To what extent is Privacy respected in Marketing involving Internet of Things?

Author: Teodora-Maria Gherasim
University of Twente
P.O Box 217, 7500AE Enschede
The Netherlands

Abstract

This paper aims at highlighting the current privacy issues in the context of Internet of Things and Marketing. The goal of the research is to see whether or not the privacy is respected in the case of IoT devices used in marketing. The extensive research lead to an in depth theoretical framework in three phases: Internet of Things, Internet of Things and Marketing, Internet of Things and Privacy. Afterwards, the theoretical insights gained were used to analyze two classes of devices in the above mentioned context, namely Smart home and wearable devices. Amazon Echo and Fitbit have been chosen as representatives for the two classes of devices. The analysis lead to the conclusion that even though both devices encounter privacy issues in their architecture as well as in their data privacy management, Fitbit is by far more transparent in its intentions than Amazon Echo. Therefore, Fitbit manages to respect the privacy of its customers far better than Amazon Echo, coming as a surprise since Amazon Echo is among the most popular choices in smart devices nowadays.

Supervisors: Dr. M. Stienstra, Dr. E. Constantinides

Keywords:
Internet of Things, Privacy, Marketing, Fitbit, Amazon Echo, Smart house, Smart wearable

11th IBA Bachelor Thesis Conference, July 10th, 2018, Enschede, The Netherlands.

Table of contents:

Chapter 1-Introduction

1.1 Introduction

The "birth" of the Internet, can be traced down back to the 1960s, which saw several historic events, most important being the Cuban missile crisis in 1962. Back then, Americans wanted to make sure that regardless of external influences (eg. bombing), the centers working on military research could still stay in contact with each other. The public unravel took place in 1972, and it was categorized by the "father" of the internet, Vinton Cerf, a "*roaring success*". (Keefer, Baiget, 2001)The Web as we know it today, with the World Wide Web file sharing was designed in the late 1980s at CERN as a tool used for locating and retrieving documents stored on servers across the world. (Naughton, 2016)

Nowadays, the Internet is seen as the technology that rules modern society. (Naughton, 2016). It became the biggest source of information in today's world, offering the World Wide Web, file sharing and multiple other features. With the evolution of Internet, smart devices evolved also in order to keep the modern human constantly up to date. With the development of technology and emergence and evolution of smart devices, scientists saw the potential behind these with embedded communication and information technology. All these "smart" devices use sensors, allowing them to perceive their environment, communicate with each other, interact with people and access the Internet. This level of connectivity between devices became known as Internet of Things (IoT). (Mattern, Floerkemeier, 2010)

There is not a consensus regarding when the IoT was born, however, it is known that Mark Weiser brought forward the concept in the 1990s. (Mattern, Floerkemeier, 2010) The importance of it has increased considerably in the past few years, proportional with the increase in smart clothing or wearable devices or simply with the increase in sensors in the environment. (Lamkin, 2017) Sensors started being used everywhere, from lighting to proximity sensors in machines, etc. Moreover, people started feeling the need of devices that monitor their daily activities, usually for health reasons. Smart watches that monitor heart rate, exercise, calories intake to glucose monitoring devices for people suffering from diabetes and mobility bands that help blind people navigate. (Lee, Lee, 2015) The IoT starts to become increasingly popular in everyone's lives.

The IoT can also be used as a powerful marketing tool. It can be used as a tool to promote immediate advertising, availability of promotions and many others, just as clients walk past a store. It has the ability of being context aware, meaning that it can adapt to changes in the environment. For example, it could be used to send promotions to potential clients as they walk into a store, based on their previous shopping history and interests. This scenario may seem impossible, but it is taking place in stores all over the world with the help of Beacons and other technologies. (Tsai et al., 2017) However, with the growth of IoT and with the growth of data produced everyday, both researchers and consumers started showing interest towards the problems this technology poses.

There is a general fear that all the data gathered from IoT devices can combine in unexpected ways, and "everything may reveal everything". (Peppet, Scott, 2014) Moreover, the companies that manufacture these connected devices are usually electronics manufacturers, trying to keep up with the fast-paced change in technology and with little expertise regarding security and privacy of data. (Milley, 2014; Peppet, Scott, 2014; Maras, 2015) Therefore, privacy in particular has been identified as a big issue in the Internet of Things technology, affecting future adoption of this technology by regular people. (Office of the Privacy Commissioner of Canada, 2016)

Companies producing IoT devices are using data collected by such devices to better understand the behavior of the customer and to better facilitate their services. However, not all companies collect such data with good intentions and sometimes they can be victims of cyberattacks, putting information at risk.

The implications of privacy in marketing involving IoT devices are crucial for the industry. Failure to ensure privacy can turn into devastating consequences not only for the company but also for the further adoption of the technology by other companies as well as customers. Therefore, it is of great interest to understand whether or not privacy is still respected, and if so, to what extent, in marketing involving IoT.

The first part of the paper will present the research gap as well as clearly state the research question. The second chapter will focus on describing the technologies behind Internet of Things, how it is currently used in marketing, and privacy issues in this environment. The third chapter of the paper will describe the methods used to choose and analyze the required information while the fourth chapter will present the findings, with a focus on wearable and smart home devices. The fifth chapter will answer the research question in a detailed manner and reach a conclusion based on the previously presented information, while the sixth chapter will emphasize the contribution of this paper to the research within privacy of IoT as well as limitations encountered during research.

1.2 Research gap

The research gap has been identified as privacy, based on extensive literature research. Most of the articles on IoT emphasize the need for privacy in this domain, presenting it as a crucial factor in the adoption and growth of the technology. (Lee, Lee, 2015; Xu et al. 2014; Stankovic, 2014, Office of the Privacy Commissioner of Canada (item 9 on reference list)). Problems are being raised lately in literature regarding "*whether it is the device being tracked or the individual*".(Office of the Privacy Commissioner of Canada) All of the information gathered from customers is intended to be anonymous and de-identified, however, it has been concluded that it is fairly easy for companies and hackers to re-identify this information and link it to a particular individual. (Atzori, Iera, Morabito, 2010). Furthermore, companies find themselves victims of cyberattacks and the information regarding behavioral patterns/locations of their customers are leaked, or, sometimes, companies willingly sale this information for marketing or financial reasons.

1.3 Research question

This paper will try to address the issues of privacy within marketing involving Internet of Things, in spite of the novelty of the concept. Therefore, this paper aims at answering the following research question: "*To what extent is privacy respected in marketing involving Internet of Things?"* This will be done through extensive literature research in the following fields: Internet of Things, Marketing involving Internet of Things and privacy of Internet of Things. In the results section, the findings will be presented with a focus on wearable devices as well as smart home devices.

Chapter 2-Theory

2.1 Internet of Things

2.1.1 What is Internet of Things?

There is no generally accepted definition in scientific literature on what Internet of Things actually is, due to the abstract concepts behind it and the novelty of the technology. Some researchers describe Internet of Things as a network of interconnected devices capable of communicating with each other (Lee, Lee, 2015), while others define the IoT as a network of connected devices through Internet, that allow remote control and monitoring (Perera et al., 2015; Chase, 2015) Internet of Things aims at providing a network where devices communicate with each other with minimal human effort and take actions based on the processed information in order to adjust and control the environment, with the help of sensors and actuators. (Whitmore et al., 2014; Perera et al., 2015; GSM, 2014)

2.1.2 Enabling Technology

The technologies that are most widely-used for IoT products and are of interest for this paper are:
1. BLE (Bluetooth Low Energy)
2. Cloud computing
3. Voice recognition

2.1.2.1 BLE (Bluetooth Low Energy)

The Bluetooth Low Energy technology is based on short range radio with a very low amount of power compared to previously used Bluetooth technology, allowing it to operate for a very long time. (Al-Fuqaha et al. 2015) It is already implemented in smartphones, making it an ideal candidate for context marketing. Moreover, its feasibility has been proven in machine to machine allowing devices to communicate to each other (eg. sprinkler system could communicate with humidity sensors through BLE in agriculture to prevent water waste).

Al-Fuqaha et al. (2015) describe the principle of functioning in their article. The BLE covers a range of around 100 meters, making it perfect for communication over relatively short distances. When a BLE device acts as a “master”, it scans the network looking for “slaves” and the communication is done through 3 communication channels. In order to allow for discovery, a “slave” send advertisements on the previously mentioned channels. When the devices are not exchanging information, they are in sleep mode, explaining the lifetime of such a device. (Al-Fuqaha et al., 2015)

2.1.2.2 Cloud computing

As presented in the article by Botta & de Donato (2016) cloud computing refers to nearly an unlimited capacity of storage of information from IoT devices (the so-called Big data), with processing capabilities and “built” with privacy and security in mind. Lately, IoT and cloud computing started to become complementary technologies, due to their strong interconnection.

The National Institute of Standard and Technologies (NIST) describes it as: “*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. (Botta, de Donato, 2016)*

In the case of Internet of things, the cloud can act as an intermediate layer between the IoT devices and the applications, allowing the processing of information that originates from the device's sensors and sending a command to the application. (Botta, de Donato, 2016)

2.1.2.3 Voice recognition

Voice recognition started gaining more attention lately with the rise of intelligent personal assistants. The working process of a voice recognition device is fairly complicated. Johnson (2016) describes in depth the working process behind such devices. Therefore, the command is captured by the voice recognition system once it is woken up by the wake word. Usually, such personal assistants are always on, listening, waiting to hear the wake word in order to "wake up" and capture the command. After the wake word has been detected and the command has been captured, the signal will be sent to the cloud and passed through the speech recognition software. The audio is given a meaning in the cloud computing software and a command is issued that will be executed by the device. (Johnson, 2016)The cloud computing process is, in fact, more complicated as described above but it is beyond the purpose of this paper.

More information on other technologies such as RFID (Radio frequency identification), WSN(Wireless sensor network), Sensors, Big data and Middleware can be found in Appendix B.

2.1.3 Architecture

Bhattarai&Wang (2018) describe the architecture of the IoT as consisting of four elements:
1. IoT device
2. The communication
3. The cloud
4. Presentation and action

1. The IoT device part of the architecture refers to the device itself that could range from smart wearable to smart enterprise etc, as presented below in Applications.
2. The communication refers to the enabling technologies that allow communication between device and the cloud, between devices themselves and the internet connectivity of the IoT device (usually Wi-Fi).
3. The cloud has the ability to store all the big data collected by IoT devices, having an almost unlimited storage capacity.
4. Presentation and action refers to the applications that take action and present messages based on the collected and processed data from IoT devices.

A more detailed presentation of the architecture based on layers can be found in Appendix A.

2.1.4 Applications

Perera et al. (2015) identifies several categories of applications. However, the following are of interest for this paper:
A) Smart wearable
B) Smart home
A brief description of each category, as well as an example is given below:

A) Smart wearable:

Smart wearable devices can be worn directly on the body or embedded in items that come in close contact with it (eg. clothing) as well as inside the body (eg. sensor enabled pill).

B) Smart Home

Smart home devices aim at making the ambient more pleasant and, in general, their main scope is to offer convenience to their tenants. From smart thermostats, lighting control to even elderly assistance, the range of smart home application is wide. Perera et al. (2015) offer in his article "The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey" an in depth categorization of the smart home appliances, based on a survey on hundreds of IoT devices.

An overview of other applications such as smart city, smart environment, smart enterprise and healthcare can be found in Appendix C.

2.1.5 Current limitations

Given that IoT is a recent technology, its adoption is difficult. There is a consensus that the issues regarding its privacy and security that surfaced in the past few years will make the adoption even more difficult. (Lee, Lee, 2015; Whitmore et al., 2014**)** As it can be observed, many articles name security and privacy among the main challenges and limitations in IoT, while some of them consider the two the main reasons why the adoption of IoT will take longer than expected. (Perera et al., 2015; Lee, Lee, 2015; Papakostas et al. 2016; Atzori et al. 2017). The issue of security will not be treated further in this paper, while privacy is going to be the main focuses in the following sections.

Another limitation identified in literature is the lack of a standard communication protocol and platform. There are currently hundreds of IoT platforms on the market, due to high-tech companies as well as startups. However, failure to connect these platforms will lead to a very slow adoption of technology. For example, sometimes devices operated by Apple cannot be connected with devices operated by Samsung, leaving users with the option to only purchase their devices from one provider in order to ensure communication between them. Moreover, the lack of standard protocols makes it hard for new developers to focus on one framework when developing their product. (Perera et al., 2015; Lee, Lee, 2015; Papakostas et al., 2016).

2.2 Internet of Things and Marketing

2.2.1 Overview

There are voices calling the Internet of Things the revolution of the 21st century. With the prognosis that around 50 billion devices will be connected to the internet by 2020, it is easy to see why. (Nowodzinski et al., 2016). Moreover, the Internet of Things has the potential of creating a global added economic value of around 10-15 trillion dollars by 2030. (Claveria, 2017) Industrial Internet of Things and M2M communications are already a reality in many countries around the globe, Germany being only one of them with around 25% of its machinery using such technology. (Nowodzinski et al., 2016) The Internet of Things has the ability to influence other markets too, such as retail, healthcare, factories, cities etc.

Marketing using Internet of Things is becoming more of a reality given the amount of smart objects that are currently on the market. Starting with mobile phones, smart watches, speakers, smart TVs, they all offer valuable information to their producers on how to improve their services and to deliver them in times of need. Mobile marketing using Internet of Things can stimulate immediate purchase when clients express interest in something or influence consideration as they are inside the store.(Tsai et al. 2017)

Also, by using data from these devices or by aggregating data and monitoring the interactions between customer and devices, companies can improve their services and their products accordingly while also understanding customer behavior patterns. (Spilotro, 2016) IoT can add great benefits to an organization by enhancing their capabilities of data collection, allowing them to offer real-time response, increase their efficiency and productivity and connect multiple and different technologies.

2.2.2 Marketing Practices

Internet of Things can be used as a powerful tool in marketing. It has the ability to collect a huge amount of information given Big data and to deliver the appropriate service when clients needs it the most. Internet of Things allows the manufacturers to approximate the life of a device, to benefit from context and content marketing and to tailor their services to the client's needs. Below, an overview will be given of the most important marketing practices currently involved in Internet of Things, as well as methods of targeting of customers and the impact they have on the client's psychology. Moreover, an overview of how Internet of Things changes and improves business methods will also be provided.

A) Content marketing

Content marketing can be described as "*creating and distributing relevant and valuable content to attract, acquire, and engage a target audience with the objective of driving profitable customer action*"(Pulizzi, 2016).

B) Context marketing

Context marketing is similar to content marketing, with the exception that the message is personalized for the customer, and delivered at the right time, in the right place. Context aware marketing is the result of content marketing delivered in the right IoT environment and a very powerful tool for today's marketers. Perera et al. (2014) identify four main features for a context-aware application: presentation, execution and tagging.

For **presentation** the context can be used in order to determine what needs to be presented to the user. An example is given in the article of Perera et al. (2014), where a user with a smartphone and context-aware applications can see upon entering a supermarket a grocery list, based on the information received from kitchen appliances such as smart refrigerators, smart sensors installed in storage containers etc.

The **execution** feature refers to action taken in a certain context. Another example is given by Perera et al. (2014) about the execution feature. The author present the case when the car sensors alert the smart thermostat as well as the coffee machine that the inhabitant left work and is heading home in order to welcome him/her with the preferred temperature and coffee.

The **tagging** feature refers to the collection of information from multiple types of sensors in order to achieve the contextual understanding of the environment. (Perera et al., 2014)

C) Sensing as a service

A way in which companies can improve their services, is the sensing as a service. This practice involves buying and selling of data collected from IoT devices with the purpose of gaining insight into the information collected by other devices that may be present in the same environment. (Perera et al., 2015) This practice leads not only to economic leverage for companies but also to an open market of the desired big data. Data aggregation comes into play in sensing as a service, as aggregating data from multiple sensors/devices will further reveal more about the environment devices operate in. For example, an irrigation system could use the data from the sensors in the soil to decide whether or not it should start.

2.2.3Psychological Considerations of IoT in Marketing

Tsai et al. (2017) analyzed the behavioral implications on the perceived usefulness of the e-commerce marketing strategies of IoT apps. The results showed that convenience, information, entertainment and interactive incentives all had a positive impact on the perceived usefulness of the app. Also, perceived usefulness was found to have a positive effect on behavioral intention.

2.2.4 Targeting of customers

2.2.4.1 Bluetooth low energy

The functioning principles behind Bluetooth Low Energy have been discussed in section 2.1.2.1. Now, the applications and usefulness of the BLE in marketing will be discussed, using Beacons. The beacon is an application of BLE and it works by broadcasting its identifier to nearby devices (in general, smartphones). When such devices are nearby a beacon, they take certain actions.

Beacons transmit a universally unique identifier through BLE, picked up usually by compatible apps. (Tsai et al., 2017) Once the connection between the beacon and the device is realized, the beacon broadcasts a signal. Such a device is of great importance in marketing, due to its abilities of tracking indoor position of clients, proximity to the device (eg. time spent in a certain aisle) and personal interaction systems. Beacons also have the ability to trigger a location-based action such as a push notification or a check-in. (Tsai et al., 2017, Nowodzisnki et al., 2016)

Nowodzinskit et al. (2016) identified several functions of the beacon in marketing, some of which are listed below:

-the have the ability to show customers available product options and additional information
-allows customers to pay or to identify themselves
-ability provide immediate rewards based on the customer behavior
-broadcast information (ex. During an audio tour in a museum)
-able to store information about the client (eg. preferences stored on their loyalty card) and provide personalized offers based on their interests and preferences, eliminating spam

Such an application is increasingly important in marketing due to the desire of marketers to be able to analyze customer behavior in the store as well as to be able to influence their behavior in the moment of action/consideration of their shopping phase. Beacons are also able to provide information about the time clients spend in an aisle and tracking inside the store in order to see where the areas of interest are as well as to provide insight for better product placement.

2.2.4.2 Voice recognition

Voice recognition systems are among the most popular ones in everyone's homes today. There are estimates that the market of smart speakers will reach a revenue by 17.43 billion dollars by 2022, having registered a revenue of 4.4 billion dollars in 2017. (Statista) In 2016, 6.6 millions of homes from America owned such a device and by 2022 there are estimates that approximately 66.3 million homes will have a smart speaker, in US alone. (Statista)

A brief overview of how a voice recognition system works and what it is has been given in section 2.1.2.3. Now, an overview of how such devices can be used in marketing, using sources from literature and media will be presented below.

Voice recognition devices can be a strong tool for brands that want to advertise their products more efficiently. Given that such devices listen at all times to conversations going on around them, waiting for the "wake word", they can provide analysts and companies with a great deal of information. Such information could range from how they can improve their services and what their clients are unhappy about, to music preference of the user, products they like, as well as habits of the customers, helping companies to take advantage of context marketing.

More information on how RFID and Wi-fi are used in marketing can be found in Appendix E.

2.2.5 Influence on business methods

Internet of Things brought great changes in marketing and in business models. Hemmati (2016) presents some of the aspects where the Internet of Things can greatly impact and improve business methods.

With regards to marketing, even though the decision making process of customers is longer, companies are able to get immediate feedback by looking at the interaction between the device and customer. Existing technologies and analysis allow for quick processing of this feedback and tailoring of the marketing methods to customer needs. However, these marketing practices can lead to a big return in investment for companies and changes in business methods.

Another prime advantage of using Internet of Things is the fact that such devices can alert the manufacturer regarding their life ending. Such an example was provided by General Electrics. GE decided to invest 1 billion dollars in creating a software that would allow them to gather information from sensors embedded in machinery they have been producing for years (windmills, pumps etc). Such information would allow them to appreciate the lifetime of the device better and to facilitate their maintenance process by ordering the spare parts beforehand. (Regalado, 2014).

Moreover, the Internet of Things can be used for predictive social network. Such a feature can be facilitated by the use of Beacons that could, besides sending push notifications, to allow the customer to post a check-in on social media. Another example is Livehoods. Such application can provide businesses with information on the popularity of their perceived popularity based on social media check-ins. (Cranshaw et al., 2012)

Advertisement can be seen as another advantage. With the help of Internet of Things and context marketing, business do not have to throw money anymore on “blind” or “mass” advertising. Rather, they can tailor their advertising for every customer in part, ensuring increased sales and return on investment. Beacons are a great example in this context, with their ability of sending push notifications with tailored offers based on existing customer preferences. Such a possibility leads to another advantage, that of creating quality, long-lasting relationships with the customers given the ability to provide a solution to their problem when they most need it.

One last advantage identified is the ability to easily collect and exchange data. Given these capabilities, businesses can use information collected by other entities to analyze demand and popularity of their products in different areas/markets. Internet of things also facilitates the ability of businesses to collect real information that reflect the inner persona of the customer, rather than their online persona.

2.3 Internet of Things and privacy

2.3.1 Overview

There is currently no consensus regarding what classifies as privacy infringement when it comes about IoT due to the novelty of the technology and the lack of population awareness towards how this data can impact their lives. (Winter, 2013; Bailey, 2016)

IoT presents, however, some serious challenges towards privacy, as identified in the literature, worth mentioning being the aspects below:

People may not know when they are being monitored nowadays due to the small size of devices that can be integrated almost everywhere, new types of data can be collected due to the endless possibilities of integration and the possibility of aggregation of such data that can lead to individual identification and linkage to other personal records. (Winter, 2013)

Winter (2013) identified the fact that consumers are particularly concerned about the type of data being collected, the storage and the possibility of aggregation of data collected by IoT devices.

One of the main issues in IoT is the possibility to re-identify the de-identified data. De-identified data can be defined as *"process to prevent a personal identifier from being connected with information". (Bailey, 2016)* Re-identification of data could lead to information leakage concerning health state, private conversation, search history, banking details etc. (Bailey, 2016)

Another challenge of IoT consists of the inability of companies to tailor privacy terms. Most users end up being bound to standard "I agree" consumer click for a regular agreement with the company on privacy terms. (Bailey, 2016) Moreover, most privacy policies lack the information regarding who the "third parties" are in information share. (Bailey, 2016)

Concerning mobile device users, the activity on the device as well as the location-tracking services allow the analysts to paint a clear picture regarding where the user is usually going, preferred places, online activity and paint an overall picture about the individual. (Office of the Privacy Commissioner of Canada, 2016)

2.3.2 Privacy issues in main IoT enabling technologies

2.3.2.1 Bluetooth Low Energy:

Das et al. (2016) point out the fact that some Bluetooth devices use unchanged Bluetooth Low Energy addresses. This means that when devices using BLE broadcast their presence and are looking for a "master" they will always be identified by the same sequence of 12 letters and numbers. Considering that such information can be captured for example by Beacons and that it can be aggregated with data from video surveillance from stores, it may lead to identification of individual.

Another identified issue by Das et al. (2016) in their work is the so called "sniffing" of the device. Instead of sending the information to the desired receiver, a Bluetooth Low Energy connection can be intercepted, and the MAC address of the device trying to establish the connection can be detected. Once again, this can lead to identification of individual through information aggregation. (Das et al., 2016)

2.3.2.2 Voice recognition:

Voice recognition systems are designed to always listen and start recording once they hear the "wake word". (Wueest, 2017) Given the working principles of this technology, it is understandable why the issue of privacy is raised in the case of devices that continuously listen to conversations taking place around them.

Moreover, Alepis et al. (2017) refer in their work to an article by Jang et al, mentioning in their work their ability of making such systems perform unauthorized commands based, using among other methods, also voice. (Alepis et al., 2017)

With the current legal framework in place at the moment, it is also unclear whether or not owners of such devices should tell their visiting friends about the existence of such devices in their household that may record their conversations. (Wueest, 2017)

Considering the above mentioned problems, voice recognition systems should be paid special attention to with regards to privacy.

2.3.2.3 Cloud based model:

Capellupo et al. (2017) treat extensively in their work the privacy issues of the cloud based model. Some of the identified issues are:

- Users may feel as they have no control over their data and that their privacy is at risk. Main reasons identified are the lack of control over the location of data, the provider, the access that is granted to cloud data as well as whether or not the data is encrypted[1] when stored or if companies engage in transactions with the data without the user's consent.

-the issue of Government access to such data is being raised more and more often. In US, data older than 180 days can be released to the Government, following a request, and the user may not be notified of such action. (Capellupo et al., 2017)

Privacy issues of RFID can be found in Appendix F.

2.3.4 Where can an attack occur?

Bhattarai and Wang (2018) describe three main areas susceptible to an attack for IoT: the device, the communication network or the cloud. The devices can have software or hardware vulnerabilities, making them susceptible to hackers. The issues for communication networks and the cloud have been described in section 2.3.2. Such security attacks can lead to leakage of personal information and, in extreme cases, even identity theft, becoming an entry point into the privacy of people's lives.

2.3.5 Privacy infringement dark side behavior

With the rise of IoT, privacy infringement has also seen an increase. An overview of how data misuse by companies can harm customers in the long term is presented below.

Cremer et al. (2016) classify the main areas of IoT dark side behavior practiced by companies into:

1. Knowledge and intelligence-based dark-side behavior
2. Transaction based dark-side behavior
3.Relationship-based dark-side behavior and negligence
4. Integrity challenge and manipulative dark side behavior

Each of the 4 categories is further divided into more specific dark behaviors of companies

1. Knowledge and intelligence based dark-side behavior

This category refers first to information misuse of companies. More and more often, companies tend to use data in ways their customers disapprove of or sell such data to so called "third-party companies" without the knowledge of the user. More often than not, in privacy policies, it is not stated who such third-party companies are.

Second aspect of this category refers to privacy issues. The problem of access of sensible information or, perhaps, information that the user may want to keep private (age, financial statements etc) is brought up. The problem of invasive behavior or collection of more data than necessary by companies is mentioned in many articles.

1.Encryption of data means that only authorized parties have access to it due to complex encryption schemes.

2. Transaction based dark-side behavior

The first behavior that belongs to this category is the confusion of customer**s**. It is becoming more and more easy for companies to "trap" customers with disadvantageous subscription plans and to confuse or mislead customers into paying extra for certain services.

Second type of dark behavior refers to financial penalties. It is a practice usually found in the case of health insurance companies that constrain clients to wear certain health devices in order to possibly calculate a premium. Failure to do so, results sometimes in financial penalties for the client.

3. Relationship-based dark-side behavior and negligence.

Customer favoritism and discrimination can be considered to belong to this kind of dark-side behavior. Companies may benefit from the collected information on their clients and tailor their offerings based on the client's economic attractiveness.

Switching barriers and sunk costs can be considered as another sub-category of such dark-side behavior. Companies want to "lock-in" customers and will not refrain from making it costly when a client wants to switch to another provider. Moreover, sunk costs are common among IoT devices with upgrades or spare parts being more costly when buying them from the provider than from somewhere else.

4. Integrity challenge and manipulative dark-side behavior

Dishonesty belongs to this category of dark-side behavior with companies putting pressure on their agents to sell as much as possible, resulting in clients being charged for accessories they may not even need.

Unfairness is another sub-category of dark-side behavior, referring to practices such as discrimination or manipulation in order to lead to unwanted behavior.

Some of such dark side behaviors are practiced by companies with the help of vague privacy policies or simply through lack of communication with the client.

Real life examples of failure of companies to provide privacy to their clients and the associated dark side behavior can be found in appendix G.

2.3.6 Psychological considerations of customers:

With all the issues and examples of IoT devices going wrong, it is of interest to see what still makes people try it.

One of the main reasons identified by Bailey (2016) is the unrealistic optimism of consumers. Even though they may be aware of the fact that IoT device can affect their security and privacy, consumers may still choose to buy such an IoT device due to the fact that they underestimate the likelihood of such a device having a negative impact on them.

Another identified reason in the same article is the hyperbolic discounting. The benefit of privacy trading might be felt immediately by the consumer, given the usage of the IoT device and perhaps even additional benefits offered by the manufacturer, while the consequence, which is loss of privacy and its implications, are delayed. (Bailey, 2016)

Another study ran by Emiami-Naeini et al. (2017) revealed that the participants feel more comfortable with data that is being collected in public spaces compared to data that is collected in their homes. Also, it has been found that participants preferred anonymous data collection and data that is not stored indefinitely, but deleted after it has served its purpose. Participants preferred to know the purpose of the data collection as well as the security risks associated with it and who the third-parties companies are.

2.3.7 Solutions:

In order to solve some of the above mentioned privacy issues regarding technology and regulations for companies, a solution has been found in literature, concerning BLE:

Hashing of MAC addresses for BLE

Regarding the BLE technology, a proposed solution was hashing of MAC addresses. Every device has a unique MAC address, which, could be used to track the individual. However, by using hashing everytime a MAC address tries to connect to a device, a new number will be generated for it, making it close to impossible to identify the original MAC address. (Office of the Privacy Commissioner of Canada, 2016)

Chapter 3-Methodology

3.1 Sample

As previously mentioned, the focus of this paper will be on smart home devices as well as wearable. The choice of this population can be explained by the fact that, according to Linkedin, smart home and smart wearable are among the top applications for IoT. (Lueth, 2015) Smart home devices market is one of the fastest growing at the moment among IoT, growing by 95% between 2016 and 2017. Speakers in particular came in second in the segment classification, with 733 million dollars worth of devices sold in the same period. (Van, 2017)

With regards to the smart wearable market, it can be considered one of the most profitable, with a predicted growth of 73.27 billion dollars revenue by 2022. (Statista)

From these populations, samples have to be chosen, given the broad range of devices they provide. For the purpose of this paper, Fitbit has been chosen as a sample for smart wearable devices while Amazon Echo has been chosen as a sample for smart home devices. The choice of sample can be motivated by the popularity of these devices. Amazon maintains dominance in the field of speakers over Google also in 2018, having 71.9% of the market share, with Amazon Echo having hold on 35.8% of this market share. (Kinsella, 2018) Fitbit is also among the dominant smart wearable devices in 2018, having currently 14.8% of the market share, behind only Xiaomi with 16.1%. (Statista) It is therefore of interest to see whether or not these IoT devices respect the privacy of their clients given that they are among the most used products at the moment.

3.2 Research tool

The research will be based on desk research, with information extracted from external sources, such as journals, media and government reports. This thesis aims at separating the information regarding Internet of Things, Marketing and Privacy and give a new perspective, rarely found in literature, with the help of Fitbit and Amazon Echo.

3.3 Analysis

In order to find the appropriate information for this paper, an extensive literature study has been done. The main topics of research have been Internet of Things, Marketing using Internet of Things as well as privacy of IoT. Sources such as journal databases have been used, for example: Scopus, Web of Science and Google Scholar as well as the UT Database, with articles extracted from scientific journals such as Journal of Marketing Management, European Scientific Journal as well as others.

The time frame for the research took place from May 4th 2018 until 22nd of June 2018. As previously mentioned, journal databases were used with articles not older than 2014 in order to account or the novelty of the information. Among the keywords used, worth mentioning are: “IoT”, “Internet of Things”, “Marketing”, “Privacy”, “Architecture”, “Enabling technologies” to name a few.
Combinations of such keywords were used in order to find the necessary articles and afterwards they were filtered out based on years and relevance.

During the literature research, a total of 78 items, comprising mainly of peer reviewed journal articles and conference material have been read and analyzed for valuable information related to the research. Some of these items provided the framework for the theory presented in chapter 2, while others focused mainly on applications such as Fitbit and Amazon Echo, contributing to the results section below. The choice of articles was done on certain criteria. First, the abstract was analyzed for useful information.

If the topic of the article was related to the research, then the article was carefully analyzed and "cherry picking" of useful information took place. The peer reviewed journals were chosen over others due to the fact that the quality of information is more likely to comply with the standards desired for this paper. In case of lack of literature on a certain topic, conference papers as well as websites and blogs were used.

In order to build the theoretical framework presented in Chapter 2, articles were analyzed with regards to information on the following topics: general information about Internet of Things, architecture of Internet of Things, enabling technologies of IoT as well as how they can be used in marketing and the privacy issues they present, classes of IoT applications, current IoT limitations, marketing practices involving IoT, influence on the business methods that IoT brings, privacy issues of architecture of an IoT device, as well as privacy dark side behavior clients may fall for and psychological considerations. The information was easily collected on most topics since they are of interest at the moment in the scientific world. However, multiple sources of information about marketing practices involving IoT were hard to find, so the few existing sources were used for this part of the theoretical framework.

For the results part of the paper, information was collected mainly with regards to Fitbit and Amazon Echo. Specifically, the research was aimed at looking into how these devices worked with the help of their enabling technology, how they are used in marketing as well as privacy issues concerning their architecture, enabling technology and privacy policy. The information with regards to how they are currently used in marketing was particularly hard to find, therefore, sources such as blogs or websites have been used sometimes. Websites have also been used in order to estimate the current market for these devices, as it can be reflected by the reference list. With regards to the privacy policy analysis, it was particularly hard to find information on Amazon Echo since it does not have a privacy policy. Instead, the Alexa Terms of Use were analyzed as well as the general Amazon Privacy Policy.

Analysis will be performed for the two devices at the end of the results section in order to draw the appropriate conclusion. The analysis will consists of comparison of the two devices based on their architecture privacy, enabling technology privacy as well as privacy policy analysis. A "+" will be given to the device that scores best between the two on a certain category and a "-" will be assigned to the device that scores the worst. Furthermore, if a device scores exceptionally better at one of the categories a "++" will be assigned to show that, and, a "--" will be assigned if a device scores particularly bad. Based on the overall score, a conclusion will be drawn.

Chapter 4-Results

4.1 Fitbit

4.1.1 Function of Fibit

The range of Fibit devices, mostly smartwatches, has been brought to the market by the American company Fitbit. The role of these smart devices is to track food intake, therefore calorie count, exercise, heart rate as well as sleeping patterns, leading to an increase in the quality of life of the user. (Weinberg et al., 2015) A Fitbit works due to its 3 axis accelerometer that detects acceleration in any direction, a gyroscope, an altimeter, as well as an orientation sensor and heartbeat sensor. (Fitbit, Sensor guides) Given its use, Fitbit can be placed in the category of smart wearable, as described in section 2.1.4 A.

4.1.2 Enabling technology

Fitbit uses BLE as described in the article by Das et al. (2016) in order to be able to send the information captured by its sensors to the smartphone. The working principles have been described in section 2.1.2.1 on Bluetooth Low Energy.

4.1.3 Architecture

The architecture of the FitBit is similar to the one presented in section 2.1.3. The architecture consists of the device itself (Fitbit), the communication (BLE), the cloud and the presentation and actions (the app).

4.1.4 Market and Marketing practice of Fitbit

The market of wearable devices is one of the most profitable ones at the moment, with the revenue from wearable devices expected to reach 73.72 billion dollars by 2022 (Statista). Moreover, in 2017 Fitbit was one of the top 3 companies with the most units shipped worldwide for wearable, behind only Apple and Xiaomi, with 15.4 million units shipped. (Statista) Fitbit saw a decline in their shipments from 2016, when it was the market leader, way ahead of Apple with 22.5 million units. (Statista). This can be explained by the introduction of Apple of updates to the Apple Watch software as well as their partnership with Nike, for Nike sport bands in the beginning of 2017. With so many units sold worldwide, Fitbit also managed to reach an impressive number of active users, 25.37 millions as of 2017. (Statista)

Fitbit's marketing strategy is mostly based on the behavioral effect social media has over its consumers. Therefore, Fitbit allows for its users to connect with other friends who are also using such smart device, and automatically uploads their achievements for the others to see, resulting in increased motivation. (Hum, 2015; Gastaldi, 2014) Moreover, association between brands such as Fitbit and Adidas in their new collaboration, Fitbit Iconic, may provide both brands with new marketing opportunities. (Fitbit Iconic)

Adidas may benefit from such collaboration by using the gathered data in order to see which clients are most likely to buy their products based on their interest in fitness and athletic performance allowing them to benefit of content marketing. Moreover, such a partnership would also provide Adidas with information into which of their clients buy athletic wear for its purpose, and which buy it for athleisure.

4.1.5 Privacy issues of Bluetooth Low Energy for Fitbit

The privacy issues of the BLE have been described briefly in section 2.3.2.1. Das et al. (2016) identified in their study on fitness trackers, among which Fitbit, several privacy issues within BLE. One of them has been identified as unchanged BLE address, as described in section 2.3.2.1. Given that the fitness tracker and the smartphone connect from time to time in order to exchange data, this leaves the fitness tracker in a disconnected mode where it constantly advertisers its presence. This presence can be picked up by other devices such as beacons. When combined with, for example, video surveillance, this can lead to identification of the individual. Moreover, the intensity of the activity of the user is directly proportional with the amount of traffic exchanged between a smartphone and a fitness tracker. Therefore, by looking at this data, an eavesdropper can figure out whether the subject is running or walking etc.

A device using BLE technology establishes communication in two phases: advertising and data communication. Das et al. (2016) describe that when in advertising mode, the device acts as the "slave" announcing its presence to nearby devices and trying to connect. Once the connection has been established, data communication takes place. Sniffing of devices using BLE can occur when the device is in advertising mode or once the connection has been established. When sniffing such a device, MAC addresses can be collected which are unique to every device. When crossing such information with, for example, video surveillance in a gym, information on the identity of the individual can be obtained.

Moreover, BLE devices such as fitness trackers can help an attacker detect a user's gait and walking speed. Gait is unique for every user, therefore, identification of an individual with very high accuracy is possible from a small group of individuals. (Das et al, 2016)

4.1.6 Privacy issues of Fitbit architecture

As presented in section 2.3.4, the main areas susceptible to an attack in IoT devices are: the device itself, the communication network and the cloud. The issues regarding the privacy issues of the communication network for Fitbit have been described in the previous section, while the privacy issues of the cloud have been presented in section 2.3.2.3. The device itself can present privacy risks due to software and hardware vulnerabilities, which are beyond the purpose of this paper.

4.1.7 Privacy policy analysis of Fitbit

A detailed privacy policy analysis of Fitbit has been performed which can be found in Appendix H. The main issues will be outlined below. The website of Fitbit has been used as a source for the privacy policy analysis.

The focus of the privacy policy analysis was on data collection as well as data sharing. The main issues identified are:

-Once the user connects with third party applications such as Facebook, Google etc, Fitbit can also collect information from these applications. Among the collected data, worth mentioning are email address and friend list. This may result in unwanted ads for the user's friends, and such practice can be qualified as knowledge and intelligence based dark side behavior (see 2.3.5)

-Fitbit gives the option to its users to grant Fitbit access to exercise or activity from another service, failing to specify how such information will be used or why is it needed. Once again, this can be classified as knowledge and intelligence based dark side behavior.

-Fitbit mentions that they do not store payment information, however, they do mention "*Note that third-party payment processors may retain this information in accordance with their own privacy policies and terms*" (Fitbit privacy policy) creating confusion towards who this third-party payment processors are as well as whether or not they can guarantee the privacy of data according to their policies and terms.

-Fitbit mentions that the user can grant access to its location and that such access can be removed at any time. However, they also mention that approximate location of the individual can be derived by the company from IP address. Once again, such practices should be classified as Integrity challenge and manipulative dark side behavior from Fitbit's side, with severe implications in the past. (See Appendix H)

-Fitbit mentions that it can share user's information when given permission to. It is also mentioned that such information could be shared with an employer as part of an employee wellness program. However, usage of such information would be further done based on company's policies and terms. Such data could, in some cases, lead to discrimination in the workplace if disabilities of the employers are revealed.

-Fitbit relies on external processing of their information by other entities for payments, sales, analytics etc. It is mentioned in the privacy policy that the data is processed in compliance with Fitbit's privacy policy as well as any other appropriate confidentiality and security measures, without mentioning which these are. It is also not mentioned if raw or processed data is stored by the above mentioned entities, leading to integrity challenge and manipulative dark side behavior, due to lack of transparency and information.

-Information collected by Fitbit may be shared for legal reasons or to prevent harm. The company is obligated to notify the user of a legal process seeking such information. However, the law can prohibit the company to do so. Therefore, the user would not be aware of such data exchange between company and government until the non-disclosure period expires.

-The privacy policy also addresses the sharing of aggregated and de-identified data with third parties or for public reports. However, there are multiple articles stating that such data can be easily re-identified. (Bailey, 2016). Such practices can be classified as knowledge and intelligence based dark side behavior but also integrity challenge and manipulative dark side behavior.

-Fitbit poses some concerns regarding international operations and data transfers: "*Please note that the countries where we operate may have privacy and data protection laws that differ from, and are potentially less protective than, the laws of your country. You agree to this risk when you create a Fitbit account and click "I agree" to data transfers, irrespective of which country you live in. If you later wish to withdraw your consent, you can delete your Fitbit account." (Fitbit privacy policy)* Therefore, Fitbit mentions that not all countries where the data is shared may have laws as strict as the EU, resulting in potential privacy risks for clients and data misuse. Moreover, clients do not have the possibility to tailor their privacy requirements to their needs, having to opt in to a simple "I agree" and comply with all the company conditions or else refrain from using the device altogether.

4.2 Amazon Echo

4.2.1 Function

Amazon Echo is an example of smart home appliance. Its ability of acting as a personal assistant simply by voice control makes it one of the most looked for appliances in modern homes. Amazon Echo also has the ability to control by Bluetooth other smart devices inside the house, such as locks, lights, smart fridge etc, acting as a control point for the household. Its principle of functioning is briefly described in section 2.1.2.3. The device "wakes up" with the help of a "wake word" set by the user or by the manufacturer. Afterwards, Alexa, the digital assistant greets the user waiting for a command. Given its increased popularity in the past years and given that it has the ability to listen to conversations as well as record them, it is of interest to see how well privacy is respected within Amazon Echo.

4.2.2 Enabling technology

As described in section 2.1.2.8, the enabling technology of Amazon Echo is voice recognition. As a brief overview, the personal assistant captures the command that follows the "wake word" and responds based on the output of the speech recognition software within the cloud.

4.2.3 Architecture

The architecture is similar with the one described in section 2.1.3. The main element of the architecture is the IoT device itself (Amazon Echo), the enabling technology is the voice recognition and all the data is stored and processed in the cloud. However, compared to other IoT devices, the presentation and action function are fulfilled also by the IoT device. Amazon Echo does have an application available through Android Store named Amazon Alexa, but its purpose is to remotely control the device as well as the devices associated with it (lights, locks, thermostats etc). (Amazon)

4.2.4 Marketing practice

Amazon Echo is currently one of the most sought after digital assistants. Amazon Alexa was the most sold Digital assistant in 2017, holding 62% of the Market share. (Statista) It is predicted that by 2020, Amazon Alexa will still be one of the leaders of the market, however, behind Google Assistant. Amazon also shipped approximately 21.7 millions of smart speakers in 2017, more than double compared to its competitor, Google. (Statista)

Companies such as Amazon take advantage of devices such as Amazon Echo to the maximum when it comes about context marketing. Amazon is taking such practices to the next level, intending to improve Alexa, the personal assistant in Amazon Echo, such that it can help customer shop more efficiently. An article in The week presents Amazon's new strategy for advertising through Amazon Echo. Therefore, when users will wish to use Amazon Echo in order to shop by emitting a simple command such as buying soap, Alexa could suggest them a brand, leaving the choice of scent for example to the user. (Lange, 2018). This sort of advertising will make it a lot harder for users to skip through them, compared to mobile or computer. Sometimes, users may even be unaware that certain items are being advertised to them, as they may be seen as simple suggestions made by Alexa. Amazon claims that such suggestions would be made based on the customer's shopping history, but certain brands may have an advantage if they have a partnership with Amazon.

4.2.5 Privacy issues of enabling technology

Once a voice recognition system registers the "wake" word, it will start recording the command from the user. All these voice recordings are further sent to the cloud and stored, with the user having the option to delete them in some cases. However, these pose serious privacy risks due to the fact that they contain identifiable information which could be used to identify the user or to perform perform malicious attacks against the owner. (Chung et al., 2017)

Moreover, even though in the privacy policy of Alexa it is specified that the owner as well as the inhabitants of the household would be able to control the device, there are real-life examples that such devices listen to anyone that mentions the wake word. One such situation took place in San Diego in 2017. Echo owners that were watching the news about a little girl that used her parent's Amazon Echo to order a doll house, found themselves billed also for a pricey dollhouse. The reason was that the news anchor said *"I love the little girl saying 'Alexa ordered me a dollhouse.'"* (Chung, H., Iorga, M., Voas, J., & Lee, S. (2017) Once the Amazon Echo devices present in the houses of those listening to the broadcast heard the wake word, automatically ordered the doll house. (Chung et al., 2017; Pfeifle, 2018)

Given that Alexa does not benefit provide any check-up measures such as voice recognition or parental control, orders are usually immediately processed. (Alepis et al. , 2017) Therefore, given such real life examples the problem of a remote hacker controlling such devices with the help of the wake word is posed.

Devices like Alexa can also connect by Bluetooth to other devices inside the smart home. Given that one device in this network is easily compromised, such as another smart speaker, control can be taken over the Amazon Echo as well. This could result in danger of the individual if, for example, the hacker commands the Amazon Echo to unlock the house doors. (Chung et al., 2017).

Since such devices are always listening, waiting for the wake word, the issue of accidental recording is raised. Moreover, since all such recordings taken by the device are sent to the cloud, the issue of companies having access to private conversations is becoming more of a reality. (Chung at al, 2017). The problem of accidental recording was first brought forward to the general public in 2017 when Arkansas Police asked Amazon to turn in the data from a certain Amazon Echo present at a murder scene, in hopes that it may contain valuable information. (Pfeifle, 2018)

4.2.6 Privacy issues of architecture

As described in section 2.3.4, the main areas where an attack can occur are the device, the enabling technology communication network or the cloud. The issues of the enabling technology have been described in the previous section, while the issues of the cloud have been described in section 2.3.2.3. The device itself can pose privacy concerns due to software and hardware vulnerabilities that are, however, beyond the purpose of this paper.

4.2.7 Privacy policy analysis

A privacy policy analysis was intended to be performed. However, upon looking up in Google Search “Amazon Echo privacy policy”, no results come up. Instead, the page of Alexa Terms of Use is the only relevant page that shows up, that also directs the user towards the general Amazon Privacy policy page.

So, the Amazon Echo itself has no dedicated page with regards to privacy policy. Moreover, the last update on Amazon’s privacy policy is 29th of August, 2017, with the GDPR taking action in the European space in May, 2018. Alexa’s Terms of Use were used as a source for the information found below.

The following terms in the Alexa’s terms of use drew attention:

-Amazon Echo also allows Alexa to perform voice purchases and to make donations to charities by using only voice. Even though this can be seen as a handy feature of the device, this exposes the user to big financial risks in case the device is hacked. There are instances in literature when such devices have been hacked, with the adversary issuing his requests via a headset. (Alepis, 2017)

-Amazon mentions that information regarding how the user interacts with Alexa, how the device is used, about the Alexa enabled products as well as auxiliary products will be provided to Amazon through the Amazon Software and that all the collected data may be stored on servers outside of the country of origin of the data. However, Amazon fails to mention if the laws of the country of origin apply for the protection of the respective data or the laws of the country where the data is stored. Such an aspect would be of particular importance to clients from Europe that benefit from GDPR as well as more strict laws regarding data privacy compared to other areas.

-One of the most worrying features of Alexa is the drop-in function. It allows previously allowed users to “drop-in” without the recipient being required to give their consent and accept the drop-in. Such drop in consists of video calls that can be seen as an invasion of privacy, especially if the recipient is not aware of it or is caught in an embarrassing situation.

Amazon mentions that if permission is granted to someone from a household to drop in, then everyone in the respective household would be able to drop in at any time, unannounced.

Amazon's privacy policy has not been included since most of its terms refer to data collection as well as data sharing in the context of the Amazon Website, not Alexa. However, a detailed analysis of this privacy policy can be found in Appendix H, along with the detailed analysis of Alexa's Terms of use.

4.3 Comparison of the devices:

Upon comparison of the two applications and their issues, it can be easily seen that higher popularity among users and higher sales does not mean appropriate privacy protection. When comparing the two enabling technologies, Voice recognition is definitely more vulnerable from the point of view of privacy. Bluetooth Low Energy connection can also be sniffed, resulting in personal information leakage, however, the consequences are a lot worse in the case of Voice Recognition.

Moreover, the Voice recognition system does not particularly require a lot of skill to control, since simple mention of the wake word can trigger an action.

From the point of view of architecture, once again, Amazon Echo is more vulnerable. Both devices can have privacy issues with regards to the device itself or to the cloud, but the proeminent privacy issues of the communication network (voice recognition) in the case of Amazon Echo cannot be overlooked.

Upon comparison between the two privacy policies of the devices, Fitbit uses a less vague language and benefits of a privacy policy tailored to the device. Amazon, on the other hand, has no privacy policy tailored for Amazon' Echo Alexa, and the last update of the general Amazon privacy policy is 29th of August 2017. This means that the privacy policy may not be compliant with the current GDPR that got into effect in May, 2018.

Within Fitbit privacy policy, the most worrying findings are the following:

- Fitbit can still detect user's location without his/her consent using IP address of the device
- Privacy and data protection laws of the countries where Fitbit data is shared may be less protective than those of the country of origin of the data

Within Amazon' privacy policy and Alexa's terms of use policies, the most worrying findings are:

-drop-in function of Alexa can be classified as an invasion of privacy for its users, but it can be classified as a failure to provide privacy by design rather than a failure from Amazon's side to provide data privacy of their clients.

-Amazon does not mention if the data provided by the Amazon Software stored in servers outside of the country of origin will comply to the privacy policies of the country of origin or not

-Amazon does not have, in fact, a privacy policy for Alexa and the Amazon privacy policy mostly addresses the Amazon Website.

When comparing the market as well as the marketing strategies of the two companies, Amazon is ahead of Fitbit regarding units sold and market share, which means that despite the privacy issues of the technology, more and more users decide to go for smart devices such as Amazon Echo.

Below, an overview will be given on the above presented aspects on privacy. The comparison will be made between the two devices, where a "+" will mean that the respective device scores better concerning a certain aspect and the "-" meaning that the respective device scores worse, compared to the other one.

	Fitbit	Amazon Echo
Enabling technology privacy	+	-
Architecture privacy	+	-
Privacy policy analysis	++	--*
Overall score	+	-

Table 1: Overview of strengths and weaknesses

*Amazon Echo scores worse concerning privacy policy analysis, due to the fact that it lacks one. In contrast, Fitbit scores a lot better by promoting transparency and by having a privacy policy to begin with.

Chapter 5-Conclusion

5.1 Summary of findings

Following the literature review, it can be concluded that there is a consensus in the research world regarding the potential disruptive impact of the IoT technology. Moreover, many researchers agree that privacy will be one of the main elements to make a difference in the adoption of the technology as well as turning it from a potentially disruptive technology to a potentially enabling technology. Scientists also agree that this issue should be paid particular attention to in today's smart devices, due to the fact that many companies producing them have little experience in privacy and security of data.

Little research has been made on the impact Internet of Things can have in marketing due to the novelty of the concept. However, researchers agree that Internet of Things can have a great impact on marketing, changing business models as well as business methods of companies and that privacy will play a big role in this environment in order to ensure company survival. With the customers having a powerful voice in today's connected world, aspects such as the respect towards privacy of the client and transparency will become key elements in building the brand and establishing a long term relationship with the client.

Examples have been used to represent two main categories of popular applications, namely Smart home and Wearable. Therefore, two of the most popular smart devices at the moment have been chosen to represent them, Amazon Echo and Fitbit. The findings showed that both devices have privacy flaws within their enabling technology and, therefore, within their architecture. However, Fitbit's Bluetooth Low Energy requires more knowledge concerning data leakage, compared to Amazon's Echo where the wake word is enough to interact with the device.

Concerning privacy policy analysis, issues have been identified within Fitbit with regards to the privacy of location of the user as well as data storage regulations outside of the country of origin of data. Amazon's Echo on the other hand, did not benefit from a privacy policy at all. In case the user wishes to see what type of data is collected and for what purpose, the general Amazon privacy policy has to be looked into. Even then, it is unclear which terms will apply to Alexa since most of the Amazon privacy policy seems to be addressed to the Amazon Website.

5.2 Research question answer

In the light of the findings presented above, a conclusion can be drawn. To what extent is privacy respected in marketing involving Internet of Things?

Privacy is respected by certain devices using Internet of Things, one example being Fitbit. Even though privacy issues may be encountered within the technology and even though certain ambiguous terms have been found in the privacy policy, Fitbit manages to respect the privacy of their customers. They promote transparency, their privacy policy is up to date following the GDPR and therefore compliant.

Compared to Fitbit, Amazon Echo encounters more issues with the enabling technology and the main downside is the complete absence of a privacy policy tailored to this device. The difference between the two devices concerning privacy can also be reflected by media, with Amazon Echo being involved in certain scandals involving information leakage. Moreover, considering the fact that Amazon Echo deals with sensitive, day to day information that is identifiable, it was expected to benefit from a complete and transparent privacy policy.

Comparing how these two devices are also used in marketing, Amazon appears to take advantage in a negative way of the many functionalities of Alexa, instructing the device to make certain recommendations concerning purchases that may sometimes be directed towards companies that partner with Amazon.

Therefore, it can be concluded that smart wearables manage to respect the privacy of their users a lot better while also being more transparent in their use in marketing. On the other hand, smart home devices, in spite of dealing with a lot more sensitive information, fail to adequately respect the privacy of their clients while also being more stealth with regards to how they are used in marketing.

Considering that the findings cannot be generalized to all Internet of Things devices, the answer to the research question has been given based on these two devices and, implicitly, extended to the populations they represent.

Chapter 6-Discussion

a. Contributions

i.Science

As previously mentioned, privacy has been identified as a research gap in multiple articles found in literature. This paper manages to not only narrow this gap but also takes on a new approach on privacy in the context of Internet of Things and its use in Marketing. Moreover, this paper manages to present IoT, privacy and marketing as individual principles, but also emphasizes the connections between them and how they can influence each other by providing a rich insight in the theoretical framework behind them, resulting in a one of a kind study. Such research, where all three concepts are brought together is rarely found in literature. The impact these three principles have on real-life markets and products is presented using as examples new products such as Fitbit and Amazon Echo.

ii. Practice

Given that real life devices have been analyzed, the contribution to practice is of great importance. Privacy issues have been encountered in particular with Amazon Echo, which may lead to leakage of sensitive information of customers but also confusion of customers from Amazon's side. Fitbit has also been found to have certain privacy issues, however, the company is a lot more transparent in their intentions and how such issues would be handled. The information presented on these two devices can offer great insight to existing and potential customers as well as to the manufacturers on the privacy issues.

b. Limitations

One of the main limitations was, at time, the lack of peer reviewed journals tailored to the necessary information. In such cases information from blogs or websites have been used. Moreover, time constraint was also a limitation, whose solution was to perform desk research on the topics of the assignment.

c. Future research

In order to gain a more broad perspective over the impact IoT, privacy and marketing have over each other, an analysis on more devices should be performed. Preferably, the devices should belong to the categories of applications identified in Appendix C. Moreover, for further research, it is of interest to perform a quantitative study for these devices in order to see how their owners perceive their privacy as well as their perceived use in marketing. Finally, an investigation could be made on how the privacy issues of Amazon Echo and Fitbit affected the companies in the past years and how it impacted their marketing strategy in order to ensure survival of the company.

Chapter 7-Acknowledgments

I would like to express my gratitude to my supervisor, Dr. Martin Stienstra, for guiding me throughout this process and offering me his support. Without his guidance, this thesis would not have been possible. Moreover, I would also like to thank Dr. Efthymios Constantinides for giving me the base idea for this work as well as offering me supporting material in the beginning of the assignment.

References:

1. Keefer, A., & Baiget, T. (2001). How it all began: A brief history of the Internet, *Vine,31*(3), 90-95. doi:10.1108/03055720010804221

2. Naughton, J. (2016). The evolution of the Internet: From military experiment to General Purpose Technology*Journal of Cyber Policy,1*(1), 5-28. doi:10.1080/23738871.2016.1157619

3. Mattern, F., & Floerkemeier, C. (2010). From the Internet of Computers to the Internet of Things, *Lecture Notes in Computer Science From Active Data Management to Event-Based Systems and More,* 242-259. doi:10.1007/978-3-642-17226-7_15

4. Lamkin, P. (2017, June 22). Wearable Tech Market To Double By 2021. Retrieved from https://www.forbes.com/sites/paullamkin/2017/06/22/wearable-tech-market-to-double-by-2021/#79358372d8f3

5. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons,58*(4), 431-440. doi:10.1016/j.bushor.2015.03.008

6. Tsai, Y., Wang, S., Yan, K., & Chang, C. (2017). Precise Positioning of Marketing and Behavior Intentions of Location-Based Mobile Commerce in the Internet of Things. *Symmetry, 9*(8), 139. doi:10.3390/sym9080139

7. Peppet, Scott R., Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent (March 1, 2014). Texas Law Review, Forthcoming.

8. Atzori, L., Iera, A., Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*, 2787-2805, doi:10.1007/978-1-4419-1674-7

9. Research paper by Policy and Research Group of the Office of the Privacy Commissioner of Canada, February, 2016. The Internet of Things: And introduction to privacy issues with a focus on the retail and home environments.

10. Regalado, A. (2014). GE's 1 Billion dollar Software Bet. *MIT Technology Review*, July/August 2014

11. Perera, C., Liu, C. H., & Jayawardena, S. (2015). The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey.*IEEE Transactions on Emerging Topics in Computing,3*(4), 585-598. doi:10.1109/tetc.2015.2390034

12. Jim Chase (2013). The Evolution of the Internet of Things. *Texas Instruments*

13. Whitmore, A., Agarwal, A., Xu, L.D. (2014). The Internet of Things-A survey of topics and trends. *Inf Syst Front, 17*, 264-274, doi: 10.1007/s10796-014-9489-2

14. GSM Association, (2014). Understanding the IoT

15. Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm.*Ad Hoc Networks,56*, 122-140. doi:10.1016/j.adhoc.2016.12.004

16. Navani, D., Jain, S., & Nehra, M. S. (2017). The Internet of Things (IoT): A Study of Architectural Elements.*2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*. doi:10.1109/sitis.2017.83

17. Al-Fuqaha, A., Guizani, M., Mohammadi, M, Aledhari, M., Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, I*EEE Communication Surveys&Tutorials, 17(4),* 2347-2376, doi: 10.1109/COMST.2015.2444095

18. Cranshaw, J., Schwartz, R., Hong, J.I, Sadeh, N. (2012). The Livehoods Project: Utilizing Social Media to Understand the Dynamics of a City. *School of Computer Science, Carnegie Mellon University*

19. Pfeifle, A. (2018) Alexa, what should we do about privacy? Protecting privacy for users of voice-activated devices. *Washington Law Review, 93(1)*, 421-458

20. How does my Fitbit device calculate my daily activity? (n.d.). Retrieved from https://help.fitbit.com/articles/en_US/Help_article/1141

21. Papakostas, N., Oconnor, J., & Byrne, G. (2016). Internet of things technologies in manufacturing: Application areas, challenges and outlook.*2016 International Conference on Information Society (i-Society)*. doi:10.1109/i-society.2016.7854194

22. Domingo, M. C. (2012). An overview of the Internet of Things for people with disabilities.*Journal of Network and Computer Applications,35*(2), 584-596. doi:10.1016/j.jnca.2011.10.015

23. Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012). RFID technology and its applications in Internet of Things (IoT).*2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*. doi:10.1109/cecnet.2012.6201508

24. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges.*2012 10th International Conference on Frontiers of Information Technology*. doi:10.1109/fit.2012.53

25. Choudhary, G., & Jain, A. (2016). Internet of Things: A survey on architecture, technologies, protocols and challenges.*2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*. doi:10.1109/icraie.2016.7939537

26. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal,4*(5), 1125-1142. doi:10.1109/jiot.2017.2683200

27. Nowodzinski, P, Lukasik, K., Puto, A. (May, 2016) Internet Of Things (Iot) In A Retail Environment. The New Strategy For Firm's Development, *European Scientific Journal,* ISSN: 1857-7431

28. Tsai, Y., Wang, S., Yan, K., & Chang, C. (2017). Precise Positioning of Marketing and Behavior Intentions of Location-Based Mobile Commerce in the Internet of Things.*Symmetry 9*(8), 139. doi:10.3390/sym9080139

29. Claveria, K. (2017, April 28). 13 stunning stats on the Internet of Things. Retrieved from https://www.visioncritical.com/internet-of-things-stats/

30. Pulizzi, J. (2016, March 12) Content Marketing Definition. Retrieved from https://contentmarketinginstitute.com/what-is-content-marketing/

31. Spilotro, Chloe E., "Connecting the Dots: How IoT is Going to Revolutionize the Digital Marketing Landscape for Millennials" (2016).Undergraduate Honors Theses. 25.
http://digital.sandiego.edu/honors_theses/25

32. Chung, H., Iorga, M., Voas, J., & Lee, S. (2017). "Alexa, Can I Trust You?".*Computer,50*(9), 100-104. doi:10.1109/mc.2017.3571053

33. Perera, C., Liu, C. H., Jayawardena, S., & Chen, M. (2014). A Survey on Internet of Things From Industrial Market Perspective.*IEEE Access,2*, 1660-1679. doi:10.1109/access.2015.2389854

34. Jian, A., Xiaolin, G., Jianwei, Y., Yu, S., & Xin, H. (2015). Mobile Crowd Sensing for Internet of Things: A Credible Crowdsourcing Model in Mobile-Sense Service.*2015 IEEE International Conference on Multimedia Big Data*. doi:10.1109/bigmm.2015.62

35. Tsai, Y., Wang, S., Yan, K., & Chang, C. (2017). Precise Positioning of Marketing and Behavior Intentions of Location-Based Mobile Commerce in the Internet of Things.*Symmetry,9*(8), 139. doi:10.3390/sym9080139

36. Margulis, A., Boeck, H., Bendavid, Y., & Durif, F. (2016). Building theory from consumer reactions to RFID: Discovering Connective Proximity. *Ethics and Information Technology,18*(2), 81-101. doi:10.1007/s10676-016-9388-y

37. Hemmati, M. (2016). Analyzing the Effect of Social Internet of Things on Making the Internet Marketing Smart.*Modern Applied Science,10*(9), 213. doi:10.5539/mas.v10n9p213

38. Milley, P. (September, 2014). Privacy and the Internet of Things, *(GSEC) Gold Certification*

39. Maras, M-H. (May, 2015). Internet of things: security and privacy implications, *International Data Privacy Law, 5 (2)*, doi: 10.1093/idpl/ipv004

40.Bailey, M. (Apr 2016). Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things, *Texas Law Review*, Vol. 94 (5)

41. Office of the Privacy Commissioner of Canada. (February 2016) The Internet of Things An introduction to privacy issues with a focus on the retail and home environments

42. Das, A. K., Pathak, P. H., Chuah, C., & Mohapatra, P. (2016). Uncovering Privacy Leakage in BLE Network Traffic of Wearable Fitness Trackers.*Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications - HotMobile 16*. doi:10.1145/2873587.2873594

43. Winter, J. S. (2013). Surveillance in ubiquitous network societies: Normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things.*Ethics and Information Technology,16*(1), 27-41. doi:10.1007/s10676-013-9332-3

44. Global intelligent assistant market share 2017-2020 | Statistic. Retrieved from https://www.statista.com/statistics/789633/worldwide-digital-assistant-market-share/

45. Smart speaker shipment worldwide by vendor 2016 and 2017 | Statistic. Retrieved from https://www.statista.com/statistics/796349/worldwide-smart-speaker-shipment-by-vendor/

46. Bhattarai, S., & Wang, Y. (2018). End-to-End Trust and Security for Internet of Things Applications.*Computer,51*(4), 20-27. doi:10.1109/mc.2018.2141038

47. Cremer, D. D., Nguyen, B., & Simkin, L. (2016). The integrity challenge of the Internet-of-Things (IoT): On understanding its dark side.*Journal of Marketing Management,33*(1-2), 145-158. doi:10.1080/0267257x.2016.1247517

48. Emiami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L.F., Sadeh, N. (2017). Privacy Expectations and Preferences in an IoT World, *Thirteenth Symposium of Usable Privacy and Security*

49. Forecast: US smart home devices and smart speaker ownership 2022 | Statistic. (n.d.). Retrieved from https://www.statista.com/statistics/794624/us-smart-home-devices-smart-speaker-ownership-forecast/

50. Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy.*Business Horizons,58*(6), 615-624. doi:10.1016/j.bushor.2015.06.005

51. Perera, C., Ranjan, R., & Wang, L. (2015). End-to-End Privacy for Open Big Data Markets.*IEEE Cloud Computing,2*(4), 44-53. doi:10.1109/mcc.2015.78

52. Use of Internet of Things (IoT) in Healthcare : A Survey Mrs. Anjali S. Yeole, Dr. D. R. Kalbande, 2016

53. Botta,A., de Donato, W., Persico, V., Pescapé, A. (2016). Integration of Cloud computing and Internet of Things: A survey, *Future Generation Computer Systems, 56*, 684-700, https://doi.org/10.1016/j.future.2015.09.021

54. Lueth, K.L. (2015, February 4). The 10 most popular Internet of Things applications right now. Retrieved from: https://www.linkedin.com/pulse/10-most-popular-internet-things-applications-right-now-lueth/

55. Hum, S., (2015, August 1). How Fitbit Grew To Become the Best-selling Fitness Tracker in 5 Years. Retrieved from https://www.referralcandy.com/blog/fitbit-marketing-strategy/

56. Sensor Guides. (n.d.). Retrieved from https://dev.fitbit.com/build/guides/sensors/

57. Fitbit Ionic: Adidas edition. (n.d.). Retrieved from https://www.fitbit.com/nl/shop/adidas

58. Mangan, D. (2016, January 08). Fitbit gets hit: Accounts attacked by hackers. Retrieved from https://www.cnbc.com/2016/01/08/theres-a-hack-for-that-fitbit-user-accounts-attacked.html

59. McGee, M.K. (2016, January 11). Fitbit Hack: What Are the Lessons? Retrieved from https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793

60. Gastaldi, M. (2014). Integration of mobile, big data, sensors, and social media: Impact on daily life and business.*2014 IST-Africa Conference Proceedings*. doi:10.1109/istafrica.2014.6880670

61. Johnson, B. (2016, November 16). How Amazon Echo Works. Retrieved from https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/amazon-echo.htm

62. Lange, J. (2018, January 2). Amazon is exploring how to turn the Echo into a Trojan horse for advertisers. Retrieved from https://theweek.com/speedreads/746201/amazon-exploring-how-turn-echo-into-trojan-horse-advertisers

63. Amazon Alexa: Appstore for Android. (n.d.). Retrieved from https://www.amazon.com/Amazon-com-Amazon-Alexa/dp/B00P03D4D2

64. Alepis, E., & Patsakis, C. (2017). Monkey Says, Monkey Does: Security and Privacy on Voice Assistants. *IEEE Access,5*, 17841-17851. doi:10.1109/access.2017.2747626

65. Stankovic, J. A. (2014). Research Directions for the Internet of Things. *IEEE Internet of Things Journal,1*(1), 3-9. doi:10.1109/jiot.2014.2312291

66. Da Xu, L., He, W., Li, S. (November, 2014). Internet of Things in Industries: A Survey, *IEEE Transactions on industrial informatics,* 10 (4), 2233-2243

67. Van, H.P. (2014, December 4). New Report Shows The Global Smart Home Market is currently growing 95%, Driven By Voice-enabled Home Gateways and New Smart Appliances. Retrieved from https://iot-analytics.com/new-report-shows-11-4-billion-global-smart-home-market-currently-growing-95-driven-voice-enabled-home-gateways-new-smart-appliances/, 2017

68. Wearables market share companies 2014-2018 | Statistic. (n.d.). Retrieved from https://www.statista.com/statistics/435944/quarterly-wearables-shipments-worldwide-market-share-by-vendor/

69. Kinsella, B. (2018, March 08). Amazon Echo Maintains Large Market Share Lead in U.S. Smart Speaker User Base. Retrieved from https://voicebot.ai/2018/03/08/amazon-echo-maintains-large-market-share-lead-u-s-smart-speaker-user-base/

70. Capellupo, M., Liranzo, J., Bhuiyan, M. Z., Hayajneh, T., & Wang, G. (2017). Security and Attack Vector Analysis of IoT Devices.*Security, Privacy, and Anonymity in Computation, Communication, and Storage Lecture Notes in Computer Science,*593-606. doi:10.1007/978-3-319-72395-2_54

71. Wueest, C. (November, 2017). A guide to the security of voice-activated smart speakers. *ISTR Special Report*

72. Wearable device revenue worldwide 2016-2022 | Statistic. (n.d.). Retrieved from https://www.statista.com/statistics/610447/wearable-device-revenue-worldwide/

73. Wearable sales by vendor (Apple, Samsung etc.) 2014-2017 | Statistic. (n.d.). Retrieved from https://www.statista.com/statistics/515634/wearables-shipments-worldwide-by-vendor/

74. Fitbit active users 2012-2017 | Statistic. (n.d.). Retrieved from https://www.statista.com/statistics/472600/fitbit-active-users/

75. Fitbit Privacy Policy. Retrieved from https://www.fitbit.com/legal/privacy-policy

Annexes:

Appendix A:

Architecture:

Multiple different architectures have been proposed throughout the years for IoT, the most extensive overview over the different types of architecture being provided by Al-Fuqaha et al (2015). In most literature, however, two types of architecture are encountered more often. The 3 layer architecture and the 5 layer architecture. The latter evolved from the first one, following evolution of both Internet and Internet of Things applications in order to ensure security, privacy and so on.

The 3 layer architecture has the following components: Perception layer, Network Layer as well as Application layer.

The Perception layer refers to the sensors/WSN/camera/GPS as well as others, embedded in IoT devices that "percep" the environment and collect information. (Jia et al, 2012)

The Network layer refers to the underlying technology that allows transmission of the information collected from sensors to the application layer. (Al-Fuqaha et al, 2015)

The Application layer refers to the processing of information received from sensors and providing service to users based on the received and processed information. (ex: sensors detect temperature reached a certain value, application layer decides to turn off heating). (Navani et al., 2017; Al-Fuqaha et al. 2015; Domingo, 2011)

The 5 layer architecture is similar, having the following components, as extracted from Al-Fuqaha et al. (2015): Objects layer, Object Abstraction Layer, Middleware layer, Application Layer and Business Layer. (Khan et al. 2012;)

The Object layer can be considered the analog of Perception Layer from the 3 layer architecture described above. It consists of sensors as well as other systems capable of collecting the information from devices and from environment.

The Object Abstraction Layer can be considered the analog of the Network Layer from the 3 layer architecture. It carries the information that results from the Object Layer to the Middleware Layer, using technologies such as Bluetooth, Wifi, RFID etc.

The Middleware Layer has the ability to process the information received from the sensors, store it and take a decision based on the previously analyzed information.

The Application Layer is responsible for providing the service that corresponds to the request.

The Business Layer is in charge of monitoring the other processes from the 5 layer architecture as well as analyzing the Big Data for service and products improvement. (Al-Fuqaha et al., 2015)

Appendix B:

2.1.2.1 Radio frequency identification (RFID)

RFID is regarded as one of the founding technologies of Internet of Things. The RFID system is relatively simple, consisting of a tag and a reader. The communication between the two elements is done through radio waves. There are three kinds of tags:

-passive: not battery powered and function due to radio frequency energy sent from the reader; used for storing identifying code (Lee, Lee, 2015)

-semi-passive: the microchip is powered by battery yet transmission is done by radio frequency energy sent from the reader (Lee, Lee, 2015)

-active: microchip is powered by battery yet they can communicate with a reader without requiring power from it but from a battery supply. These are the tags usually used in IoT applications such as healthcare, temperature monitoring etc. (Lee, Lee 2015)

2.1.2.2 Wireless sensor network (WSN)

Wireless sensor networks consists of networks of smart devices equipped with sensors, usually dedicated for monitoring of environmental conditions (temperature, pressure etc) as well as physical conditions (usually used for preventive maintenance). (Lee, Lee, 2015)WSN is considered superior to other technologies such as RFID due to the fact that its sensors gather more information and they are intelligent compared to the RFID tags. Moreover, in the case of RFID, proximity or line of sight are required in order for the information to be transmitted and this is not the case for WSN (Choudhary, Jain, 2016)

2.1.2.3 Sensors

Sensors are without doubt the most important part in the IoT technology, having the ability to gather data and convert it into electrical signal. Choudary and Jain (2016) give a classification on sensors regarding the type of data they gather. (Choudhary, Jain, 2016)

2.1.2.4 Big Data

Given the big number of devices and applications that use IoT, the amount of data generated by these is huge. This data is also known as big data. The analysis of this "big data" is of great interest for businesses around the world given the knowledge it contains and, therefore, the competitive advantage it gives to companies. However, given the huge amount of data and limited space to store it, companies start taking into account keeping relevant data only or deleting data that exceeds a certain amount of time. (Al-Fuqaha et al., 2015) All of the data that humans produce in the online environment (e-mails, conversations, social media posts, surveillance footage) is stored, sometimes indefinitely. Some examples of big data usage is given by supermarkets that combine their fidelity card data with the social media data of the customer in order to gain a leverage in the buying patterns. (Gastaldi et al. 2014)

2.1.2.5 Middleware

Middleware provides standard interfaces that allows developers to overlook the problem of compatibility of infrastructures when developing an application. Through usage of middleware, applications and devices that have different interfaces can share and exchange information with one another. Middleware can support many applications, operating systems and platforms. All of these qualities make it a key component in the development and further adoption of IoT solutions, as it is discussed in section 2.1.5 on limitations. (Lin et al., 2017)

Appendix C:

C) Smart city

Given the growing population and the amount of resources cities hold, a great deal of attention has been given recently to the idea of smart city. Resource management, quality of life of inhabitants as well as traffic management are some of the aspects researchers tend to look into in their quest for a smart city.

D) Smart Environment

Smart Environment applications refer to monitoring of areas such as : air quality, water, natural disaster as well as farming.

E) Smart Enterprise

IoT has long been known to be a solution in supply chain management systems, but it can also be used in Infrastructure, Safety, Energy, and Resource Management.

F) Healthcare

IoT is revolutionizing the healthcare domain with smart applications that track patients even from miles away, deliver their medication in the appropriate quantities at the right time and register any subtle changes in their body.

Appendix E:

2.2.2.1 RFID

The technology behind RFID has been described Appendix B. Now, the usefulness of it in marketing as well as examples will be provided. Margulis et al. (2016) offer a broad perspective over RFID as a technology as well as its use in marketing. Some of the most important aspects extracted from their article will be presented below.

RFID has recently been brought into the spotlight as another method of tracking customers inside the store. However, this assumes that either the client is carrying the RFID tag or that it is embedded in products. Ethical implications of this technology are brought into question given that clients may not be aware they are being tracked in the case in which the tag is embedded in products and the tag is uniquely identifiable. Such RFID system has been used by companies such as Tampa Bay. RFID tags were sewn into jerseys for the customers that purchased season passes. Such tags were used to offer them discounts at the stadium's concession stand. In this case, the RFID tag was used to provide rewards for the clients.

Another example has been provided by Disneyland USA. Visitors were offered bracelets with an integrated RFID tag that allowed tracking of customers such that they can pinpoint their location as well as to determine the location of children for child safety. In this case, the RFID tag was used for customer tracking. This practice might have also offered information to Disneyland about the track customers tend to take in the adventure park as well as time spent in certain exhibitions.

RFID tags can also be used in the context of social media advertisment. Customers at Sunglass Hut were provided with wristbands with an integrated RFID tag that allowed the clients to try on items and share their pictures on social media. Such practice can be seen as a marketing campaign "under disguise" for Sunglass Hut.

RFID tags have also been used for information broadcasting. In 2006 Prada attached RFID tags to items that allowed the customers to get information on the chosen item and suggestions for similar products. This practice allowed Prada to assess the interest in different products as well as the customer behavior.

In Japan, McDonald's allowed payment with the mobile phone using RFID systems once clients set up their electronic wallet online. In this case, the RFID tag has been used as a payment method.
RFID tags have also been used as identification method by a Highschool in San Antonio that allowed students to identify themselves with cards equipped with RFID tag upon hischool entrance. (Margulis et al., 2016)

2.2.2.3 Wi-fi

Wi-Fi can be considered another useful application in the domain of IoT marketing. When a device has wi-fi turned on, it is continuously looking for a network to connect to. Therefore, if a store has an open wi-fi network that smartphones can connect to, their MAC address can be captured, giving insight into how many people are in the store. (Office of the Privacy Comissioner of Canada, 2016)

Appendix F:

RFID:

Main problems regarding RFID technology are authentication and data integrity. Given that RFID are small devices, usually passive, they do not have the computational power to support complex authentication measures. Therefore, cases such as the one presented by Atzori et al. can occur. The author describes how an attack such as man-in-the-middle can occur.

Moreover, since RFID systems are usually left unattended, data integrity can be compromised. Therefore, an adversary could potentially modify the data in a transaction without the system's knowledge, while data traverses the network. (Atzori et al., 2010)

Appendix G:

Examples of IoT failure towards privacy from literature:

An example of privacy issue took place in 2015 when Lenovo, one of the biggest computer manufacturers on the market, sold computers with a preloaded software that was able to track users' movements without their consent or knowledge.

An example of Data misuse was given by a Breathometer that sold a breathalyzer, without telling their customers that all the data will be stored indefinitely in the cloud and that it could be user against them in case of a trial.

An example of financial penalty dark behavior was given by an car insurance company that insisted on their clients to use a car-plug in that would track their driving data in order to calculate an insurance premium.

FitBit took the decision to sell employees data to employers, with the aim of offering incentives to those that do participate. However, there were cases in which health conditions, pregnancies etc were revealed to the employer with some employees being fired due to a smoking ban.

These are some of the examples presented by Bailey that reflect the reality behind the industry's dark behavior towards IoT.

However, these devices are not only susceptible to dark practices by companies and manufacturers. They are also susceptible to hackers. A couple in Houston heard a voice inside their baby's room in 2013. When entering the room, they realized the voice was coming from their baby's monitor and the hacker started cursing them. (Peppet, 2013)

Moreover, the website Shodan contains a database of surveillance camera from all over the world that do not have proper authentification enabled or the users stick to the standard passwords and admin names, making it easy for hackers to guess them.

There is an increased concern towards IoT device in healthcare. Many of these devices do not have enough authentication and security measures due to the fact that they have to be easy and fast to use by hospital personnel or patients. However, in the case in which such a device would be hacked, the consequences could be fatal. (Peppet, 2013)

Appendix H:
Fitbit privacy policy analysis:

A critical analysis of the privacy policy of Fibit will be performed, with a focus on data collection and data sharing. Also, implications for the clients will be approximated based on similar cases or findings from literature as well as the possible dark side behaviors the company may engage in.

Fitbit collects information from third party companies, given that the user has chosen to connect to one of these services, such as Google or Facebook. Therefore, Fitbit may receive information stored in these profiles, such as profile picture, age range, email address and friend list. Given that Fitbit collects some of the above mentioned information when creating an account, the only problem is left with the access to the email address and friend list. These channels may be used for marketing by Fitbit without the user's knowledge. This can be qualified as a dark side behavior for Fitbit if used as such, pointing towards the knowledge and intelligence based dark side behavior, as described in section 2.3.6. This could lead to clients exposing more than they would wish for, and resulting in unwanted advertisements for them and their friends.

Moreover, Fitbit mentions that the user can choose to grant access to Fitbit to exercise or activity data from another service, failing to specify to what use such information would be to the company, pointing once again towards knowledge and intelligence based dark side behavior.

In their "Payment and card information" section of the privacy policy, Fitbit mentions that they do not store payment information, only shipping address for order fulfillment. However, this is followed by "*Note that third-party payment processors may retain this information in accordance with their own privacy policies and terms*" (Fitbit privacy policy) creating confusion for a potential customer with regards to who the third party payment processor is and also how this sensitive data will be used later on according to their privacy policies and terms.

Fitbit mentions that they use precise location data such as "*Wi-Fi access points, GPS signals, cell tower IDs"*. (Fitbit privacy policy) Access is granted by the user and can be removed at anytime. However, it is also mentioned that Fitbit can derive approximate location from IP addresses. Once again, it is unclear if this is done with or without the user's consent and if the user can opt out of complete location tracking. Such practices can be classified as Integrity challenge and manipulative dark-side behavior for Fitbit with great implications for the privacy of their users. In 2016, many Fitbit users have been victims of hacking due to leacked passwords and email addresses from third party sites, with the hackers gaining access into the GPS history of the Fitbit user. This provided the hackers with great insight into where the users usually run or cycle as well as what time they usually go to sleep. (Mangan, 2016; McGee, 2016)

Information sharing

Fitbit shares information of its users when agreed or given access to do as such. Therefore, it can share information with a third party application, provided that the user gave it access to his/her account as well as with an employer for an employee wellness program. Further on, it is mentioned that, for the latter, the usage of information will be done based on their privacy policy and terms. Employers may sometimes engage in dark side behavior and discriminate based on such data. As Bailey (2016) points out, such data has the risk of revealing disabilities, pregnancies etc that may not have been known to the employer beforehand and may result in increased health insurance costs for the employee. There is even the possibility that employees may end up fired due to undisclosed disabilities (Bailey, 2016).

Moreover, information revealed by a Fitbit such as inability to delay gratification and impulsivity could show the potential of an employee to indulge in alcohol and drug abuse, smoking, debt, etc. Lack of sleep which is tracked by Fitbit has been linked to a poor psychological well being, health problems, and negative emotions. (Peppet, Scott, 2014)
Users can, however, revoke at anytime the consent to third party applications or employee wellness program.

Fitbit also relies on external processing of their information by corporate affiliates, service providers and partners for customer support, information technology, payment, sales, marketing data analysis, research and surveys. However, Fitbit fails to mention if the raw or processed data are stored or used later on by these entities. Such behavior can fall under the integrity challenge and manipulative dark side behavior, given the lack of information and transparency.

Fitbit mentions that they also share information collected by their devices for legal reasons or to prevent harm. Such information could be disclosed in order to "*comply with a law, regulation, legal process or governmental request*". Fitbit is obligated to notify the user of a legal process seeking access to his/her information, however, they can be prohibited by law to do so. In such cases, the user receives a delayed notice, after the expiration of a court order non-disclosure period. Therefore, a user's information may end up being used in court without his/her knowledge and without knowing exactly the type of data that is going to be brought forward.

Moreover, Fitbit mentions that non-personal data may be shared in an aggregated or de-identified manner with third parties or for public reports. However, there are multiple articles in literature stating that such de-identified data can easily be re-identified when crossed with data from other devices, posing a big threat to the privacy of the individual. (Bailey, 2016) Fitbit in particular poses a great threat in re-identification due to the fact that the gait of every person is unique. (Das et al., 2016) Such practices may fall under knowledge and intelligence based dark side behavior but also integrity challenge and manipulative dark-side behavior.

Another point of concern in the Fitbit privacy policy is the international operations and data transfers. As stated: "*Please note that the countries where we operate may have privacy and data protection laws that differ from, and are potentially less protective than, the laws of your country. You agree to this risk when you create a Fitbit account and click "I agree" to data transfers, irrespective of which country you live in. If you later wish to withdraw your consent, you can delete your Fitbit account." (Fitbit privacy policy)* Therefore, Fitbit mentions that not all countries where the data is shared may have laws as strict as the EU, resulting in potential privacy risks for clients and data misuse. Moreover, clients do not have the possibility to tailor their privacy requirements to their needs, having to opt in to a simple "I agree" and comply with all the company conditions or else refrain from using the device altogether. In order to be able to withdraw their consent, the only option left for clients is to delete their Fitbit account which means that the data from their device will no longer be sent to the app, and therefore customers won't be able to see their progress or data anymore either.

Alexa terms of use:

Amazon Echo also allows Alexa to perform voice purchases and to make donations to charities by using only voice. Even though this can be seen as a handy feature of the device, this exposes the user to big financial risks in case the device is hacked. There are instances in literature when such devices have been hacked, with the adversary issuing his requests via a headset. (Alepis et al., 2017)
Amazon mentions that Alexa can automatically recognize the voices of the users in a household, contributing to personalization of certain features of Alexa.
However, it is unclear which are these features, and why such a function is desirable. It is expected from such devices to answer to requests issued by their owners, however, it is not desirable to answer to requests that frequent the household (eg. housekeeping, acquaintances, etc).

Amazon mentiones that the Amazon Software will provide information about how the user interacts with Alexa, how the device is used, about the Alexa enabled products as well as the auxiliary products. Such data however, may be stored in servers outside of the country of the user and they fail to mention if the rules of the country of origin apply regarding data protection or not. Such an aspect would be of particular importance to clients from Europe that benefit from GDPR as well as more strict laws regarding data privacy compared to other areas.

It is mentioned that all of the data will be handled according to Amazon Privacy policy but little information can be found regarding this aspect. Lack of clarity regarding such details can be classified as knowledge and intelligence based dark-side behavior from Amazon's side. For example, in case such data is stolen, it is unclear under which country legislation such a case would be handled.

One of the most worrying capabilities of Alexa identified also in media is the drop-in function. It allows to a previously authorized user to "drop in" without the recipient having to give its consent. Such drop in consists of video calls that can be seen as an invasion of privacy, especially if the recipient is not aware of it or is caught in an embarrassing situation. Amazon mentions that if permission is granted to someone from a household to drop in, then everyone in the respective household would be able to drop in at any time, unannounced. Such a feature can be seen as a big invasion of privacy and can be related to the earlier mentioned capability of Alexa of receiving commands from people that are in a household (perhaps including also the ones that may frequent it).

Amazon privacy policy:

Concerning the Amazon privacy policy that the Terms of use refer to, a few points of interest have been identified.

Regarding gathered information, Amazon mentiones that they store information provided by the user on their Web or in any other way. Amazon mentions that the user has the possibility of not offering certain information, but then he/she may not be able to access certain features. Such behavior falls under Relationship-based dark-side behavior and negligence, given that it constrains the user to provide certain information in order to be given access to particular services.

Regarding cookies, that collect data on websites, Amazon's policy stands out. They recommend their clients to keep their cookies on, otherwise they may not be able to have access to basic functionalities such as adding items to their Shopping Cart, Checkout or be able to use any of the Amazon.com products and services that require a sign in. Once again, such practices can be classified as relationship-based dark side behavior and negligence, as explained in section 2.3.6 since, in essence, they require the customer to trade his/her privacy in order to be able to have access to basic functionalities.

With regards to the information the client provides to Amazon, among other expected pieces of information, such as name, address, phone number, credit card information etc, Amazon specifies that they will also have data regarding Social Security and driver's license numbers. However, nowhere before in the privacy policy is it mentioned when such personal data is collected and for what intent. In case such data is stolen from Amazon or sold by Amazon, it would provide hackers and third parties with large amount of information that could result in severe issues such as identity theft. Moreover, it is particularly hard to understand why Amazon would collect such data and how it would benefit improving its services.