will help end-users to get an idea of how their information is managed in the devices and services of the Internet of Things.

1.2 Scope of This Thesis

This research work will stay in the boundaries of personal privacy and how it is managed in the Internet of Things era. Privacy is something that a lot of people take for given but in regards of the enormous data breach happening each year we can see that it is not always the case. The Scope of this thesis is focused on the Internet of Things because it is a new trend that may be an industrial revolution. Therefore, it will change everybody's life in a way or another and need to be thoroughly researched concerning our personal privacy. The scope is focused on the personal privacy, toward the consumer market, because it will be larger than the business-only share and therefore would have a bigger impact on our life if it happens to be plagued with privacy problems.

1.3 Out of Scope

This thesis is not about hardware matter but more about the thinking around our personal information and how they are managed in the Internet of Things. Therefore, I will not write about which kinds of sensors or detectors need to be used for a certain application. The different ways of transferring the data between the IoT devices and the Internet will not be part of the talk either, unless the transfer are unprotected and creates a threat for personal privacy. On the same subject, the different attacks patterns who does not compromise the personal privacy of the customers will not be discussed here.

Regarding the different framework available to help IoT products to communicate I will only look at them in a security way, privacy orientated. I will not try to classify whether a certain frequency or channel of communication is better than another, unless it could be a threat to our information.

2 Background theory

2.1 Introduction

The subject of this thesis can be divided into two separate entities and will be treated like this in the background theory part. First I will write about the Internet of Things and then about the privacy. The purpose of this background theory is to get a clear description of what is at stake and to learn more about the subject of the thesis. It is here to support the research work.

I decided to start with the Internet of Things because not everybody has an idea on what it is, how it works or even its purpose. This part will be divided into four subchapters. First, I will write about what is at the origins of the Internet of things. In this part the Internet, the cloud, mobility and even RFID will be discussed. The second part will be about the Industrial Internet and M2M (Machine-to-Machine) communication, another foundation for the IoT. The second to last part will focus more on the consumer devices and their range of applications. Last but not least, there will be a part about the risks and concerns raised by this new ultra-connected world.

Concerning the privacy, it is a topic that is entirely subjective. Each person will consider information about themselves differently. For some, a birthdate should be private but for others there is no point in that. I will write about how privacy is managed on the Internet that we know and another part will be about the existing laws regarding that subject.

2.2 The Origins of the Internet of Things

We are now on the verge of an enormous change in the Internet that we know. We are currently ascending on the technology adoption curve introduced in 1957 by Joe M. Bohlen, George M. Beal and Everett M. Rogers from the Iowa State University. This curve, similar to a bell curve, is describing how any new product or solution has a roughly predictable trajectory of adoption. Along this trajectory they defined groups of people. “Innovators” for the first to adopt, then comes the “early adopters” followed by the “masses” and finally we got the “laggards”. This model is still true in our decades; it just happens in weeks or months instead of years (Greengard, 2015, xii). We know it is an important change and it is getting real now more than ever but, the question there is how we got here.

I will not recall here the entire development of the computer and the Internet along but let us take a few steps back and look how the world has massively changed in the last decades.

Before the smartphones, cloud or even the Internet, data was stocked directly into the enormous computer that we all have seen pictures in black and white, filling an entire room. Later, it was available on our personal computer but still located directly into our hard drives. Then came the floppy drives. It was the only way of transferring data from one stand-alone computer to another, except for the few blessed who had access to a local area network (LAN). Looking at the first floppy drives now that we have 128Go micro-SD card, and even more, is a surreal experience. The firsts disk, in the late 1960s measured about 20 cm in diameter and only stocked around 80 kB of data, roughly 40 pages of plain text. Twenty years later they were reduced to 9 cm and stocked 2.4mB of data. Incredible for that time and still ridiculous for us (Greengard, 2015, 4-5).

In the 1990s the massive adoption of computer networks into organisation changed that. They were able to transfer their data internally or to partners. It was expensive, slow, difficult to parameters and set up but it existed and paved the road for the next evolution, the commercialisation of the Internet and the World Wide Web in 1995. Connection speeds were still slow; large pages would take a few minutes to load on the browser but it was a revolution. Samuel Greengard described this moment and what it means in its book “The Internet of Things”, 2015 as such:

> Like the first railroad tracks laid down during the Industrial Revolution, the framework for a wired and connected future suddenly existed. The inventors of the Internet – including Robert E. Kahn and Vint Cerf – envisioned a world where networks connected to other networks – thus creating an interconnected fabric of networked systems. They foresaw a world with smarter machines that would spawn remarkable capabilities and incredible transformation.

This was the first step for the Internet of Things, the Internet itself. As stated in the upper quote, we can see that its creators had foreseen what it would look like and how the network will be interconnected (Greengard, 2015, 5-9).

After this first key-stone, comes another component of the IoT, mobility. Right now we can see smartphones about everywhere but it is going to grow even more. In the last Mobility Report made by Ericsson it is stated that we have around 2.6 billion smartphones and the

forecast for 2020 will go all the way up to 6.1 billion, more than the double. 70% of the world's population will then use a smartphone (Ericsson, 2015).

Before this massive amount of different smartphones, whether they use Apple, Google or Microsoft OS, there was the rise of mobile (dumb) phones. Beginning from a fantasy that was only seen on comic strips, the idea of mobile communication picked up the mind of researchers at Bells Labs, Amos Joel Jr., W. Rae Young and D. H. Ring. Together they created the first mobile phone system. A way for callers to talk while moving and the technology behind who switched on which cell tower the device had to connect based on location. The fantasy was becoming a reality. A little while after that, in the summer of 1946, mobile phone communication was available in St. Louis, Missouri but it was not really convenient as the phones weighted more than 35 kg and an operator had to manually connect the calls. Decades passed, we are in 1973 and the first call made from a "modern" mobile phone is passed on the street of New York City. The weight has been then reduced to a kilo but the battery has only enough energy to provide 20 minutes of communications. The marketplace only began to growth in the early 80s with the launch of cellular service in Japan (1979), the different Scandinavian countries (1981) and the United States in 1983 (Greengard, 2015, 30-31).

Then there is the growth that we know. More and more mobile phones and more capabilities at each iteration. In 1993, IBM presented the Simon. It was the beginning of the digital smartphones era. A condensed of capabilities and mobility. It was a phone, a fax, a pager, a calendar, an address book, etc. All of this in the palm of your hand. Talking about it, the Palm Pilot will follow shortly in March 1997. You could store data on it and synchronise it via your computer and even add applications or, connect it to the Internet. Of course, the connection was still slow and not always in use as we intend today in our connected phones, but it was the beginning of a new competition between the different phones manufacturers. It all rose steeply when Apple introduced the iPhone. The chip supported both Wi-Fi and cellular connection, allowing users to connect to their own network as Wi-Fi was becoming more and more ubiquitous. The possibilities were immense and the introduction of the App Store allowed developers to introduce new features and capabilities that were just concepts in the mind of everyone (Greengard, 2015, 31-32).

At the same time the cloud allowed users to synchronise, save or exchange their documents, photos, videos and data of any kind more easily than ever. The business side was also evolving and it takes place mostly on the logistic side with the help of RFID (Radio Frequency Identification). For some companies it was a new way of boosting

efficiency in a factory and for others it was used to manage their supply chain. But RFID is more than a tool for optimising its profits or reduce diverse costs. It is the ability to connect anything and everything to the Internet by attaching a small tag or a chip on an object/device. Look at your credit card, there is probably a logo representing little waves. It is RFID enabled and therefore allow you to pay without contact. The race number wore by runners is also RFID enabled and the RFID reader at the end of the race measure the time precisely. You can even track your golf ball via a smartphone app, thanks to RFID (Greengard, 2015, 33).

This changes everything. You can tag about physical objects and transform it into a data point that can be read with a smartphone. It helps us, humans, to get a better analysis of their environment and gives us enough data to stop doing hypotheses and transform that into real insight. This mobility offers us a different way to identify, measure, analyse things that we could not previously. It also removes the time, money and troubleshooting needed when you have to wire every object you want to be connected. This alone does not represent the Internet of things. Samuel Greengard compare it in its book “The Internet of Things” to a highway:

> Just as a highway system requires more than roads and signs – an entire infrastructure of gasoline stations, cafés, motels, and other amenities must exist – the IoT requires systems, software, and tools for supporting everything. Without these components, it’s merely a disparate collection of technologies that achieve limited functionality.

One of these components or tools is the latest buzzword of the recent year: Big Data. The chips, sensors, mobiles, tablets and RFID tag are producing a huge amount of data for us to analyse. According to the latest Visual Networking Index of Cisco Systems the global mobile data traffic grew 74 percent in 2015.This growth made the mobile data traffic reach 3.7 Exabyte of data per month! If you want another comparison, the mobile data traffic has grown 4000 times over the past 10 years (Cisco Systems, Inc., 2016). Eric Schmidt, then CEO of Google and now chairman for Alphabet Inc. its parent company, stated in August 2010 that we create in about two days as much information as humanity did from the beginning of recorded history until 2003. Of course the growth of HD Video is responsible for a big part of the amount but it is nevertheless very impressive (Jordan, 2012, 304).

Simply put we have an enormous amount of data and we need a solution to manage it. Gartner, Inc. Has a well know explanation on what is big data and the so-called answer reside in the 3 V’s (Volume, Velocity and Variety), a concept that came from the analyst

Doug Laney in 2001. But in fact the 3 V's are only a third of this explanation according to Svetlana Sicular, a research director at Gartner. Let us talk about those V's first and the rest of the explanation later. The Volume is the big in Big Data, it is the simple measure of how much data you have in your data-set. The Velocity refers to the speed at which the data are generated, analysed and even the speed at which they change by themselves in accordance with other data or events in the data-sets. Finally, the variety is the largeness of data available and their different application, when used. Gartner make a point by differentiating data used to get insight and dark data that lies in the organisation but is not used by the companies. The second part of the definition concerns the application of Big Data. Not every problem is a big data problem, to know whether or not it is one you have to see it as a cost-effective and innovative form of data processing. It is not necessarily to bring inexpensive solutions. The last part concerns the goals of big data. Its purpose is to bring an enhanced insight to the companies and help the decision making progress. For it to be effective, you have to act upon the new understanding you have of your own organisation (Sicular, 2013).

The Internet, the cloud, mobility, RFID tags, Big Data, etc. These are the foundations of the Internet of Things and at its heart there is the Industrial Internet. We will see in the next chapter what it is and its relationship with M2M communication.

2.3 Industrial Internet and M2M Communication

The Industrial Internet is a term that refers to the infrastructure supporting the numerous connected machines and their data. It is broadly speaking the integration of sensors, software and communication systems into the machine to enable the Internet of Things. It is seen as the fourth Industrial Revolution by some actors. Following the mechanisation, the production lines with mass production, the digital revolution that came with electronics and computer. We finally arrived to this smart industry or smart manufacturing, the name tending to differ. The purpose is the same as in IoT, blurring and blending the digital and physical world in order to get more of it. It is currently focused on utility measurement (smart devices that records electric consumption), tracking and optimisation of about everything, from the production lines to the machines themselves (Greengard, 2015, 51-53).

The basic common factor between IoT and the Industrial Internet is the use of data and the value extracted from it. We have seen earlier that we, via our computers, tablets, phones or other connected devices are generating more data than ever. This is, of course, beneficial for the array of connected devices and algorithms that need to use them in

order to provide insight or value. From a connected bed in a hospital to your smart lamps at home both need data to function or provide a valuable feedback. This ability to transform data into a usable result via diverse algorithm is the ultimate goal of every connected device and is described by data scientists as “value of perfect information”. The weather forecasting industry is the perfect example. The data available is already highly detailed and correct enough to process but they need the right algorithm and enough computing power to use it and generate a theoretically 100% accurate forecast. The meteorological industry is not the only one interested in forecasting, it touches every industry. Who would not want to identify, analyse and understand an event before it happens? Whether it is to prevent a customer to switch banks or which product a person walking in a shop aisle will purchase, every industry can benefit from predictive analytics (Greengard, 2015, 54-55).

To arrive at this level of predictability the M2M vendors need to do more than just providing a sensor implementation. They need to provide tools to monitor reports or generate specific alert. The strategic value comes only from the analysis of the data that has been collected over the course of a long period of time. This allows the creation of date-time pattern that could not be seen without stepping back from a daily observation. This kind of monitoring could, for example, allow companies to pre-schedule reparation of machine parts based on their average usury and life-time (Cronin, 2010, 241).

We have seen the benefits that M2M could provide but what is it really. Machine-to-Machine communication is the smaller picture of the IoT, its kind of ancestor. The purpose of M2M is to turn a range of objects into intelligent resources. In order to do so chips and sensors are added to the objects and allow us to control them remotely while they gather insightful data. Then, the Machine-to-Machine communication takes place and all these smart assets can talk to each other and modify their behaviour accordingly without a human intervention. The range of applications is nearly without limits, from the automotive industry to health-care centre passing by logistics and transport, every industry can use M2M solutions (Vodafone Limited, 2015).

We know IoT and we know M2M but the line between them seems kind of blurry. What is really the difference between the IoT and M2M? Let us start with a similarity, they can both be remotely controlled. But the rest of the reasoning is different. M2M communication is traditionally relying of point-to-point communication between the machine, via a cellular or wired network inside a given company. On the other sides IoT is based on IP-solutions from the devices to cloud solutions or services (Polsonetti, 2014).

Another way to understand the difference between the two of them is to think wider. The famous Finnish architect Eliel Saarinen stated one day, “Always design a thing by considering it in the next larger context – a chair in a room, a room in a house, a house in an environment, an environment in a city plan.” What M. Saarinen meant was for us to zoom out and get the bigger picture of what we are trying to create. M2M is the depiction of isolated systems of sensors who generate data for themselves. IoT purpose is to join all of these disparate systems in order to create a bigger one which would allow a new application. Thus the following quote “If you consider M2M in the larger context, you get the IoT” (Cox, 2015).

2.4 Consumer Devices

For each evolution to be massive enough and become a revolution it needs to affect the masses, the people. M2M communication has been used by companies for sometime now but the revolution comes from its larger context, the IoT. The IoT came with a great number of devices available for the wide array consumer and not just companies or niche market for engineers. This is why it is now perceived as a revolution and, as seen before in the Gartner report concerning their prediction for 2020, the consumer share will be the biggest of the entire market (Gartner, 2015).

The obvious example regarding the rise of IoT and its smart device is the fitness tracker. Last December the department store John Lewis had sold four times as many trackers from the Fitbit brand compared to 2014. On Black Friday, the sales were even increased by a colossal 1200% (Siddique, 2015). Let us get back to where it comes from.

Not so long ago performance and route tracking was done with a pencil/paper combo. Then, a range of objects, not connected yet, appeared and offered to wealthy athletes a GPS on their wrist. Later, these objects gain the ability to sync your data via a cable or even using Bluetooth. It was a rough display of the possibilities of the Internet of Things. Now a new variety of fitness tracker is taking tracking to a whole new level. Fitbit, the largest fitness device vendor, has for example a range of products going from a simple connected pedometer for 60€ all the way to smart fitness watches for 250€. Their wristband can track steps, distance, elevation (floor climbed), calories burned, active minutes, sleep patterns and even recognise which sport you are practising. These devices provide direct insight via an OLED (Organic Light-Emitting Diode) readout and connect to smartphones or computer using Bluetooth LE (Low Energy) to transfer all the data and display it in charts and graph on the application or the website. The real power of these devices is to extend beyond the wristband and the official application. Their API are

integrated into the treadmill, bicycle and diverse fitness equipment so you can have a personalised experience even in a gym. Furthermore, you can associate a heart monitor (if not included in your watch) and even synchronise is with your preferred route tracking application. In addition to all of this, they also sell a connected weight that can recognise up to 8 people and synchronise their profiles to their respective connected devices. There is even the possibility to add your food intake and calculate the number of calories associated. The technical progress is obviously big but what is really impressive is not so much the measuring and tracking but more the ecosystem of services and applications that, together, can provide a fairly accurate depiction of someone's personal activity and health, including food intake and sleep (Greengard, 2015, 38-40).

Along the monitoring of their activity, customers can now access a wide range of machine who previously cost hundred or thousand euros. Whether it is a to calculate blood pressure or the amount of sugar in your blood, you can now do that at home and synchronise it easily with your smartphone. There is even dispensing systems that will ring an alarm on your phone to take your medications and automatically dispense the right dosage. These machines can even contact medical professionals if there is an issue. The future made of medical nanobots who transfer all our health information in continuous to our doctor is not that far. They could automatically assess any of our problem and prevent us a useless visit to the doctor (Greengard, 2015, 97-100).

The other revolution occurring with IoT is taking place in our homes. The connected home depicted into every sci-fi movie is not that far away any more. There are two main elements that make the connected home a good news for consumers all around the world: convenience and cost-reductions. Let us talk about the latter first because cost-reduction concerns not only your monthly energy bill but also the impact on the planet.

An interesting presentation "The Smart Thermostat, Using Occupancy Sensors to Save Energy in Homes" has been given at the Swiss Federal Institute of Technology Zürich regarding cost-reductions in the modern home. 70% of a typical Swiss home energy consumption is devoted to HVAC (Heating, Ventilation and Air Conditioning), no need to specify that is it a lot. There are a lot of points that could be improved like energy losses on the windows and better isolation but here the focus is on the thermostat. The reasoning behind the idea of the smart thermostat is simple: why keep heating a room when there is nobody in it. When we leave a room and even our home we do not change every thermostat manually. There is a programmable thermostat but you have to find your own pattern and input the hours on it. The smart thermostat is here to combine the programmable thermostat with the intelligence coming from the occupancy sensors. There

is a lot of discussion about the algorithm and when they do have to update the temperature not to waste energy or bring discomfort to the consumer but this is not the point. The researcher, Daniel Pauli, simulates its systems on 8 different homes on the month of July and January to test both Heating and AC algorithm. The results regarding cost-reductions are incredible it goes from a minimum of 25% to more than 47% for an estimated average energy saving of 38.22% (Pauli, 2011).

The previous example is remarkable but it is based on sensors and a programmable thermostat, not really a IoT solution. There is now a range existing IoT solutions who does not require any new sensors and programming tools. One of this solution is made by Nest, a company bought by Google in 2014. Nest is manufacturing smart thermostat who adapt themselves to different patterns. The principle is the same as before, it can automatically sense when you are away and switch to energy-saving mode. It calculates how quickly your home is heating and thus adapt when it needs to switch on or off. The temperature is then adapted to your life pattern and even the weather because it will pull the information from the Internet based on your location. You can control it remotely and there is even energy-saving tips personalised to your home on the application. Because it is connected to your HVAC systems, it also provides a reminder to change filter and alarms when it detects a problem with the furnace, for example. The company behind this smart thermostat has also created a label “Work with Nest” to provide a simpler place to IoT devices from other companies and enhanced their function altogether. In the U.S. where the HVAC is responsible for 44% of a household energy consumption Nest can provide 15-20% of energy reduction just with standard parameters (Nest, 2015).

Apart from improvement via smart thermostat, the IoT is bringing a lot of different devices in our homes. Smoke detectors, IP-Camera, connected lamps and even smart lock for garages and other doors. The IP-Camera can automatically activate when you leave your house and use a motion detector to alert you when there is something suspicious happening. It can even recognise different people and alert the authorities if someone not identified break into your house (Greengard, 2015). The smart lock, some of them are compatible with the label “Work with Nest”, allow you to use your smartphone as a digital key. Either with a Bluetooth detection or with a generated password. It can send you an SMS when it detects that your children are back home, lock itself after a period of time and even generate temporary code for your neighbours to water your plant (Yale, 2015).

The other home automation devices are located in the kitchen. Samsung and LG are leading the way here. The latter brought an entire kitchen set – oven, refrigerator and even a washing machine – that can be activated by the voice using natural language. It

means that you can simply tell your washing machine to start washing at 30°C and it begins. Where it really begins to be impressive is when it is linked with your door lock or your smart thermostat: it will then automatically wash your clothes when you leave the house and it will be ready to be ironed/folded when you come back, without even thinking about it. Of course, you can manage all of these smart machines remotely via your smartphone. For example, the inside of the refrigerator can be accessed at distance via an inside camera. Convenient if you are shopping for, say, a cake and you forgot how much eggs you have left. Apart from this inside view, the smart refrigerator can track aliment freshness – their expiration date – and plan meal accordingly to its content (Greengard, 2015, 95-96).

There are three more important areas where IoT will support the path of the consumer. Think about buying groceries, clothes or anything for that matter. It can roughly be separated into three different issues. First the transportation to the shop. The search for products in the aisle and finally paying. All of these steps are getting smart improvement from the Internet of Things. Whether it concerns security, cost-reductions, convenience or a more precise marketing, all of these areas will change drastically in the years to come.

Automobile is where the shift will be the biggest in the transportation industry. Automakers have been pushing for security in their car since the beginning of this industry. The security-belt, the airbag, the different assistance to manage to break and the steering, the cruise control, etc. All of these features are here to help cars to be more secure for their passengers and their environment. It is, kind of, working. According to a rapport from the European Commission, in the EU the road fatalities have been constantly decreasing since 2001, passing from 54,900 deaths to 25,900 in 2014 (European Commission, 2015). This trend is also visible in the U.S. but the decrease is slightly slower. All over the world, death from road accidents are responsible for over 1.2 million losses each year.

The problem is that even with all the new security included in our car, automakers cannot really change the inner source of road accidents: The human error. It is, according to Google, responsible for up to 94% of the accident in the U.S. To palliate to this problem, automakers have been trying to create autonomous or self-driving cars. Let us take Google as an example for two reasons. First, it is not a traditional automaker and secondly it is the most advanced and unusual prototype. The Google self-driving car project started at Google X, the research and development lab operated as a subsidiary of Alphabet Inc. the parent company of Google. They began working with Toyota Prius cars equipped with multiple sensors, among which a LIDAR – a contraction of light and radar – that allows the car to “see” its surroundings. Then in 2012 they added Lexus RX450h to

their test fleet. Both of these cars were only navigating on the freeway. They shifted to the city where everything was way more complex and created a prototype unveiled in December 2014. This prototype is not a car modified to be autonomous, it is engineered since the beginning to be self-driving. No steering wheels, no pedals. Since their beginning in 2009 their self-driving cars have travelled over 1.6 million kilometres autonomously. Their array of sensors can detect “objects as far as two football fields away in all directions, including pedestrians, cyclists and vehicles—or even fluttering plastic shopping bags and rogue birds.” (Google Self-Driving Car Project, 2015).

This project is not currently working with IoT. The cars are retrieving the data, making decisions and acting by themselves, without being connected to one another. But this is the future of tomorrow. Cars will talk to each other in order to get a better global visualisation of the road conditions and adapt their comportment and path accordingly.

Shopping is also an area that is changing slightly. Thanks in part to the Internet, you don’t have to search for a car retailer in phone directories. You can research and buy what you need at the click of a button without moving from your desk chair. It exists applications for your phone that will use your camera to snap a picture of the bar code on any product and research where it is the cheapest. Retail vendors had to adapt to these new digital trends. They now propose digital loyalty cards stocked on your phone and QR (Quick Response) code in their magazines and shelf to get more information on a given product. But the real revolutions come from RFID tags and Apple iBeacon’s solution. It is an indoor positioning system that use Bluetooth LE. It can locate you in a store and push information on your phone according to what you are looking for. Say you are wandering in the aisle not knowing what to buy for tonight’s dinner, this technology can push a reduction coupon for pasta if you buy it right now. The same technology can be used to remind you of your buying list when you are passing by what you need. In addition to all these benefits for the clients, the owners get some too. They can precisely know how much time you spend in which aisle and could even modify the price in real-time in order to make you buy a product (Greengard, 2015, 105-110).

Payment is the last but not least area of our example where our habits are already changing. Contactless payment is beginning to be a routine in a lot of shops around the globe. You just wave your compatible credit/debit card in front of the payment machine and, under certain amount restrictions, your payment is made in a few seconds. Then Apple Pay and Android Pay appeared, they allow you to wave your smartphone, or Apple Watch, in front of the NFC reader instead of your card. Along this update in convenience, they generate a new unique and secure number for your card so the store will not see

your credit card number passing through their machines. Following this trend, Visa Inc. announced in February at the Mobile World Congress in Barcelona (Business Wire, 2016) that they are expanding their Visa Ready Program to the Internet of Things. The Visa Ready Program is a way for companies to integrate secure payment, in coordination with Visa, in their different products and services using a tokenization system, the digital identifier that replaces your card number. The firsts IoT orientated companies to join this program will bring mobile payment to wearable and even automotive. Just imagine stopping at a gas station, putting the gas your car and that is it. When you leave the station the amount is automatically debited from your account seamlessly. This high level of connected devices will allow us to pay with about every device that we own. Whether paying a drink after your morning run via your connected wristband or even paying all your groceries just by passing the door to the outside of the supermarket (Visa Inc., 2016).

2.5 Risks, Concerns and Repercussions

As stated before, every change in the history of technology comes with a lot of enthusiasm, optimism and nearly utopian thought but it is also filled with fear as with everything that in unknown to us. Every change bears its positive and negative but there is also, especially in new technologies, a whole lot of unintended changes that can occur. You can never know precisely how your technology will interact with the existing ones or the social system. The IoT is the exact representation of that phenomenon. Hardly anybody will discuss the benefits that it can provide: better automation, reduction in costs, greater convenience, etc. But all of these benefits can be transformed into negative points rapidly and transform our utopia into a dystopia (Greengard, 2015, 135-137).

In nearly every dystopia, the government try to remove the access to the knowledge by burning books. But what if we do not own physical books any more and use an e-reader? Amazon, one of the biggest online retailer, has made an ironically great example of that case with their Kindle. It is an electronic reader that can synchronise thousands of books from the amazon book online shop and you can download them from your amazon account directly on your reader. In July of 2009 they remotely deleted books (among which “1984” by George Orwell who depicts a dystopian future in which, among other things, books are burned) that were sold, on their own platform, by a company who did not have the right to (Stone, 2009).

One of the most common problems of the IoT is derived from its core purpose. The goal of the IoT is to manage everything as a whole. Imagine a city where every circulation light, pedestrian and cycle included, are functioning as a whole and can modify their own

comportment according to the other and a lot of other factors (weather, time, vacations, etc.). This smart city transportation system seems highly convenient but now imagine if it gets hacked, or simply shut down for a time. It is not an isolated crossroads who will be defective but an entire city. The smaller repetitive problems may be transformed in less occurring but bigger tragedy. In June 2009, a subway accident happened in Washington D.C, two subway trains crashed in each other killing 9 peoples. It was due to a computer error in the routing program and the fact that the operators did not brake manually quickly enough. Theses human's errors are referred as the "automation paradox". The more automated system is, the more a human using it will slowly "switch off" and relay on it without even thinking. There are plenty of illustrations of it, for example it happened to some drivers to get lost by a hundred kilometres by blindly following an old GPS, an error that could have been avoided by looking up just sometimes (Greengard, 2015, 138-139).

Another obstacle, but not for long any more, to the rise of IoT is their complexity. Horrible user-interface, strange operating controls and multiple failures are filling much of the existing smart devices. Home automation, whether IoT or not, has been available for the consumer for nearly 25 years. But the connected home of our dream is not that easy to achieve. The task is, or at least was, daunting for a lot of non-expert home-owner. This is slowly beginning to change, most of the newly available devices are nearly plug and play and the numerous associations between the product manufacturer allow, sometimes, your different devices to communicate and benefit from each other. In the near future, connected devices should be as easy to use as the power switch they want to replace. You just connect the power cable and that is it (Greengard, 2015, 142-143).

Not having to parameters a new connected device will be extremely convenient but it raises then another question about the effect of technology on our intelligence. Nobody is memorising contact numbers any more, you just add them onto your phone. It is the same with the GPS and a good old-fashioned map, less and less people know how to read it. As a final example let us use the fitness tracker again, we have more and more ways to control everything fitness-related but obesity and lifestyle-disease is still a continuing problem. The more devices are doing for us the less we are connected with our environment and surroundings. The psychologist Douglas Lisle coined that term "pleasure trap". Our brain is designed to usually adopt the simplest and most pleasing way of doing things, even if it is not the best. The debate on whether technology will enhance or reduce human intelligence is still on is way, and probably will be for long, but one thing for sure. Our brain will adapt itself to our use of technology (Greengard, 2015, 147-148).

Among the benefits IoT will bring there is also a question of who will profit from them. With the advance of the Internet in the 1990s a digital gap emerged and reinforced economic and social inequality. The point is pretty basic, those who have access to more information, data and thus knowledge are more eager to benefit. The problem is in the repercussion that is engendered from it: lack of opportunity in school and work, just to cite the most important. With the Internet of Things, the gap could get even wider. Of course, connected lighting and smart watches will not really dig the gap but there are other areas which could lead to leave non-connected people far behind. They would have to work way more to earn a decent salary or could even miss basic tools in their everyday life. In its book “The Internet of Things”, Samuel Greengard describes it as “the digital equivalent of farming with a hoe compared to a combine”. There are also other consequences, particularly in the health-care sector. With the help of sensors in the body or simply wearable devices, doctors can detect issues and diseases within the body at early stages and take actions to prevent them. The peoples who are not connected and the countries where it is not available will not be able to profit from it even if their own life may be at stake, without them knowing it (Greengard, 2015, 148-149).

Another fear that has been present constantly with every new technology is the anxiety of job losses. It happened in the beginning of the industrial age and then again with the digital revolution. Normally these jobs are just moving from sector to sector, usually leaving the first one to go into services. But according to the Associated Press, this trend is slightly changing. The jobs are not redistributed between the sectors or lost to a more profitable market (say China or India), they are given to machines. At first it was in the manufacturing that technology reduced most of the jobs, now it is beginning to eat into the service sectors, responsible for 2/3 of the workforce in the developed countries. Workers who are doing repetitive tasks are the most at risk because developers could write a program to replace human involvement into such tasks. The recession forced companies to be more efficient and replaces middle-class jobs with machines. Now they will not come back from this new level of efficiency. New jobs are still created but not middle-class one, they are more supervisor/manager type of jobs. The core problem with these cuts in jobs is that they vanish and are not moved into another country. Joseph Stiglitz, a Nobel Prize-winning economist who studied at Colombia University put it like that “It doesn't have political appeal to say the reason we have a problem is we're so successful in technology. There’s no enemy there.” And the fact that everyone is directly or not contributing to this is not really reassuring. Of course not everybody writes software to replace someone but we all got a part in this. Using a self-checkout lane, that was a cashier job. Buying things online, used to be with the help of a salesman. Booking flight tickets and hotels online,

reducing the number of travel agents. The number of examples is enormous but the bottom-fact stays the same: technology is reducing the number of jobs because the pace at which it moves makes it very hard for humans to adapt (Bernard Condon, 2013).

The last and maybe the most mediatised risk is the cyberterrorism. Fraud, cyber-espionage, data breaches and more have made the headline for the past few years. These issues can be devastating is they happen in highly sensitive companies. For example, in June 2010, the computer worm Stuxnet was discovered in a set of controls used, inter alia, at a nuclear plant, electrical power grid and oil pipelines in Iraq. The threat was destroyed but it had infected more than 30'000 machines before being taken care of. There was even suspicion that this malware was designed by a government agency. When hackers do not use a virus or worm to threat our life they use the rest of the technology as a support to bypass the law. A group of researchers have produced a functional firearm with the help of a 3D printer. You could virtually pass any metal detectors with a plastic gun in your pocket and commit a crime in a supposedly controlled environment. Guns are just the beginning of 3D printed weapons, you could also print a homemade grenade or even weapon launcher. Drones are also something now widely available that could help terrorists to reach their goals: spying celebrities, dropping chemicals or bombs, delivering drugs payload, etc. Marc Goodman, head of the Future Crimes Institute and a former police officer think that the emerging technology could "bring about great change for our world. But in the hands of suicide bombers the future can look quite different. (…) We constantly underestimate what criminals and terrorist can do. (…) Every time a new technology is introduced criminals are there to exploit it." (Greengard, 2015, 160-162).

The future is not a dystopian world where technology threat us at every instant but government, companies, researchers and schools needs to be conscious or the risks. A rethink of security, law, social interactions and consumption needs to be done in order to embrace the benefits of the IoT and not stay blocked in the face of fear (Greengard, 2015, 165).

Privacy

Privacy is a fundamental human right. It has been recognised in the Universal Declaration of Human Rights at its creation in 1948 by the United Nations. The article 12 is explicitly about the right to have your personal privacy and use the law to defend it, if necessary. The articles 18-20 are also connected to privacy because they defend the freedom of

opinion, religion, thought, peaceful assembly, etc. Everyone should be able to do that and do not have to report it to anyone (United Nations, 1948).

Now we got that privacy is not just a term used a lot in recent years but a fundamental right that ought to be protected so let us see what it means. According to the Oxford Dictionary of English, privacy is “a state in which one is not observed or disturbed by other people”. It is also “the state of being free from public attention” (Oxford University Press, 2013). Being free from public attention sounds like a difficult plan to execute when the purpose of being online is to be connected to one another.

At the finalisation of the UDHR (Universal Declaration of Human Rights) and the definition of privacy by the OED (Oxford English Dictionary) we had the right to be protected offline, simply because our online status did not exist then. In a resolution adopted in December 2013 by the United Nations General Assembly they recognised, “The right to privacy in the digital age”. They noted that the rapid rise of new technology allowed individuals to gather new information and ways of communications but it also enhanced government capabilities in surveillance, data collection or even interception. All of these which may violate the Article 12. The General Assembly noted that, in some cases, concerns about public security may justify the gathering of certain information, but it still needs to be within the international human rights law. This is the part that has been added following this resolution. “The General Assembly (…) Affirms that the same rights that people have offline must also be protected online, including the right to privacy.” (General Assembly, 2013).

The main problem with privacy is that it is a subjective matter. There is no Manichean stand on whether an information should be public or private, good or bad, acceptable or not, etc. It should be discussed every time and take people’s experiences, values, choices, etc., into consideration. The purpose is not to stop totally the information’s flow but to ask yourself if the information is handled in a way that you consent to (Jordan, 2012, 322). This is when the marketing department of companies are trying their best to get the most of your consent. In order to do so they use a simple trick, added value in exchange of information.

The biggest criticism of companies using a lot of our personal information is the “creep factor”. It is a term that describes the way brand have a very intimate knowledge of you and can follow you or your thought via your online activity. One recent incident involving Uber, the sort-of cab service, illustrates that very well. A reporter had an interview with one of Uber’s executive at one of Uber’s office. As soon as the journalist walked into the

building, the executive was coming down the stairs as if he knew the exact moment she would arrive. In fact, as he himself told her, he really knew. He was following her movement using a version of Uber called God View that allow to track every Uber car. The same technology that is used to track your phone and send you a car as fast as possible was used to track a journalist. Everyone using Uber can agree that sharing your location is useful for the car to find you but using it for tracking people is quite strange and may be something to fear (Nesamoney, 2015, 169).

The example of invasion of personal privacy does not stop at Uber. Another famous example happened in 2012 with the retailer Target. It all began when Andrew Pole, a statistician at Target since 2002 created, upon the request of the marketing team, a pregnancy prediction model. A tool that uses recent purchases, age, city of shopping and a lot of other statistics in order to predict if a woman is pregnant or not. New parents are the holy grail of every retailer because they usually buy everything they need at the same place instead of changing store for groceries, toys, appliances, etc. The prediction tool worked quite well and did a blow in the public relationship of Target. One day in a Target of Minneapolis, MN an angry man asked to see the manager. He came with coupons that his daughter received in the mail, coupons for baby clothes and crib. The manager was astonished and apologise to the dad. Days later when he called the man to apologise again the father was a bit ashamed. He told the manager that in fact his daughter was really pregnant and Target knew even before himself (Duhigg, 2012, 30).

This is one of the grey areas of personal advertising. There are a lot of times where we accept to share personal information in exchange for a personalised service. Whether it is your personal location for Uber or your sleep pattern, calorie intake, steps when you use your fitness tracker the heart of the reflexion is the same. We accept to give some of our information when we think it is a “fair trade” for a more rewarding experience of a service. The same information can be seen differently regarding the usage that is made of it. If Uber was selling your location to other people it would, probably, not be a “fair trade” any more to share your location with the app (Nesamoney, 2015, 170).

It is quite fair to say that until recently, about a decade, peoples were not really concerned about their online privacy. It is not that they do not have an idea or stance on the subject but this is not something that people tended to think about. Now this is something that is changing rapidly. The revelation from Edward Snowden, a former analyst at the CIA, about the way security services from the government are accessing all of our personal data easily seemed to force people to really think about it. Media across the globe are now talking about this topic and peoples are getting interested in it (Strong, 2015, 150).

This trend can be observed into a lot of different polls. A 2013 study by Unisyss based on American citizens showed that 83% have high concern about identity theft. Another study, also conducted in 2013 by the ISACA (Information Systems Audit and Control Association), found that 92% of the person surveyed are concerned about IoT devices and 90% fear that their online data may be stolen. These are not small problems concerning a third of the population, this is a real fear that nearly everybody can relate to (Greengard, 2015, 155).

These statistics take us to the newly discovered “privacy paradox”, particularly among teens. They are frightened by the nearly endless possibilities of the government agencies and do not hesitate to protest against it and on the other side they use social without restrictions and seems not to care about their online privacy. There has been a lot of harassment and blackmailing in the recent year over personal pictures or videos posted online. Teens not taking care of their privacy may indicate a change in the entire future society. Mark Zuckerberg, Facebook CEO, has even claimed that privacy was no longer a social norm in order to justify changes in the social network privacy settings (Strong, 2015, 181-182).

The stake of your own privacy is also highly influenced by economic factors. We have seen before that people are willing to give away some of their information in exchange of added value in the service. Researchers from Carnegie Mellon University and Harvard Business School decided to find what is privacy worth. Their research was based on offers given to shoppers in Pittsburgh, PA and their relation to privacy and personal data. They gave a 10$ discount to some shoppers and offered them 2$ more if they revealed the content of their shopping cart. In this case, around half of the people took the 2$ and the other half refused it. The other shoppers received a 12$ discount and could exchange it with a 10$ discount if they wanted to keep their purchases private. This time 90% of the shoppers kept the 12$. This trend, called endowment effect, occurs when people place a greater price on things they own than identical things they do not. This research showed that privacy is as influenced by this effect as any other valuable objects or services (Alessandro Acquisti, 2013).

What we can take from this study is that privacy is an asset like all the goods and services that we possess. Some people are estimating it at a high price, others do not. But it is still viewed as something tradable when we got a great, or not that great, offer.

3 Research Plan and Method Choice

The research work of this thesis can be split into two parts, the first one being the biggest part of the work. First, I will dive into the world of the Internet of Things standard, consortium, alliance, etc., in order to assess whether or not privacy is mentioned in their guidelines and rules. This part will not only stop at the global alliance movement but also focus the different certification of compatibility offered by IoT companies (for example “Works with Nest”). This overview of all the IoT groups will allow us to get a better picture of the privacy and try to understand what are the consequences for the end user. In order to find information about this, I will use the official website of each group and have a look at their documentation and supports thread. Privacy is a good selling point so if it exists they must have written it clearly to attract more people.

Then the research focus will point on the already existing IoT devices to see if the best practices have been taken into account in the things itself and the ecosystem that comes with it. In this part I will see if information protection is part of the product and at which degree of advancement. I will take two real-life cases hack from two big IoT manufacturers that happened in the recent years and explain the story behind it from each point of view. This part alone may be biased because negative feedback is more often seen than neutral or positive one. This is why it is only a part of the research work and should not be taken as the best possible depiction if read alone. But I still think that it is interesting to see and compare what is described in the privacy policy and security guidelines and what really happens when the products are in the hands of everyone.

Overall this approach will allow us to have the best possible overview of the relationship between IoT and privacy. We have the theory in the groups of companies, how they want to manage the privacy and how they communicate on it. Then the practice with the existing smart devices, their possible hacks and vulnerabilities.

I choose to associate these different phases because it is, in my opinion, much more suitable to get a complete picture. I could have just picked different smart devices and test them but I think that this is not fair and we must objectively look at the alliance and consortium guidelines and not just judge IoT devices separately. I prefer this theoretical approach because we are not judging a final product but a growing ecosystem. It means that some already available product should not be assessed as representative of the IoT era but instead the focus should be aimed at future ones and what directions the companies are pushing for it.

There is also another method that I could have used but I choose not to because I think it would be biased if used alone. I could have only checked media articles about IoT and privacy and see what subject was in the most articles. This method would have given us a great media perspective but maybe a bit too different from a real one. The reason is quite simple; media are writing on this linked subject only when there is a problem. Smart devices X has been hacked by researchers at Z, the information of every customer of company B has been stolen, etc. It is a normal way to treat the subject in the media but for a thesis it is not a suitable one if used alone.

4 Research Work

4.1 Alliance, Consortium and Other Groups

4.1.1 Introduction

This part of the research work is focused on the grouping of different company under a same name to represent a way of thinking in the IoT field. There is, to put it bluntly, way too much of them. Where the Internet that we know is unified under a single set of standard that allow everyone around the world to see the same content and even create new one, the Internet of Things is not at this point and is stuck with different groups representing different standards. There are even companies who are backing more than one group, maybe to know for sure that they will be on the winning side at the end.

In this part I will check the documentation available online of the main groups and focus on the privacy side. The goal here is to find out if these groups are talking about privacy or not and at which degree do they talk about it. Another comparable program with these groups is the label that use the “Works with X” semantics. I will have a look at them to see whether the same privacy protection guidelines are respected or if it is simply to display a hardware and/or software compatibility.

Just a little disclosure there. I will research and judge the different groups with their available documentation online, from their official company website. It may happen that some groups are not giving this documentation to “customers” but reserved them for the companies that are signing the agreement. If it happens to be the case, it is an unfortunate choice for the end consumer because they deserve to know what happens to their data and how it is managed.

The following groups, alliances and other consortium below are not classified by any importance order. I just tried to retain the main groups (backed by well-known companies). Concerning the labels, I choose the best known and most used system to try to get a more real picture.

4.1.2 Open Connectivity Foundation

The OCF, known as the Open Interconnect Consortium until 19/02/16 and created in July 2014, is an IoT industry group. It was created by prestigious names as Intel, Broadcom and Samsung as principal sponsors. Broadcom left the consortium but there are still plenty of other so-called Diamond Members: Cisco, Electrolux, Qualcomm and even

Microsoft. They also have Platinum members among which IBM and Dell. So this group is pretty big and represent an enormous market share in the electronic world if you combine its participant. The Open Connectivity Foundation stated mission is to create a new specification and sponsoring an open source project (IoTivity Project) in order to allow communications between the billions connected devices existing and to come. To do that they provide a communication framework easy to use for everyone that allows interoperability between devices. This common platform will be provided by the OCF to discover, address and message the different devices, all of this with a security layer.

They will also propose to certificate products to ensure the end user that he/she is buying a compatible product but this is a feature still in development and therefore non-accessible on their website.

Their way of describing the security layer in their solution is “Basic security for network, access control based on resources, key management etc.”. In a bit more detail they provide a secure resource manager layer that encrypts the messages end-to-end, transfer ownership of the new added object, manage the access control list and finally allow to use symmetric and asymmetric credentials to establish secure link. Their specification goes more into the details of the different security implementations but there is nothing concerning the privacy for their users.

4.1.3 Thread Group

The Thread group is the non-profit organisation that represent Thread, their network protocol and certification system for all Thread product. It was also created in July 2014 and has a lot of big names in it as well. For example, ARM, Qualcomm, Samsung, Microsoft and Nest (Owned by Google) are just a few of them. As you can see some of them are even present in more than this Thread Group. This is a bit morally unusual when the Thread Group goal is “to create the best way to connect & control products in the home”, something that sound about the same as the OCF.

The resemblance does not stop here. Their network protocol, Thread, is made to solve different problems usually associated with the IoT world: reliability, security, power and compatibility issues. They want to connect our devices “Once & for all”. Let us have a look at their what security means for them.

The Thread network protocol bases its work on proven standard such as IPv6 and more particularly 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) with

mesh communication. This is a pretty similar solution also used, for example, by ZigBee another communication protocol made for the Internet of Things era.

Thread is functioning with an IPv6 addressing of all the devices in the mesh network. It allows for an end-to-end IP Security because the inner network uses the same security as the Internet and the border router does not have to adapt it when it is passing through it. In terms of security they are using “smartphone-era authentication scheme”, based on recommendations from the NIST (National Institute of Standards and Technology). Concerning the encryption, they use AES-256 public-key, the most secure key-length of AES (Advanced Encryption Standard).

Thread is not shy on the security side, they published a white paper on this subject where they document all their effort to bring maximum security and convenience into their network protocols, but there is not a word on privacy. They describe how they intend to protect the transport, application and network layers but do not talk at all about the storage of the data for example (Thread Group, 2015).

4.1.4 AllSeen Alliance

The AllSeen Alliance is another group who wants to simplify the way the Internet of Things and more precisely device connections work. This alliance was created in December 2013 and is based on the AllJoyn framework originally made by the processor manufacturer Qualcomm. As with the past two consortia that we have seen, the AllSeen Alliance also has a lot of impressive members. Their list of premier members includes, along with Qualcomm, of course, Canon, Electrolux, Microsoft, Sony, LG, and others.

The AllSeen Alliance is managing the AllJoyn framework, on the one hand, and also provides a certification program. This certification program allows products which pass a series of tests to benefits from compatibility with all the other AllJoyn Certified products and the right to use the AllJoyn Certified mark to boost their branding. There is currently (on the 27/03/16) 24 products that are certified. Their type range from lighting to audio, smart controls and even tablets.

The AllJoyn framework is an open platform composed of a set of different services framework which work together. It includes discovery, connection management, messaging between the devices and security. Concerning security, the FAQ on the AllSeen Alliance website indicates that the AllJoyn is designing security only for the encryption and authentication of the application level. The certified objects can implement

both secure and non-secure interface depending on the needs and the requirements of their product/service.

In a presentation made at the Linux Collaboration Summit in February 2015, Art Lancaster, CTO of Affinegy and member of the AllSeen Alliance talked about how the Gateway Agent of AllJoyn was good both for security and privacy. The Gateway Agent is what separates the local network of devices from the Internet. AllJoyn use it to filter the traffic and only allow remote controls or access to the user's cloud service. This means that the rest of all the communications stay in the LAN and therefore minimise the amount of personal data that transit on the Internet. When there is the need for the user to access from the outside he/she can configure exactly what data needs to be routed eternally, a process that enhance security and privacy (Lancaster, 2015).

4.1.5 Internet of Things Consortium

The Internet of Things Consortium is another non-profit organisation dedicated to help the Internet of things. Its goal is to accelerate the rise of the IoT and particularly focus on the usability, security and interoperability. The members list is a bit less prestigious than the other groups but still got big companies like Nestlé, Fox, Logitech and even Smart Things (an open platform for smart home bought by Samsung).

This Consortium also differs from the others because it is not based on a framework, a service solutions or even a certification program. It is more defined as a canvas which gives opportunities for companies to meet, exchange and participate in working groups with others leading IoT companies. Their website lacks of official documentation on the rest of their work and they do not seem to particularly promote or impede privacy.

4.1.6 Industrial Internet Consortium

The IIC was founded as an open group in March 2014 by AT&T, Cisco, GE, IBM and Intel, quite big name for the industry. Their organisation does not focus on the IoT for consumers. Their goal is "to accelerate the development, adoption, and wide-spread use of interconnected machines and devices, intelligent analytics, and people at work". In order to do that they focus solely on industries like energy, healthcare, transportation, etc. (Industrial Internet Consortium, 2016). Even if the focus of this work is on the consumer side of the IoT I think that it is interesting for us to have a look at what is being done on the industrial side, hence this part on the Industrial Internet Consortium.

The IIC does not support a specific service or technology but instead is open to any idea that could help them achieve their goal. Their only desire is to have an open standard and help it develop in the best possible way. In order to do that they provide a framework, use-case and test beds that can be used for real-world applications in a variety of industries.

They are splitting the task in different working groups. Theses working groups are created when there is a great interest in a certain aspect of the task. Currently there are 19 different working groups, they work is separated into broader categories like Legal, Marketing, Security, Technology, Testbeds, etc. I will focus my research on the Security categories to see if anything regarding privacy appears.

The total documentation is, of course, only available to the member of the IIC but they also wrote some documents explaining their approach of the security. They acknowledge that security threats are becoming very important in the Industrial Internet field and that privacy is also a shining point on it. They project to work on five characteristics regarding their framework for the business process, industry norms and regulatory compliance: safety, reliability, resilience, privacy and, of course, security. Another task of the Security Working Group is to provide guidance and counsel regarding security and privacy to the test beds that are created by another Working Group. According to their website, they will release their Security Framework to the public in the coming months.

IEEE – Internet of Things

The Institute of Electrical and Electronics Engineers was originally formed as an association of technical professionals. It is now not only reserved to engineers but professional from all fields of technology and science. One of the biggest parts of the IEEE is the Standards Associations which, as stated in its name, create standards. The IEEE is widely known for their computer networking standards as Ethernet (IEEE 802.3) and wireless communication (IEEE 802.11 and 802.16).

The Internet of Things is such a big revolution that the so-called I triple E has created an IoT Initiative in 2014. The mission of this initiative is to gather technical companies and create a community platform where the professionals can exchange their ideas and collaborate on the subject of the Internet of Things. Along this exchange place, the IEEE IoT Initiative also provides a set of different use-case, service descriptions, business models and reference implementation for a real-life scenario.

Another part of this initiative is to create and define a standard for the IoT. This draught of a global standard for every IoT device is currently name P2413. The purpose here is not to replace the IoT groups that are already existing but rather to create an architecture standard that all companies and manufacturers could use. In this project there are also big vendors like Cisco, Huawei, Toshiba, Intel, Qualcomm just to cite a few of them. This standard will also provide a blueprint regarding data abstraction based on four qualities: protection, security, privacy and safety.

The IEEE group understand that privacy may be a problem in the Internet of Things, they even write an article about it on their magazine The Institute. This article named “The Value of Privacy”. In this piece, one of IEEE senior member Raul Colcher explains that the privacy that we know and the meaning we make of it will need to be redefined entirely. That there will be a new scenario that we never even thought of and we will have to address them. “The inclusion of the IoT all around us is inevitable,” Colcher says. “The only thing to do now is to prepare the best we can.” (Rozenfeld, 2014)

Their interest in privacy and security does not stop there. The IEEE Initiative also published in the 2015 summer a case study on connected Garage door openers. They primarily focused on security but also took account of the privacy issues that could happen. One of their founding was that the company asked for their home address, a very personal information which, coupled with the fact that they work with cloud services, can be a very serious security issue.

In another of their more generic study they focused on the privacy problems which accurate location systems could cause. Given the fact that we can be more and more precise and also that the amount of time our locations is shared by our devices is getting bigger. They also wrote about the privacy issues of clear-text information transfers whether it is user identifiers or even connected lighting devices names. Their article also makes the point that standards bodies and experts have to take privacy into account and create minimum requirements when creating standards. We will see if they took their own advice when the standards P2431 will be finished.

4.1.7 Cloud Security Alliance – IoT Working Group

The CSA is an organisation with a focus wider than just on the IoT. It is here to define and raise attention on the best practice to have a highly secured cloud environment. Their member list is, as always with this kind of group, very impressive. They can count on Microsoft, SAP, Hewlett Packard, Cisco, Google and many more. If you think about an

actor in the technology field, it is probably in the Cloud Security Alliance. They also deliver certification for different services and also for users.

What really interests us in the CSA is their IoT Working Group. It is focused on IoT and its relation to the cloud. The Cloud Security Alliance create working groups to work on different subjects separately because every subject does not require the same amount of time, member or even investment. Whether it concerns identifying threats, defining controls, creating best practices or even privacy management, the IoT Working Group is working on it.

This group published two different papers on the subject, the one that is the more developed is on the security guidance for early adopters of IoT solutions. In the report they identify privacy as a main concern regarding the IoT Security. They particularly point the fact that they could be data-capture from sensors users are not even aware of. This raise questions concerning consent and what recourse you can have when you a company or an organisation has been gathering information without you knowing it. Another concern for them is the same has seen in other groups: the aggregation of information from different sensors and devices in a single point that can be highly vulnerable. They want company to perform privacy impact assessment whenever they are creating IoT devices to see how our privacy may be affected by their actions. This point is also backed by the European data protection advisory body in the EU and the Federal Trade Commission in North America. This paper also raises the challenge involved in order to regulate all of these issues and give possible solutions or recommendations (Cloud Security Alliance - IoT Working Group, 2015).

4.1.8 Online Trust Alliance - IoT Initiative

The Online Trust Alliance is a charity group of industry workers created in 2005. Their mission is to enhance trust, innovation and market vitality on the Internet. Created to reduce the amount of spam in our electronic mail box the OTA is now a well-renowned group with more than a hundred members and is affiliated with the All Seen Alliance among other groups. Their members list contains names like Symantec, Microsoft, Epsilon and even Twitter.

Their focus on privacy is very important and it is one of the main initiatives on which they are working on. They also created the Protection and Privacy Day to celebrate the first data privacy directive signed on the 28th of January 1981. This day includes a lot of different events centred on data protection and best practices regarding privacy.

One of their other initiatives is on the Internet of Things. They created the IoT Trustworthy Working Group (ITWG). This is a working group with a focus on security, privacy and sustainability. It was created in the early 2015 to accompany the rise of IoT devices adoption. After about a year of work, they released their IoT Trust framework on the March 15, 2016. It contains 30 principles and their recommendations are separated into two different categories for now: connected homes and wearable technology, limited to health & fitness technologies. For each and everyone of their 30 principles they either require or recommend applying the principle, depending on its category and level of security needed. This is a definitive version that will serve, in the future, has a base for an OTA certification.

The list of principles is separated into different categories: Security, User access & Credentials and finally Privacy, Disclosures & Transparency with nearly half of the principles in the latest category, the one that interest us the most. In this category there is advice on nearly everything you could think of. It starts with how users are supposed to access privacy policy in the easiest and clearest possible way. Advice includes, prominent placement on the website, QR codes, short-URL, etc. Then the majority of points are about disclosure from the company regarding the security patch, data collection, sensitive data handling, data anonymization, etc. The framework also protects the resell or transfer to other companies of our data without the user content (ITWG, 2016).

Along their IoT Trust framework, the ITWG is also creating (it is still in progress) a resource guide dedicated to their framework. This resource guide is here to help companies, manufacturers, service providers, etc., to adopt and implement the Trust framework. It gives context, consideration and resources for every principle in the framework and serves as an official aid to the establishment of the Trust Framework. Before their work on this framework, the IoT Initiative also created checklist to support users in the purchase and setup of smart products. This resource guide also contains, maybe more obvious, additional considerations on IoT devices. This checklist contains separate parts regarding security and privacy. It is a great addition for consumers as it helps them to avoid mistakes and gives them tips to use their everyday products with security and privacy in their mind.

4.1.9 Works with Nest

Works with Nest is a certification program created by Nest to inform customers that the devices they just bought can be compatible with already existing Nest products and will therefore work within their ecosystem. Their list of companies who have built certified

“Works with Nest” (WWN) products include names like Amazon, Whirlpool, Philips, Logitech and many more. To be in that list companies have to get reviewed by Nest regarding their compliance on development requirements and also their design and marketing policy. WWN is made to be easy to use for the end-user, to add and remove a certified product into the Nest ecosystem is very fast and can be done directly in the Nest app of your phone. However, to ensure a minimal protection, only the owner of the Nest Home (the equivalent of the administrator) can manage WWN products or services.

Even is Nest has been bought by Google, they are still run as an independent entity and do not share any personal information unless you want it, with any Google services or products. They are very thoughtful of the concerns we may have regarding privacy and even have an entire part of their website, named “Home is a safe haven” dedicated to this subject. I will briefly focus on their privacy policy and see how and if they are applied to their WWN certification program. First of all, Nest only share personal information when a permission is explicitly given by the user. You can also review all the permission you have given, know why they exist and revoke them at any time. They also use encryption to protect their connections and, according to their website, stay up to date on security and possible threat to be as vigilant as possible. Along its “best-in-class data security tools”, Nest also has a Delete My Account option that will remove every trace of your data from their servers. This option still let you use the product you bought, it will just be a little less smart (Nest Labs, 2016).

Concerning the WWN program, the privacy requirements to be certified are about the same. Every third party that is added to the Nest Ecosystem in your home will have to show details about information exchange between the Nest products and them. The WWN developers also have to use OAuth 2.0, a well-renowned authorisation system, to secure the access to the data with tokens. This security protocol is the same used in Nest products. The rest of the guideline follows the same principles as with every Nest product: the third parties have to ask permission and it can be revoked by the user whenever he/she wants it. On the Nest Developers web page, they have a paragraph about the guidelines to follow and how serious it is. They named this part “We can revoke access at any time. And so can our users” (Nest Labs, 2016).

4.1.10 Apple HomeKit and Its Certification Program

The smartphone manufacturers are also trying to create an ecosystem where their product could be smart together. Apple announced the framework HomeKit in 2014 and a certification program that would help to connect smart home devices through the use of

iOS devices. Nearly two years after there are 42 certified products, including colour declination. It is not the trendiest certification especially if you compare it to their similar, in a certain way, program “Made for iPhone/iPod”.

Apple has a paragraph regarding HomeKit on their privacy web page. We can learn here that Apple does not know what smart devices you own and when you use them or not. Then the applications that support HomeKit are not able to perform any other functions than home configuration or automation services. Everything regarding the data generated by your smart devices is stored in the encrypted part of your Apple device. Communications between the objects, your phone, apple servers or even third-party applications are all encrypted.

As with other certification programs, Apple has made a list of requirements every hardware or software developers who want to be part of the HomeKit family must follow in order to be certified. These requirements are very strict regarding the hardware aspect according to multiple companies. When building a will-be HomeKit device that use Bluetooth LE and Wi-Fi connectivity you sort-of need to include an encryption chip in your device. If you choose not to, you will probably have a not-so-great experience. According to Forbes, who contacted different companies with HomeKit products certified by Apple, the level of encryption necessary to obtain the certification is very high. It is so demanding that Bluetooth LE devices are having issues when they need to generate and send the encrypted key because of their lack of computing power. It seems that Apple wants to force security and privacy but that the current chips are not ready for that and according to Diogo Monica, an IEEE security expert, it may be a good thing. He said that the industry has not really cared about security for their Internet of Things devices and now Apple if enforcing them too with their certification program (Tilley, 2015).

4.1.11 Samsung SmartThings and Certified Products

SmartThings is a company specialised in smart home and the IoT for consumers. It has been founded in September 2012 with the help of people from all around the world via the crowdfunding company Kickstarter and has been bought in August 2014 by Samsung who now use it as its main IoT platform. The difference between SmartThings and other IoT services and product providers is the addition of a physical hub instead of a virtual one on the cloud. This hub allows you to monitor, control and secure your home as well as connect your IoT enabled devices regardless of the communication protocols used by them. This allows SmartThings to be compatible with more than a hundred different smart things, including ZigBee and Z-Wave radio compatible devices. This hub-orientated

system allows the Samsung solution to be compatible with more devices than its competitor and reduce the possibility of lock-in, where users who decided to embrace a particular standard or solution stay need to stay with it forever. The downside of supporting multiple protocols is that it could allow for more potential vulnerabilities for each new protocol or standard you decide to accept within the hub.

Samsung was recently pinned for privacy issues concerning their Smart TVs which were sending unencrypted data-voice and text to a third party over the Internet, I will write a bit more about that in the second part of this research work.

The privacy page on their website is basically the Privacy Policy you have to accept when you use any of their services because it is in the Terms of Use. This is not as easily readable as other privacy web page but it has the merit of being totally transparent, everything you need to know about your information can be found in this page. They are describing which kind of information can be shared with third parties and how they protect still try to protect our anonymity.

For example, they inform via email users every time they change their Privacy Policy. The problem is that you can opt-out of the email notification and thus could miss the Privacy Policy update you automatically agree on. They also explain every kind of information they may collect and store, but it would be only data that you would knowingly provide them. The SmartThings account you use has privacy settings that you can modify to change which Personal Information are displayed on your profile and visible to the others. They also indicate what could happen (in this case asset transfer to the new company) if there is a business transfer or if another company buy them. Concerning more specifically their SmartThings hub, it can collect video streams but do not store it on the cloud unless you specifically ask for it or if it triggers an alert. In this case it will send just the concerned portion of the video flux and not the entirety to protect your privacy when transferring the data.

4.1.12 Results

The way privacy is described in the group, alliance, consortium and other labels is very different but a lot of groups agree that privacy is an important part of the security processes and that they should act to prevent issues on this subject. I will use here the term “group” do discuss the alliance, working groups, consortium and label as a whole without any distinctions between them.

These groups may seem similar but they are not all doing the same jobs. For example, WWN is the label made by Nest and therefore apply the same privacy concept as Nest. But if you look to the Thread Group, which is also linked to Nest, there is not a word on privacy on their website. There are other groups who serves a standard creator, other who are there to simplify communications between leaders of the industry and some of them who are trying to build an ecosystem based on their own solutions.

Regarding the group categories here is how I visualise it after my research. The groups can be roughly separated into three different categories regarding of their stance on privacy. There are the ones who do not talk about privacy at all. The ones who write about it but do not act in a very protective way and finally the rest who seems to handle privacy as part of major importance in their products and services. Let us describe a bit whom is in which groups and what are their impacts on privacy protection.

The first group does not seem to be concerned at all about privacy and the related issues. The Open Connectivity Foundation, the Thread Group and their associated framework and The Internet of Things Consortium are represented in this category. These groups are focused on the technical part of issuing a communication framework, for example. They all take into account security in their writing but there is nothing specifically on privacy. They are describing how their protocols/standard work and the security gains that will result but there is not a word on how it could or will change the course of privacy when applied.

The second group acknowledge that privacy can be an issue and that companies should do something about it. These companies are taking privacy into account and describe how they are trying to protect it. This is a good point but after reviewing their privacy policy we could argue that it is not enough compared to the rest of the third group. In this second group there is the Industrial Internet Consortium who does not really focus on the consumer side of the IoT market and therefore do not focus that much on the privacy side either. Then there is Samsung and its SmartThings certified products. There is not much information on which verification is made by SmartThings when they accept a certain kind of smart devices in their hub. It has caused them prejudice with the ZigBee “insecure rejoin” function that allowed hacker to access the SmartThings hub with a ZigBee compatible product. Their own Privacy Policy is clear but the compatible products need to be more thoroughly verified. These companies have plans regarding privacy and it is a great start but it does not seem to be as advanced as the companies in the third group.

The third group is taking real action toward privacy issues and consider it as a central threat for customers that need to be taken into account. Surprisingly, the groups involved

in this category are not the one focus only on IoT issues but instead it is the working groups of bigger technologies. The CSA IoT Working Group and the OTA IoT Initiative are the best examples of this category. They are part of a bigger picture but their focus on privacy is exemplary. They drafted principles, recommendations, advice and much more for companies to work on when creating IoT products and services. The OTA IoT Initiative even created check list and tips for the consumers, in order to help them apprehend this new world of connected smart devices. In this category we could also cite Apple and Nest who seems to really eager to protect our privacy, even with third parties in their certification program. Apple is asking for so much computer power in terms of encryption that simple devices cannot even handle it without causing enormous lag during the utilisation. Then there is the IEEE who is working on a new standard. I choose to put them in this category because, even if the standard is not yet released, they did a lot of research and case study based solely on privacy and it will probably be seen in their standard too.

Another trend that we can observe from this topic is the way companies are forming and joining groups. Technology companies are joining forces in order to create a better future for the Internet of Things era but they do not seem very sure of the way to operate. A lot of them are present in multiple groups. Some of them are not mutually exclusive, after all the CSA and OTA are not solely focused on the IoT and a membership there does not create a threat for the other groups. But in other cases there are companies like Qualcomm and Microsoft who are in both the Thread Group and the AllSeen Alliance. These two groups are working on a framework whose purpose is to become the standard in IoT. It may seem counterproductive but backing the two of them ensure them to be on the winning side at the end. As with the Blu-ray and the HD-DVD, or even the VHS and Betamax format, there will be only one winner at the end of the race.

4.2 Real-Life cases

4.2.1 Introduction

In this part of my research I will aim my focus on real-life examples of privacy protection, or destruction, with the existing IoT devices available on our shelf. I will show two examples of smart devices that are linked to the previous groups we have seen in the first part of the research work to see whether or not they act accordingly with their saying.

As stated before this part of the research will be mainly issues within an ecosystem or a smart device as reported by the media. I will try to focus on the long story, and maybe the resolution, each time and not just look at the problem alone.

4.2.2 Samsung SmartThings and the ZigBee Insecure Rejoin

Let us start with a recent issue that has been discovered, fortunately, by Tobias Zillner a security researcher at Cognosec and presented last summer at a conference in Las Vegas. However, for security reasons, the issue as only been published in the mid-February of this year by Forbes. This hack can potentially happen in every home equipped with the Samsung SmartThings hub and even more as the hub technology is coming to their smart TV and appliances.

As we have seen before, the SmartThings hub act like a central alarm system. It connects all the sensors and it is in charge of alerting the users when something does not seem normal. Tobias Zillner first discovered that he was able to decrypt the key exchange between the hub and a motion sensor and thus decrypt further communication on the network layer. He was also able to jam the signal by sending a strong one at the same frequency. This result in the sensors not capable of detecting any movement and even worse, not alerting or logging the fact that it has been jammed.

These discoveries are to be taken seriously but there is one who is even more of a threat. M. Zillner later discovered that he could use a weakness in a feature of the ZigBee wireless protocol known as “Insecure Rejoin”. This feature was originally made for not always active devices to rejoin their previous network even if the network key had changed in the time where they were not active. But in our case this allows the researcher to ask the hub for new communication keys and therefore enable a hacker to retrieve the active encryption key at any time he wants. A related issue with this hack is that you cannot reset the encryption key of your device (Fox-Brewster, 2016).

The SmartThings team has known this problem since the beginning of December and tried to act on it. Dan Lieberman, the head of research & standard at SmartThings has published on the fifth of December a post on the SmartThings forum to explain the issues, the impact and what is being done about it. He explained that all the issues of the Forbes article are issues with the ZigBee Home Automation standard and thus impact many companies and are not specific to SmartThings. He also indicated that they were working on an update to allow users to disable the insecure rejoin feature and that in the long term the next ZigBee protocol update will also fix this vulnerability.

The SmartThings update exists now and effectively allow users to disable the insecure rejoin, pending a better solution from ZigBee themselves. In addition to their update they created a FAQ on this “Insecure Rejoin” problem that explains what is the situation, how to deactivate this function and what are the pros/cons of doing it. They also did a step-by-step resolution problem if after deactivating the function some of the ZigBee device does not reconnect automatically to the network. In this FAQ we also learn what is SmartThings doing for the security and privacy of its users and that they scored highly in the recent FTC privacy conference (SmartThings, 2016).

4.2.3 Nest Thermostat Hacking and Overall Reliability

According to multiple security researchers, including for example Synack, Nest is one of the leaders regarding the small but not for long IoT security world. After a benchmark of 16 different devices from the thermostat to cameras and other home-automation devices Nest was the overall leader across the different categories (Moore, 2015). But its leader status does not prevent it from getting hacked, among other things.

Security researchers at TrapX Security were able to hack a Nest Thermostat and use it as a jumping off point to gain control into other devices in the connected home. They used a discovery from last year made in the University of Central Florida in which during the boot of the device they could load a custom software into the connected thermostat. TrapX Security use this information to load their customer firmware into the processor chip. When they are inside they can obtain the Wi-Fi password and even know whether you are home or not (via the Away status of the Thermostat). During the demonstration the researchers showed that they could stop the data transit onto the Nest servers and use it for their own purposes instead.

However, there are a few downsides for the hackers, and upsides for everybody else. Regarding company security, this type of hack will most of the time not work because it uses ARP spoofing to jump into other devices and it is normally protected in a company environment. But the foremost reason this hack is not a reason to throw our connected thermostat by the window is that hackers would need a physical access to the device to implement the custom firmware. This hack is impressive but the fact that physical access is needed is reducing immensely its impact. According to TrapX the majority of hack like this would be made by people buying the thermostat and getting a refund or people selling used one on the Internet.

The problem with this kind of hack resides in the hardware part of the device and therefore cannot be fixed easily. It has been more than two years that this vulnerability exists and nothing has been done to prevent it. But according to Nest, none of their connected thermostat has been compromised by an attack of this type (Tilley, 2015).

Another little but still existing problem has bugged Nest devices in the past month and it concerns reliability, especially for parents. Nest bought in June 2015 Dropcam and rebranded one of its products into the name Nest Cam. A connected security camera that works within the Nest ecosystem and can be used, inter alia, for monitoring your baby.

According to the Time not everything works well with the Nest Cam and there have been issues with video feed outages, even after a reboot of the app, phone and camera. In September there has been an outage for more than four hours and it also concerned the remote control and alerts of other Nest products, their thermostat and smoke detector. There have been at least three major outages, counting this one, in the year before the publication of the Time article. Nest has well-encrypted camera and was not on the list of the numerous hacked baby monitor but there still have some troubles with their servers. These three, hours long, outages can be seen as quite reasonable but for new parents who rely on these services it can change a decision between a basic baby monitor and the Nest Cam (Pullen, 2015).

4.2.4 Results

These two real-life cases are not the worst that have happened in the small life of consumer IoT. It is just two examples of what can happen, even to enormous firm. Of course, the likewise of this attack related to these examples is very low but it is still existent and could compromise the sanctuary of privacy that is your home. As seen in the cases above, the privacy issues that could result are not only due to security problems in

the company. Samsung is, according to some research, taking great care of our privacy but it should look a bit at its open philosophy regarding the hub and protect what others cannot or take too much time to. Regarding Nest, no burglars in their right mind with a physical access to your home would steal your thermostat instead of your valuables for now. But when a lot more objects will be connected, the malicious code in one thermostat across your home could have enormous privacy consequence.

Finally, if we look at other, maybe smaller, companies that build IoT devices we can observe a small trend that appears in nearly every growing market. This trend is something that looks as “ship first, patch after”. Everyone wants to be present on this mounting market and do not hesitate to sell their product a bit early and fix them later in order to grab precious market share.

5 Evaluation

Results evaluation

At the beginning of this work I set goals that I hoped to fulfil by realising the thesis. The main objective of this thesis was to assess the privacy situation in the Internet of Things. It has been done during the research work with different methods who gave a better overview of the situation. The research on the different groups was the most necessary point to avoid falling into a judgement too soon, especially with a growing platform like the Internet of Things. As stated before, if I had only looked at media articles I would have had a biased version of the story on privacy. With the help of the first research part we can see in the long-term and get a better view of what is ahead.

I also tried to categorise and sort a bit the different groups who are working on these different standards regarding their stance on privacy. This categorisation is empirical and subjective, it is not based on a scientific classification but on my own experience and wishes concerning my online privacy.

Results Validity

My research results are based on my reviewing of the different groups and their official communication on their website and the documentation available through it. I tried to stay objective on everything I discovered and only transmitted the facts and not personal interpretations. On the real-life cases I gave a full overview of the stories and tried to bring the point of view of everybody involved when it was possible.

Everything included in the research work was valid and right at the time of the writing of this thesis but as with every technological subject, especially in IT, it can change rapidly. The Internet of Things is still at the beginning of its market adoption by the world's consumer and a lot can change in the next few years.

Regarding the Sources

Before writing the background theory, I reserved a book at the library: "The Internet of Things" by Samuel Greengard, 2015. This pocket book helped me to specify my ideas on the subject and write the theory in a very efficient way. Then I added a few other books, some about Big Data because it is a linked subject, others about the stake of our information on the Internet and how marketers use it to create more personalised ads. I

also added a book whose approach of technology and information was more generic and fitted greatly in the thesis.

Along the books I used and cited in the background theory I also borrowed information from the official website of diverse technology groups, security report, magazines and other online newspapers. The Internet of Things is a rather new term, at least for the consumer world. It only started to grow exponentially in Google Search in 2013 but there is still a lot of different articles about its development, issues and future. The subject is well covered and I tried to get a maximum of different source points. Theses eclectic references make about 40 different sources that allowed me to depict more clearly the privacy situation in the Internet of Things.

Project Management and Learning

Regarding my project plan I respected more or less the multiple deadlines I fixed and I did not have to work countless hours on the last days and weeks. I began my thesis by reading the book by Samuel Greengard which I wrote about just above. After finishing this book, I had a clearer view of how to structure my thesis and finalising my project plan. The project plan did not change very much. I changed the work repartition for the research and focused more on the technology groups. It allows this thesis to be more valuable in the long term than if I had stopped my research at the different articles about hack that happened in the recent years. I also removed a little part of the research part that was supposed to contain the point of view of experts. After reading a lot of interviews from experts of the field, security researcher, IoT manufacturer and so on I decided not to include them because the opinions are too unalike in their view of privacy and the future of IoT. Therefore, it would not have added anything useful for the research because there is no common thinking of that subject that could be generalised.

Then began the writing process for which I tried to write minimum a page per working day. This strategy helped me for many reasons. First, it allowed me to divide my thesis into little parts that I could complete and review on the same day and not have to worry any more about it later on. Then, with this working methods I was always focused on my subject and did not forget where I was in my work and where I needed to go from there. Finally, by working a bit each day it was a rather easy task to respect the delay I fixed myself and to still have a work-life balance even when approaching the deadline. This way of proceeding taught me a lot about time management and I could see every day how it affected positively my research work.

I learned a lot in this thesis work on a rather broad spectrum of subjects. In addition to the work methods I wrote about above I also absorbed new information on nearly every aspect of the Internet of Things. From its beginning to the newly created standard groups and objects emerging every day, I acquired a lot of knowledge about the Internet of Things and its surroundings and I keep learning every day about it.

6 Conclusion

6.1 Summary

The IoT is a growing market and according to multiple research group it will be a billion-dollar market counting billions of connected devices. To put it bluntly: This is going to be enormous. Alongside we have more and more revelation from whistle-blowers on the stake of our privacy online and how it does not really exist any more.

This research thesis was written with one purpose in mind to see whether the stake of our personal privacy is taken into account in the IoT revolution that is coming. But before going into the research phase I first wrote a bit of background theory about the IoT, the cloud, privacy a few other things.

The Internet of Things is a vast subject with a lot of ramifications. To simplify my explanations, I started from its origins. It includes the creation of the Internet, how the cloud evolved from it, the beginning of mobility in our technology solutions and so on. Then I explained a bit how a part of the IoT is already in use for years in the industrial sector with the Industrial Internet and the M2M communication. To complete the overview of the market I wrote about the consumer side of the Internet of Things, the one who will have the biggest market share according to Gartner. I used the example of the smart fitness trackers for this because a lot of people know them or even wear them. The next chapter is a bit more negative because it is about the risks and repercussions involved in this revolution. A lot of sensors and connections centralised in a point can be a very good optimisation for the city traffic but when the centralised point fail the rest follow rapidly.

To finalise the background theory part, I wrote about privacy and how it is defined according to the dictionary. I also discovered that it is a fundamental human right defended by the United Nations, even in its online meaning. In this privacy part I also write about how subjective privacy is and that it cannot exist a unified line between private and public because it would change for every person. Additionally, I used a research that show how privacy is valuated by consumers and it can act as any tradable goods or services once you get an offer from it.

Then I began the research work with an analysis of the different groups that want to revolutionise the Internet of Things. These groups are made of different actors from the technology field with big names like Intel, Microsoft, Qualcomm, Cisco, etc.

Their main purpose is to facilitate communication between the vast range of existing IoT devices by creating new wireless communication framework. I also analysed something I defined as a label, like the “Work with Nest”. This is a certification given by Nest after a product has passed the different requirements of Nest. I looked deeper into these conditions to see whether or not privacy management in included in this kind of label like this is the case with the WWN.

Then I did a little research on security vulnerabilities that have been exploited by hackers or researchers on products made by companies included in the first part of my research. I explained two different cases, one involving Samsung SmartThings and the other with the Nest ecosystem. These examples helped me to show that even successful and well-recognised companies like Samsung and Google (via its Nest acquisition) can have security vulnerabilities that can impact our privacy.

6.2 Further Research and Development

When I wrote this thesis not every framework, standard and protocols were fully developed. It could be interesting in a further research to see what the final version would look like and if they implemented more security to enhance our privacy what was their approach to it and how they manage to protect it.

This further research could also focus on the choice and grouping of the different technology companies to support a certain standard or framework. It is already happening with the Open Connectivity Foundation, a result of the merger of the OIC (Open Interconnect Consortium) and a part of the AllSeen Alliance. The OCF is very important because it groups two processor manufacturer, Intel from the OIC and Qualcomm from the AllSeen Alliance and make it possible for them to work together at the future of IoT hardware. There is also Microsoft who announced a version of Windows 10 tailored for the connected devices and also that all of their windows 10 versions will support the OCF standard. Now we have to wait a bit more if these mergers and collaboration announcements are going to be a trend or will stop there.

Another step that could change the IoT landscape is the finalisation of the IEEE standard. If the technology firms will follow the lead of this standard and act as unified as with the Ethernet and Wi-Fi standards, then the evolution of the Internet of Things will be transformed into real revolution. This would benefit both the product manufacturers and us, the consumers.

Finally, along the upcoming frameworks and standards there is another point in which a further research could focus. It is the advancement, or reduction, of privacy not necessarily related to the Internet of Things. After the recent terrorist attacks across the globe, some governments are taking extreme measures to protect their citizen and sometimes at the expense of their privacy. Related to this security/liberty debate Benjamin Franklin, founding father of the U.S. once said and was later echoed by Edward Snowden: “Those who surrender freedom for security will not have, nor do they deserve, either one.” The citation itself is prone to a lot of debate on its original meaning but I cannot talk about privacy and security without using it.

7 References

Affinnova. (2015, January 4). *Infographic: Why the 'Internet of Things' Hasn't Really Caught On Yet*. Viewed on February 16, 2016, retrieved from AdWeek: http://www.adweek.com/news/technology/infographic-why-internet-things-hasnt-really-caught-yet-162134

Alessandro Acquisti, L. J. (2013, June). *What is privacy worth?* Viewed on March 17, 2016, retrieved from Carnegie Mellon University's Heinz College: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-worth.pdf

Bernard Condon, P. W. (2013, January 23). *AP IMPACT: Recession, tech kill middle-class jobs*. Viewed on Mars 8, 2016, retrieved from Associated Press, The Big Story: http://bigstory.ap.org/article/ap-impact-recession-tech-kill-middle-class-jobs

Business Wire. (2016, February 21). *Visa Brings Secure Payments to the Internet of Things* . Viewed on February 29, 2016, retrieved from Business Wire: http://www.businesswire.com/news/home/20160220005021/en/Visa-Brings-Secure-Payments-Internet

Cisco Systems, Inc. (2016, February 3). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper.* Viewed on February 24, 2016, retrieved from Cisco - Visual Networking Index (VNI) : http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

Cloud Security Alliance - IoT Working Group. (2015, April 20). *New Security Guidance for Early Adopters of the IoT.* Viewed on March 30, 2016, retrieved from Cloud Security Alliance - Research: https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

Cox, L. (2015, January 2). *IoT vs M2M: Understanding the Difference* . Viewed on February 25, 2016, retrieved from PubNub: https://www.pubnub.com/blog/2015-01-02-iot-vs-m2m-understanding-difference/

Cronin, M. J. (2010). *Smart Products, Smarter Services.* Cambridge: Cambridge University Press.

Duhigg, C. (2012, February 19). How Companies Learn Your Secrets. *The New York Times Magazine*, 30.

Ericsson. (2015, June 3). *Ericsson Mobility Report: 70 percent of world's population using smartphones by 2020*. Viewed on February 22, 2016, retrieved from Ericsson: http://www.ericsson.com/news/1925907

European Commission. (2015, October 7). *Statistics – accidents data*. Viewed on February 28, 2016, retrieved from European Commission, Mobility and Transport - Road Safety: http://ec.europa.eu/transport/road_safety/specialist/statistics/index_en.htm

Fox-Brewster, T. (2016, February 17). *Samsung Fails To Secure Thousands Of SmartThings Homes From Thieves*. Viewed on April 10, 2016, retrieved from Forbes - Security: http://www.forbes.com/sites/thomasbrewster/2016/02/17/samsung-smartthings-vulnerabilities/#1562b7324e59

Gartner. (2015, November 10). *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015*. Viewed on February 12, 2016, retrieved from Gartner: http://www.gartner.com/newsroom/id/3165317

General Assembly. (2013, December 18). 68/167. The right to privacy in the digital age . Geneva, Geneva, Switzerland.

GeoHive. (2012). *Population of the entire world, yearly, 1950 - 2100*. Viewed on February 18, 2016, retrieved from GeoHive: http://www.geohive.com/earth/his_history3.aspx

Google Self-Driving Car Project. (2015, June). *How it works*. Viewed on February 28, 2016, retrieved from Google Self-Driving Car Project: https://www.google.com/selfdrivingcar/

Greengard, S. (2015). *The Internet of Things.* Massachusetts Institute of Technology: The MIT Press.

Industrial Internet Consortium. (2016). *Frequently Asked Questions*. Viewed on March 28, 2016, retrieved from Industrial Internet Consortium: http://www.iiconsortium.org/faq.htm

ITWG. (2016, March 3). *IoT Trust Framework - Security, Privacy & Sustainability.* Viewed on April 1, 2016, retrieved from Online Trust Alliance: https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_released_3-2-2016.pdf

James Macaulay, L. B. (2015). *Internet of Things in Logistics.* Viewed on February 16, 2016, retrieved from DHL: http://www.dhl.com/en/about_us/logistics_insights/dhl_trend_research/internet_of_things.html

Jordan, J. M. (2012). *Information, Technology, and Innovation.* Hoboken, New Jersey: John Wiley & Sons, Inc.

Lancaster, A. (2015, March 20). *My Scale Just Told the Cloud I'm Fat: Access Management, Security, Privacy and IOT.* Viewed on March 27, 2016, retrieved from Wiki AllSeen Alliance, Gateway Agent Project: https://wiki.allseenalliance.org/_media/gateway/security_privacy_and_iot_linux_foundation_collab_2015-02.pdf

Moore, C. (2015, March 14). *Home Automation Benchmarking Results*. Viewed on April 11, 2016, retrieved from Synack: https://www.synack.com/2015/03/14/home-automation-benchmarking-results/

Nesamoney, D. (2015). *Personalized Digital Advertising.* Old Tappan, New Jersey: Pearson Education, Inc.

Nest. (2015, February). *Real Savings*. Viewed on February 26, 2016, retrieved from Nest: https://nest.com/thermostat/real-savings/

Nest Labs. (2016). *Home is a safe Haven*. Viewed on April 4, 2016, retrieved from Nest: https://nest.com/privacy/

Nest Labs. (2016). *Overview - Security*. Viewed on April 4, 2016, retrieved from Nest Developers: https://developer.nest.com

Oxford University Press. (2013). *Oxford Dictionary of English.* Oxford: Oxford University Press.

Pauli, D. (2011). *The Smart Thermostat, Using Occupancy Sensors to Save Energy in Homes.* Viewed on February 26, 2016, retrieved from ETH Zürich: https://www.vs.inf.ethz.ch/edu/FS2011/DS/slides_talks/2011-05-24_daniel-pauli_smart-thermostat.pdf

Polsonetti, C. (2014, July 15). *Know the Difference Between IoT and M2M*. Viewed on February 25, 2016, retrieved from AutomationWorld: http://www.automationworld.com/cloud-computing/know-difference-between-iot-and-m2m

Pullen, J. P. (2015, September 9). *Here's Why Parents Are Angry at Nest*. Viewed on April 11, 2016, retrieved from Time: http://time.com/4026192/nest-outages/

Rozenfeld, M. (2014, March). *The Institute - The Internet of Things.* Viewed on March 28, 2016, retrieved from IEEE - Internet of Things: http://iot.ieee.org/images/files/pdf/The_Institute-IoT.pdf

Sicular, S. (2013, March 27). *Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s*. Viewed on February 24, 2016, retrieved from Forbes: http://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/#5a27b4da3bf6

Siddique, H. (2015, December 4). *Fitness trackers enjoy healthy sales despite lack of evidence they work*. Viewed on February 26, 2016, retrieved from The Guardian: http://www.theguardian.com/lifeandstyle/2015/dec/04/fitness-trackers-healthy-sales-despite-lack-of-evidence-work

SmartThings. (2016). *ZigBee "Insecure Rejoin" FAQ*. Viewed on April 11, 2016, retrieved from SmartThings Support: https://support.smartthings.com/hc/en-us/articles/208201243-ZigBee-Insecure-Rejoin-FAQ

Stone, B. (2009, July 17). *Amazon Erases Orwell Books From Kindle*. Viewed on February 29, 2016, retrieved from The New York Times: http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html?_r=0

Strong, C. (2015). *Humanizing Big Data.* London: Kogan Page Limited.

Thread Group. (2015, July 13). *Download - White Papers - Security and Commissioning.* Viewed on March 27, 2016, retrieved from Thread: http://www.threadgroup.org/technology/downloads

Tilley, A. (2015, July 21). *Apple's HomeKit Is Proving To Be Too Demanding For Bluetooth Smart Home Devices*. Viewed on April 4, 2016, retrieved from Forbes: http://www.forbes.com/sites/aarontilley/2015/07/21/whats-the-hold-up-for-apples-homekit/#63eb3c3c322b

Tilley, A. (2015, March 6). *How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home*. Viewed on April 11, 2016, retrieved from Forbes - Tech: http://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#12b096225cb0

United Nations. (1948, December 10). *The Universal Declaration of Human Rights.* Viewed on March 17, 2016, retrieved from United Nations: http://www.un.org/en/universal-declaration-human-rights/

Visa Inc. (2016). *Visa brings secure payment solutions to the Internet of Things*. Viewed on February 29, 2016, retrieved from Visa: https://usa.visa.com/visa-everywhere/innovation/visa-brings-secure-payments-to-internet-of-things.html

Vodafone Limited. (2015). *What is M2M?* Viewed on February 25, 2016, retrieved from Vodafone Business: http://www.vodafone.com/business/m2m/what-is-m2m

Yale. (2015). *Secured by Yale. Connected by Nest.* Viewed on February 27, 2016, retrieved from Yale: https://yale2you.com/LinusLock