Ca' Foscari University of Venice

Department of Computer Science

Master Thesis

Associating the Impact of Smart Home Technologies on Privacy

Bertukan Yohannes Tarekegn

Supervised by

Professor Agostino CORTESI

June 15, 2016

Abstract

Smart home is the general term commonly used to represent a resident that uses a home controller to integrate the resident's home automation systems. It is promising social, economical, environmental and other benefits such as computing elasticity, scalability and cost efficiency. However, every generation of technology opens the door to new opportunities but also opens the door to new challenges, thus, smart home with all these benefits also comes with the critical concerns of data privacy. The main characteristic of smart home is the prevalence of devices, sensors, readers, and applications which have the potential to collect a multiple stream of data types of individuals as they move through such environments. The possibilities to identify objects may lead to an automatic identification of persons that are directly or indirectly related to these objects. Failure to properly address this problem can cause considerable damage to company's reputation, income and other costs as well as negative effects for data subjects. This paper tries to associate the impact of the use of smart home technologies on privacy. The study explores the state-of-the-art on the way towards the smart home, the application fields that have already proved their potential for realising the vision and promises related to the new technology, the growing market and challenges that have to be addressed. The success and sustainability of smart home will depend on how privacy and other rights of individuals can be protected and how individuals can feel confident to trust the intelligent world that surrounds them. This study addresses these issues by analysing scenarios for smart home applications that have been developed over the last few years. It elaborates the assumptions that promoters make about the likely use of the technology and possibly unwanted side effects. The paper analyses number of threats for personal privacy that become

evident and assessed their impact rate on individuals and companies. It also reviews current legal legislations in data privacy and finalizes by introducing some of the ongoing research efforts that address smart home privacy issues.

Acknowledgements

First and foremost I would like to thank God. In the process of putting every activity together. I realized how true his gift is for me.

Secondly, I would like to express my special gratitude to my thesis advisor Professor Agostino Cortesi. The door to Prof. Cortesi office was always open whenever I ran into a trouble spot or had a question about my thesis. He has always insisted me to keep moving forward with his valuable comments and ideas.

I would also like to acknowledge my internship supervisor Privitera Roberto, head of Innovation and Technology at GRUPPO HERA, who gave me the golden opportunity to do a project which later helped me in doing this thesis and come to know about so many new things which I am really thankful to them.

I must express my very profound gratitude to my family. My mother Aster Tessema, My father Yohannes Tarekegn, My brothers; Nebiyou Yohannes and Gion Yohannes and my only Semeneh Mewled; thank you for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of my whole life.

I can not finish with out saying thank you to my special friend Helen Sileshi, not just a friend but also more than a sister and the family: Professor Paolo Santacroce, Fatuma Mohammed and Zereay Semagn, I will never get enough of thanking you for all your supports and love. I thank all my friends, classmates, family and everyone else around me. This accomplishment would not have been possible without your support, love and prayers.

THANK YOU GOD THANK YOU ALL!

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The concept of smart home environments is viewed as a key element of the future internet, thus many homes are becoming ”smarter” by connecting devices to improve home security, energy efficiency and comfort. At the same time data privacy is being identified as the main critical issue for realising the vision of smart home systems. Given the increasingly important role of assisted living with technologies in our everyday life, enhancing user's privacy protection is also another a critical issue. Increasing amounts of both personally identifiable information (PII) and sensitive (e.g., medical, financial and family) information continue to be leaked[20]. Through the introduction of online social networks, targeted advertising, online payment services, smart sensors and others computing technologies, the situation of privacy has been aggravated. Privacy has been given several type of definitions as it is always dependant of users choice. The general concept of what privacy is will be discussed in section 3 of this paper.

While doing my internship in a utility company called GRUPPO HERA, on the first phase of my project which is, scouting analysis on the smart home technolo-

gies, i discovered a lot of smart home technologies available in the market and the corresponding functionalities they provide. Thus, i was also able to see the characteristics that the devices posses and the privacy impacts behind the use of this products. I realised doing a deep research on this area could be important in creating awareness of the impact they cause on the users as well as the companies deploying and developing this products.

The task of protecting users privacy is made more difficult by their attitudes towards information disclosure without full awareness. Even after numerous press reports and widespread disclosure of leakages on of personal informations on the use of smart devices, many users appear not to be fully aware of the fact that their information may be collected, aggregated and linked with ambient information for a variety of purposes. However, still the collection, processing and dissemination of personal information can raise serious privacy issues among users when they let sensors collect their data, for a variety of daily activities such as eating, sleeping, having break fast and other daily based activities.

The use of smart thermostat, for example, has given rise to concerns about user's privacy in the case where, it adapts to user's habit in order to setup the auto services, it records all the activities that we do in a day and night 24/7, at what time we go to sleep, at what time we wake up, when we leave the house, when we come back and other activities. Although the practice of tracking individuals' activities increases the effectiveness of the devices, it also undermines the privacy of users, mainly because it relies heavily on users' personal information. The possessors of such data may use it for identity theft, social engineering attacks, online and physical stalking, selling to third parities and so on. As it will be discussed in detail in

section 2.4, the market of smart home is expected to grow fast. For instance, It has been forecasted by IHS Technology, a research firm By 2018, 45 million smart home devices will be installed. This shows the fact that issue of privacy will also be aggravated as well, as long as there is no any mitigation technique deployed in practice.

This paper makes contribution in answering who knows about us what, and creates awareness of what happens when we use smart home technologies. The target groups of this document are stakeholders who are concerned with deploying smart home technologies and also non-security experts with information to better understand dependencies and developments in the area of privacy. The document will also be of interest to policy-makers by providing an overview of the threats and good practices in smart home. It identifies existing policy measures supporting smart home privacy and further action that may be required for various stakeholder.

For the risk analysis, we have implemented Privacy Risk Assessment Methodology (PRAM) called Privacy Risk Management Framework(PRMF) developed by NIST(National Institute of Standard and Technology). In order to use the methodology we have identified two main use cases from smart home devices and exploit the problematic data actions related to the devices including the impact they cause. The analysis is performed in two cases: The first, *Individual case*: We analysed the impact of the use of the smart devices on individuals privacy. Second,*Business case*: We analysed the impact of deploying or developing smart home products on involving companies. By using smart meters and wearables as representing use case also for others smart solutions, we were able to show the

high risk we face while using these devices when there is no any privacy mitigation technique in place.

The study is organised as follows: First, we will discuss about the general analysis of the sate of the art of smart home that is, the technologies and protocols used, the main services they provide, the market of the use of this technologies and the general challenges in use of this technologies. Second, we will discuss about the general concept of privacy, its definition, history, privacy in ubiquitous computing and related legislations to protect privacy. In the third section, we will review related works about privacy in the smart home area. Fourth, we will show the general threats presented by use of smart home products, mainly from those of utility management devices and health and wellness monitoring devices. Fifth, we will associate the impacts of use of smart home technologies on individuals' privacy and business as well by creating use cases to understand the general scenario of what happens when we register to those services. We will finalise the paper by giving recommendations for individual users and also companies deploying and developing smart home products and providing open issues for future work.

Chapter 2

State of the Art

2.1 Smart Home Introduction

With the rapid advancement in technology, more objects are being connected to the internet than people in the world. Based on different market predictions, which will be discussed in section 2.4, this rapid increment will keep growing up as objects get the ability to directly interact with the internet through the fast evolution in technology. Smart homes are homes furnished with advanced technologies that provides the tenants with information about the conditions of their home and enables them to remotely control all connected devices. In addition to this remote control of the home, Smart home devices ability to learn the choices of its inhabitants and adapt to their preferences from time to time is another important feature of smart home. It enables automated and smart monitoring and control of a home and its appliances. Using home automation, we can make the home, a smart home.

Smart home definition and its goals have evolved continuously due to the fact

that there is a rapid evolution of diverse technologies, emerging from different research in smart home related technologies and from home automation developments. There is no a final accepted definition of what exactly 'smart home' is, the meaning of this term varies based on the technology or the service the home provides. Several terms are considered synonymous with this term in different contexts, such as: 'assistive technology', 'e-health', 'digital house', 'smart environments', 'automated house', and 'intelligent living'[5]. A smart home is described by L.C.D. Silva et al[11] as a "home-like environment that possesses ambient intelligence and smart control" which is capable of learning the behaviour of inhabitants and to offer various accommodations based on their preferences and is further divided into different types of services: security services, entertainment services, wellness monitoring service and energy management services, a definition which is supported by D. Zhang et al[31] and M.A.A. Pedrasa[24] among others.

Smart homes connect all the devices and appliances in the home so they can communicate with each other and with inhabitants. Anything in the home that uses electricity can be put on the home network and at our command. It has possibility to react when the command is given by the user to the devices by using voice or remotely. It also enables the inhabitants to connect, control and monitor all the smart appliances and information's in the home through intuitive user interfaces, cloud computing to display and process data and correlate and interpret the data through big data analysis.

Smart home is centralisation on a unique user interface of main home systems: home security, home energy and utility management, entertainment and comfort management and health and wellness monitoring. Examples of smart home de-

vices include: smart fridges, smart TV, smart camera, smart fork, automatic pet feeders, smart lighting, smart thermostat and others. Smart home solutions has increased over the past years due to the fact that the various smart home components, devices and systems have reached high level of technological advancement for entry into the market. Moreover, nowadays smart home devices have become more affordable. The interconnectivity of devices and intelligence related to living habits, combined with the automation of important utilities, smart homes constitute an attractive field for developments and future deployments. The technology aims to increase efficiency and quality of life. However, besides benefits, smart home also bears security and privacy risks.

Currently there are a lot of big companies and startups playing high role in the market of smart home. Samsung Smart Thing's currently is providing high amount of smart devices that can be used for energy saving, health monitoring, comfort, security and safety. Google Nest Labs is also a home automation producer of programmable, self-learning, sensor-driven thermostats, smoke detectors, and other security systems. On the other side, Apple provides a framework called "Home kit" to overcome the interoperability issue between devices which are from different manufacturer and controlling connected accessories in a user's home. Apple currently provides home kit enabled smart devices such as smart tv, thermostat and others. Another large player in this market is Logitech, Known for its universal remote solutions for home automation systems, Logitech is starting to move into home automation with its vision set on providing a whole home automation system. However, it has a way to go with its home smart hub solution but will continue to offer the solution for controlling home entertainment systems. Other players and startups including wink, Iris, Philips Hue, GE, Belkin, AlYT, Swannone, Quby etc., their products range from systems consisting of a starter kit that

can be remotely controlled and access to an application based ecosphere, to an ecosystem of integrated products.

2.2 Technologies and Communication Protocols

The fast evolution of ubiquitous computing technologies have allowed the implementation of smart home technologies. Embedded devices such as sensors, actuators, gateways, network devices, home appliances, and others which are interconnected and interacting with intelligent software to cooperatively collect environmental information about the state of the home environment and the activities and behaviour of its users. A smart home can function to a certain extent in an interactive and independent way. Since smart home interconnection specifications and communication technologies are relatively new and under development, most available technologies currently used were developed prior to the advent of the smart home vision.

The fundamental concept of a smart home is one fitted with a range of interconnected sensors (light, temperature, motion, moisture, pressure, smoke, etc.), systems (Heating and Air Conditioning System, lighting, security, etc.), and devices (media devices, appliances, laundry machines, fridges, stoves,TV, etc.), which can be automated, monitored and controlled. For example, through a computer, smart phone or tablet including from outside the home, or via the Internet. Smart homes can either be the result of integrated design, or the accumulation of interconnected objects over time, perhaps in response to changing needs or availability of technology[12]. The reason is to provide the users with realtime information

about the state of their home, and to allow them to control the connected devices.

In addition to remote control of the home, a smart home may also be able to 'learn' the preferences, activities and routines of its inhabitants and adapt to them. In this case, the control interfaces may fade into the background. This shift is seen as critical to avoid overloading the household with the task of monitoring and programming the smart home[8]. Smart meters can transmit energy consumption information back to the utility on a much more frequent schedule, a smart meter connected to smart grid is able to respond to fluctuations in the per-unit cost of energy by slightly adjusting the temperature of the house, a smart-home-connected refrigerator might be able to monitor its contents, and use this information to suggest potential menus or to order replacements, a smart home might respond to the presence of certain occupants by switching on/off the light automatically, Smart homes have also been identified as particularly beneficial for assisted living for ageing populations. From general perspective home automation consists of five building blocks: sensors, actuators, control network, controller and remote control device.

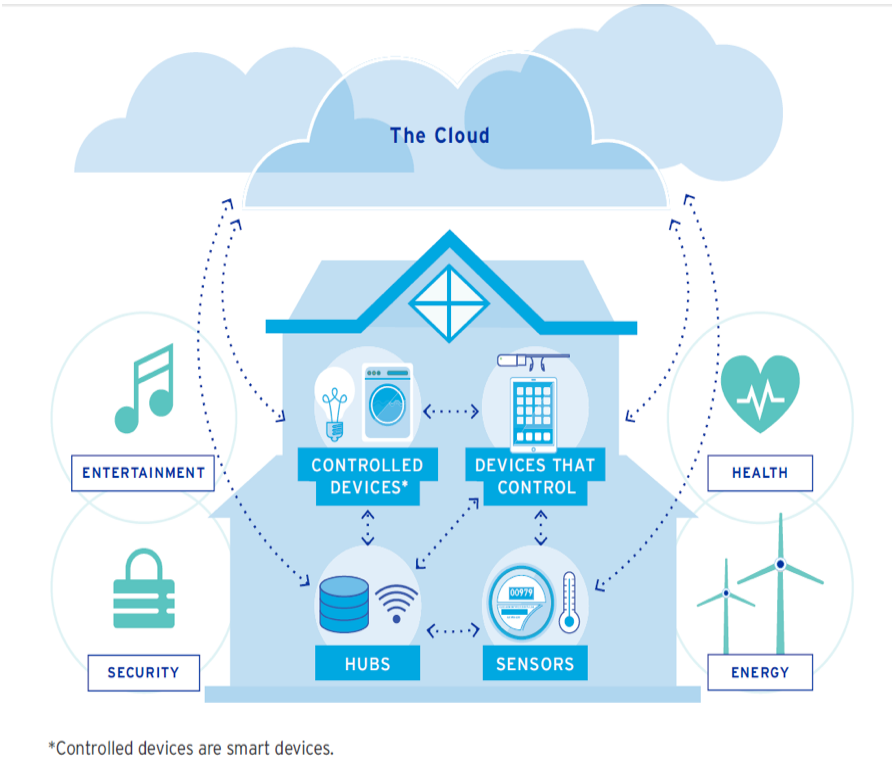

Figure 2.1: Smart Home Building Blocks

Element	Description
Sensors	This components of smart home system receives and responds to a signal so they are considered as the eyes and ears of the network. It convert a recognised signal into an electrical-analog or digital output that is readable and detect by receiving a signal from a device, then responding to that signal by converting it into an output that can easily be read and understood. Sensors have wide range of application: such as measuring humidity, temperature, light, moisture, smoke, motion and noise.
Devices Under Control	These are home appliances, consumer electronics, thermostats, washing machine, and other components which are connected to and controlled by the smart home system.
Actuators	They actuates or moves something, more specifically, it coverts energy into motion or mechanical energy so they are called the hands of the home network.(for example, if the temperature is too hot, then it turns on the cooling system)
Network	It provides the connectivity between all the components of the system: devices under control, sensors, and actuators and the controller with remote control devices. There are two main technology options to build the control networks : Wireless and Wireline.
Controller	It acts as the brain of the home automation system. It collects data through sensors and receives commands through remote controlling devices. It acts based on predefined set of rules by using actuators or means of other communication such as loud speaker, email, or telephone.

Table 2.1: Smart Home Building Blocks

Most of the communication protocols currently being used in smart home are developed prior to the advent of smart home. Some of the new smart home interconnection specifications and communication technologies are relatively new and under development. There are variety of platforms, protocols, on which a smart home can be built in which each one of them has essentially their own language. Each language speaks to the connected devices and commands the devices to perform function. Table 2.2 shows an overview of some of the most popular communication protocols used in smart home system.

Name	Description
ZIGBEE	ZigBee is based on the IEEE's 802.15.4 personal-area network standard. ZigBee is a very low-cost, very low-power-consumption, two-way, wireless communication standard that is being developed by the ZigBee Alliance, ZigBee is targeted at radio frequency (RF) applications that require low data rate, long battery life, and secure networking. Uses mesh networking topology[1, 14].
Z-WAVE	Z-Wave runs on the 908.42 MHz frequency band. It uses the same mesh networking strategy as ZigBee. It is also used for remote monitoring and control and ideal for home-area network. RF-based communication technology designed specifically for control, monitoring and status reading applications in residential and light commercial environments [14].
Bluetooth	Bluetooth is a wireless technology standard for exchanging data over short distances. Bluetooth offers an infrastructure of direct connection from smartphones and tablets, allowing users to control home appliances from their mobile device [14, 21].

WIFI	WiFi (IEEE 802.11) has become the de facto standard for broadband networking of wireless LANs (local area networks) in the home, in offices and at an increasing number of commercial 'hotspots' around the world. WiFi is the clear industry leader for broadband, wireless networking in the home. WiFi is well suited for sharing files, streaming video and other data intensive applications. IEEE 802.11, the standard underlying WiFi, actually comes in several different version, a, b, g and n. 802.11a is for licensed operation in the 5 GHz band and is mainly used by businesses. 802.11b, g and n are the WiFi versions that power most wireless networks. Version b, capable of communicating at 11 Mbps (megabits per second), appeared on the market in 1999, followed by version g at 54 Mbps in 2002. Version n, at 100 Mbps or more, began shipping in 2006 [14].
Insteon	Insteon enables simple, low-cost devices to be networked together using the power line, radio or both. The power line is typically used as a backup to the RF frequency used by the system [7].
Thread	Thread is a simplified IPv6-based mesh networking protocol developed by industry leading technology companies for connecting products around the home to each other, to the internet and to the cloud. It is very simple to install, highly secure and scalable to hundreds of devices[22].

Table 2.2: Communication Protocols

2.3 Smart Home Services

Smart homes have the ability to make life easier, enjoyable, convenient and peace. Whether you're at work or on vacation, the smart home will alert you to what's happening in your home, and security systems can be built to provide an immense amount of help in an emergency. For example, when there is a fire, smart home sensors sense the smoke and turns the fire alarm, the smart home would also unlock doors, dial the fire department and light the path to safety[26]. Currently, almost all of the appliance that we have at home are being presented with some degree of automation. The combination of automation and programmability of the device with artificial intelligence is the next step in the evolution of the smart home solutions. Smart home devices provide energy efficiency savings through the use of utility management devices such as: connected learning thermostat, connected lighting and connected energy tracking. Based on the fact that systems like Z-Wave and ZigBee can set devices at reduced level of functionality, they can go to "sleep" and wake up when commands are given. When a person leaves home, the lights are automatically turned off so that electric bills can go down, and rooms can be heated or cooled based on who's there at any given moment. One smart home owner heating bill is about one third less than a same-sized normal home with no smart devices available. Some devices can track how much energy each appliance is using and command it to use less.

Smart Home technology provides numerous advantages for an elderly individual living alone and general wellbeing checking at home. Smart solutions, such as: fitness tracking, connected scale, elderly/child activity uploading, connected pill case, connected forks and so on could tell the inhabitant when the time had come to take medicines, alerts the doctor's facility if the occupant fell, track how much

the inhabitant was eating and it can also make emergency calls. In the case that the individual is somewhat forgetful, the smart devices would perform assignments, for example, closing off the water before a tub flooded or turning off the stove if the cook had meandered away. It additionally permits adult children who are living somewhere else to participate in the care of their ageing parents. Individuals with disabilities can also benefit from the automated system services of smart home. In the following section we will try to see the general advantages of smart home solution in four divisions.

2.3.1 Utility Management

Since sustainability becomes part of our daily activity, reduction of energy consumption became a very important aspect in the context of the sustainable technological development of the modern society with a major impact on the future development of the mankind. On one side the technological progress requires the use of more energy, while on the other side energy became a limited resource. One of the major benefits of smart home to users is its ability to incorporate energy management features through lighting, air conditioning, heating and using other home appliances. Smart homes hold the potential for increasing energy efficiency, decreasing costs of energy use, decreasing the carbon footprint by including renewable resources, and transforming the role of the occupant. Recent studies suggest that 40% of total energy consumption and 36% of total carbon dioxide emissions in the European Union can be attributed to homes and buildings[2]. The lights in smart home can be turned on and off automatically based on motion sensors available in the home. An appropriate placement of temperature sensors and the use of heating and cooling timers can reduce the energy used and hence saving

money and also the house can set to turn off air conditionings when no one is in the room. Smart home can even go further in energy management by keeping track of the energy usage of each and every appliance in the house. The high power consuming devices can be scheduled by controllers for instance: dish washers and electric water heaters can take maximum advantage of off peak electric rates.

Smart homes can ensure appliances are on only when they are in use. It can regulate light usage, monitor heating and cooling equipment. For instance, A programmable thermostat offers flexibility and power to control the climate in our home efficiently to save energy and lower energy bill. With programmable thermostat we can set the temperature to different levels during set times throughout the week. For example during winter we can set the inside temperature to a lower level when you are at work and the house is unoccupied. This can save a lot on utility bills and energy.

2.3.2 Security and Safety

The safety of our home and our loved once ranks tops in life priorities. Smart home security systems do a better job of preventing intrusions and home invasions than security systems that require manual settings. Keep an eye on our home with home alert systems that remotely monitor and control our home. The security systems also have the advanced capability of warning residents of potential threats on the property or inside of the home. Smart alarms, intrusion detection through motion detectors, or door/window sensors, video surveillance are some of the products we can use. The fire alarm system can be set to unlock the door and alert the local fire department. It is also possible to remotely activate or deactivate motion

detectors, sensors or webcams possible to remotely monitor their home setting send notification(SMS, Email) of there is any security breaches movement detection, door opening, power outage locking and unlocking doors remotely detect gas or water leaks, using sensors that trigger and alarm in the event of abnormal gas or water consumption this enable user to take action remotely if they are on holiday or alternatively the service provider as part of the extended package could handle the situation fire detection, installing connectable smoke detectors using specific radio protocols would enable the consumer to be notified remotely when smoke is detected and connect to the webcam to check the home or alert the fire service.

2.3.3 Health and Wellness Monitoring

Having advanced technology in our homes will lead to various opportunities in the near future in this area. One of the most important is the monitoring of a person's cognitive and physical health and as a consequence of an ageing population, an area of critical need is eldercare. Suggestive kinds of smart healthcare technologies contain simple devices (blood glucometers, oximeters, blood pressure monitors, etc.) which deliver Standardised outputs for specific physiological conditions. Smart applications able to analyse and process body signals, sensor integrated smart devices (gaming devices, smartphones and pads), wearable sensors (e.g., wrist straps, T-Shirts) and additional devices entirely manufactured for the purpose of body signal monitoring/processing (e.g., mainframe computers, tablets). Older people can take advantage of smart home features that help them monitor their medications, call emergency numbers, and track caloric intake. Since memory lapses are common as senior citizens age, automatic light, water, and stove turn off functions will ease the concerns of loved ones.

2.3.4 Comfort and Entertainment

Smart home lets us enjoy personalised comfort settings that can be activated on a schedule or with just a few taps on our phone or touch screen. When we wake up it welcomes us to our "Good Morning" scene our favourite streaming music station kicks in over the bedroom speakers and the lights gradually brighten. The thermostat adjusts to the temprature while the shades slowly rise. Same happens when its time to sleep; turns off the light except the one at our bedside, put the shades down to block out light and lock all the doors before we get in to bed. shut down the thermostat and save our bill when it learns we are on our way out of home. Smart homes present the best sound and visual quality available for home entertainment systems. The television will be able to display what's online and residents can listen to music in any room inside of their homes. Internet access from outside of the home will allow home owners to record favourite television shows or download multimedia files to the stereo system. With a single remote, we can control virtually everything in our entertainment system and our entire home.

2.3.5 Smart Appliances

Smart homes can also make our live more easier by using smart appliance like smart refrigerators, smart oven/stove, smart laundry and other home appliances. Smart refrigerators monitor food storage temperatures and receive an alert whenever a particular food item falls below a designated inventory level or it orders milk and other ingredients before they run out. All appliances: fridge, freezer, stove, microwave, are now can be 'smart', which means they are able to sense their environment and communicate among themselves, with us, and with other things

and people via the Internet. We can set controls for energy usage of the appliances, adding a feature that adjusts light and heat consumption. Faucets, freezer, and stove coordinate the use of warm water and electricity with the local power plant to minimise our energy costs.

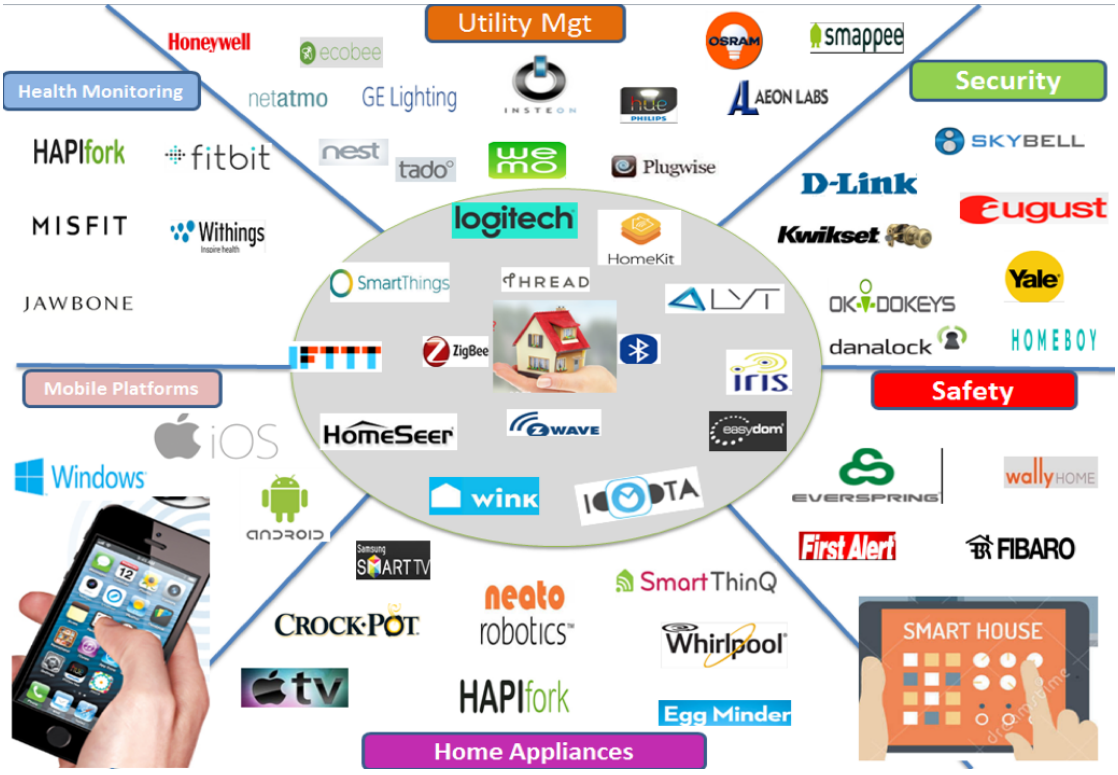

Figure 2.2: Smart home products, platforms, companies and main players of the market

2.4 The Market

Smart home system is not limited to single features or benefit rather, the digitalization of our simple tasks is saving us time and those times can be used to be spent on special things: families, careers, or other passions that we give priorities in our life, which is a strong marketing proposition. Smart Homes also have the potential to be sustainable innovation and efficient: optimising energy consumption, which could lower our energy usage, bills and reduce carbon footprint.

The Research firm, IHS technology, predicted that 45 million homes will be smart by 2018 and the annual business volume will grow to $12 billion dollars. Another Prediction by ABI research says that the growth will be $14.1 billion on the same year. Allied Market Research predicts that by 2020, the global smart homes and buildings market will grow at a compound annual growth rate of 29.5%, and the market will be worth $35.3 billion. A report from Juniper Research has also predicted that the market will grow to $71 billion by 2018.

According to M2M research series, in Europe and North America 68 million homes will be smart by 2019. In North America from 2014 to 2019, adoption of smart home system by households is forecasted to grow at a compound annual growth rate (CAGR) of 37%, resulting in 38.2 million smart homes. Market revenues reached US$ 4.2 billion (€3.2 billion) in 2014, an increase of 48% year by year. The market is expected to grow at a CAGR of 34% between 2014 and 2019, reaching US$ 18.2 billion (€13.7 billion) in yearly revenues at the end of the forecast period.

In terms of market maturity and penetration, the European market for smart home is still in an early stage of 2-3 years behind USA. In the EU28+2 countries there were a total of 3.3 million smart home systems in use at the end of 2014.The number of households adopting smart home in Europe is forecasted to grow at a compound annual growth rate (CAGR) of 61% during the next five years, resulting in 29.7 million smart homes by 2019. The market is forecasted to grow at a CAGR of 58% between 2014 and 2019 to reach €7.6 billion (US$ 10.2 billion) at the end of the forecast period.

Chapter 3

Privacy

Technological moves dependably brings new approaches for how privacy can be influenced, subsequently inciting the need to reassess one's comprehension of what protection is and how it ought to be ensured. With the advent of current telecom and PCs, Privacy is identified with, yet not indistinguishable with, mystery, isolation, autonomy, freedom, closeness, and individual hood. A last meaning of protection is troublesome, Privacy infringement can be seen as involuntary border crossing, that is, at whatever point data saturates obstructions without our assistance (or in opposition to our endaevors) boundaries, for example, letters, shut entryways, the trust of classification with a dear companion, or the passage of time. Keeping in mind the end goal to better see how to create a away that shields privacy, one needs to take a gander at how one's privacy can be damaged. It is essential since privacy, pretty much as security, is regularly not an objective in itself, not an administration that individuals need to subscribe to, but instead a desire of being in a condition of assurance without having to effectively pursue it.

3.1 Privacy History

Privacy has been an issue even before when there was no internet availability. Everybody seems to have some sort of natural perception of what privacy is on a case-by-case premise, yet it is difficult to fairly describe what absolutely it is. *justice of the peace act* is one of the earliest reference found in the 1361 in England. It set down the sentence for peeping Toms and eavesdroppers. in 1763, The British parliamentarian William Pitt on his speech in parliament said:

> "My home is my castle, the poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail" its roof may shake-the wind may blow through it-the storm may enter-the rain may enter-but the King of England cannot enter-all his force dares not cross the threshold of the ruined tenement"

Even though the concept of privacy is old, its exact meaning stills seems unclear until today[19].

Two U.S. Lawyers Samuel Warren and Louis Brandeis wrote the first legal article In 19 century. The article framed privacy as a tort action, that is, a civil wrong that one could sue for compensation of injuries. In their 1890 Harvard Law Review paper, they described privacy as "the right to be let alone", a condition of isolation and segregation that would guarantee a general right to the insusceptibility of the individual, the privilege to one's identity[29].

Today's advancements of "Smart Meter" appear to reflect the sudden innovation shifts experienced by Warren and Brandeis, opening up new types of social connections that change one's desire of privacy protection. Be that as it may, even the

solid likeness of technological advancement can't overlook the fact that their "right to be let alone" looks scarcely practicable today. With the large number of associations in this age of interconnected world, users got themselves always needing managing individuals that don't have any history together with them in person, hence require some type of data from them to judge whether such a connection would be advantageous. Safeguarding privacy through detachment is simply not as much an alternative any longer as it was 100 years back.

Another book called "privacy by design", the authors defined privacy as "the claim of individuals, groups, or organizations to decide for themselves when, how, and to what degree data about them is imparted to others' [30]. It focused on the way that the individual's need for protection is never absolute, since cooperation in the public arena is a similarly intense yearning. Being in control of one's private data is stand out aspect of privacy.

The term "privacy" implies distinctive things to various individuals. The idea of privacy appear to originate from different points of view, uniquely the sociological and legal. Idea of privacy from the sociological point of view contends that a meaning of privacy is not direct or static. It is not direct on the grounds that one's view of protection is different from the others. Likewise it also happens when policymakers, masters, specialists, and researchers, from different hypothetical foundations, try to characterise the term, its concerns, and its protection. Moreover, the meaning of protection is not static, since its definition will change from time to time and the scope will stretch out because of new social standards, people, religion, belief and attitudes, and new innovations being presented.

3.2 Privacy in Ubiquitous Computing

The idea of ubiquitous computing (ubicomp) tries to build up a dispersed and organized figuring foundation to bolster client exercises, while staying straightforward to the clients. Universal Computing (UC) alludes to situations where most physical articles are improved with computerized qualities. It infers that little, frequently minor measured gadgets, with registering capacities which are remotely interconnected, are installed imperceptibly into most protests utilized as a part of regular life. Universal or surrounding knowledge situations present a scope of new central issues related not just to innovation (for occasion, planning inconspicuous gadgets, dynamic systems, and characteristic client collaboration) additionally to social, moral and lawful contemplations, for example, security assurance.

The concept of ubiquitous computing (ubicomp) seeks to develop a distributed and networked computing infrastructure to support user activities, while staying straightforward to the consumers. Ubiquitous Computing (UC) refers to situations where most physical objects are improved with computerised qualities. It infers that little, frequently minor measured gadgets, with computing capabilities which are remotely interconnected, are embedded almost invisibly into most objects used in everyday life. Ubiquitous or surrounding knowledge situations introduce a range of new fundamental problems related not only to technology but also to social, ethical and legal considerations, such as privacy protection.

The advent of Ubiquitous Computing has brought a set of new challenges along with numerous advantages. One of the most controversial issues discussed about ubiquitous computing is privacy. For the end user there are several advantages and disadvantages of living in smart environments. On one side, ubicomp has

the capability of radically changing, in a positive way, the safety, efficiency, and convenience of users (e.g., to help family members, doctors, or nurses to monitor elderly persons). However, ubicomp environments also introduce the potential for the misuse of the personal information produced by the system. Users indicate discomfort regarding the possibility for abuse and the absence of control, hence they desire privacy tools in ubicomp systems [16]. There are four properties that makes ubiquitous computing different from other computer science domains with respect to privacy: *Ubiquity*(the fact that everywhere availability of Ubiquitous computing will affect every part of our lives, from what we eat to when we sleep,when we go office.), *Invisibility*, *Sensing*, *Memory amplification*[9].

3.3 Privacy Legislation

Any data related to individual, whether its related to professional, private or public life, it is called personal data. Personal data can be: name, email address, photo, age, bank detail, medical information. In the advanced digital age, the processing of personal information is essential part of how the technology works. Data is being processed by all businesses: social media sites, insurance firms, banks and search engines. Further more, in the connected world there is transferring of data to third countries through the cloud computing. Data may be sent from Berlin to be processed in Italy and stored in Florida with no online borders.

So many studies have been performed by many governments and standardisation bodies for the how personal information can be processed and handled. As a result, to assure and provide adequate privacy protection for processing of personal informations, they have regulated different practices to individuals and companies.

But given the global nature of the IoT, both the data subjects and data controllers are confronted with a number of national/regional data protection laws providing different levels of protection. The transfer of data to third countries has become an important factor in daily life. When data controllers of IoT systems and individuals affected by the systems are based indifferent countries, this potentially leads to lots of different applicable laws.

One of the Legislation adopted in the european union is called EU Data Protection Directive (also known as Directive 95/46/EC). It is designed to protect the privacy of processing of personal data about the citizens of EU. It mainly relates to the sharing, utilising, and collection of personal datas. The Directive holds the key elements from article 8 of the European Convention on Human Rights which covers the protection of the right of privacy in personal and family life and also in the home and personal correspondence.

The recommendations in the EU Directive 94/46/EC are based on seven principles: *Notice*: subjects whose data is being collected should be given notice of such collection. *Purpose*: data collected should be used only for mentioned purpose(s) and no further repurposing, Consent: personal data should not be disclosed or shared with third parties without taking consent from the data subject(s), *Security*: once the data is collected, personal data should be kept safe and secure from potential abuse, theft, or loss, *Disclosure*: data subjects should be informed when the parties collect their data, *Access*: subjects should granted access to their personal data and allowed to correct any inaccuracies, *Accountability*: subjects should be able to hold personal data collectors accountable for adhering to all seven of these principle.

Although the Data Protection Directive guarantees an effective protection of right to personal data protection, the differences in the implementation the directive by each member state have brought inconsistencies which creates uncertainty, complexity and administrative costs. This affects the the effective implementation of the directive and create trust and confidence issues on individuals. Thus the EU adopts a reform package for the protection to make Europe fit for the digital age. The reforming processes is an essential step fundamental rights protection and facilitate business by unifying and avoiding differences for companies in the digital Single Market. The data protection reform package includes the General Data Protection Regulation ("Regulation") and the Data Protection Directive for the police and criminal justice sector[10]. The Regulation updates and modernizes the principles enshrined in the 1995 Data Protection Directive to guarantee privacy rights. The changes will give people more control over their personal data and make it easier to access it.

While this study was in process, the proposal for the new reformed regulation and directive have been published on 4 May 2016 in the EU Official Journal in all the official languages. Although the Regulation has entered into force on 24 May 2016, it is not being implemented yet since the EU member states have to transpose it into their national law until 6 may 2018 and its expected to be implemented from 25 May 2018.

Chapter 4

Related Work

There have always been research going on in security and privacy issues in the smart home solutions by different communities. A recent survey by Komninos and others [18] presented the challenges related to the smart grid and other smart home technologies. They demonstrated the impact of security threats of smart grid by using risk assessment method of FIPS199. In many researches smart meters have always been identified as the potential privacy vulnerability in the smart home technology. The authors in [27] presented a theoretical framework to quantify the utility privacy trade off in the smart meter data. It addresses the potential threats to privacy which can be exploited through the use of smart home technologies communication technologies. In similar way, [28] also have described that activities in the home such as eating, cooking, taking shower, and sleeping can be detected by intercepting on the transmissions of sensors in a home, even when all of the transmissions are encrypted. For the approach, A combined Fingerprint and Timing-based Snooping (FATS) attack have been used. In [6] the paper provide a review of Smart Home projects and the related technologies of wearable health monitoring systems and assistive robotics which support elderly

and disable people. The paper particularly points out that the advantages of remote monitoring which should be carefully evaluated for privacy, confidentiality, and security purpose.Various projects are also identified, which tries to address this need. In [17] the authors performed an analysis of the privacy risks and mitigation techniques for the sensors networks (IEEE 802.15.4 and ZigBee).

Chapter 5

Privacy Threat Analysis of Smart Home Technologies

The smart home is a point of intense contact between connected technology and physical space. This creates new threats and vulnerability models that would effect from claiming bringing together both those virtual and physical contexts. While it's easy to get lost in the excitement of deploying smart home technologies, it is very important to take the time to really understand where our personal data is going and who is doing what with it. All of smart home products are based on a cloud hub solution, thus it enables the user to hook up with a variety of sensors and connect each sensor to a hub in the home. This is great for efficiency, but what's negative about this new automation is that the data about our everyday life, which is emitted from our home, is now beingăcollected and analysed for the benefit of the solution owners.

Smart home is a good way forward but recognising that privacy awareness should be a prerequisite of ownership. Privacy issues in smart home is not only about

confidentiality and access control. Smart home sensors in particular will generate a large amount of personal data about activities performed within the home. Too many personal data combined together in a smart home system create the possibility of getting contextual background that reveal patterns of behaviour of the inhabitants [9]. Smart home systems may include embedded features that are opaque to the user, and do not inform the user about the status of their operation. Usually once the companies make users sign some privacy agreements, they don't ask users again for repurposing of those shared datas. It is also difficult to update and patch in response to identified vulnerabilities. Smart homes include sensitive systems related to the occupants' healthcare, finances and systems related to the physical security of the home, which may be open to dangerous manipulation by attackers.

According to Finn, R. L., Wright, D. and Friedewald, [13], Smart home functions may have serious impacts upon privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image, privacy of location, and privacy of association[13]. Here are the seven types of privacy concerns that we will try to associate in section 6.

1. **Privacy of the person**: Focuses on the right to keep body functions and body characteristics (such as genetic codes and biometrics) private.
2. **Privacy of behaviour and action**: This concern mainly focuses on very sensitive issues such as political activities and religious practices, sexual preferences and habits. However, the notion of privacy of personal behaviour concerns also activities that might happen in public space and private space.
3. **Privacy of communication**: Aims on avoiding the interception of com-

munications, including mail interception, directional microphones, the use of bugs, telephone or wireless communication interception or recording and access to e-mail messages.

4. **Privacy of data and image**: Includes protecting of individual's data from being automatically available or accessible to different organisations and individuals. So that people can exercise a substantial degree of control over their data and its usage.

5. **Privacy of thoughts and feelings**: Means that the person has the right not to share his thoughts or feelings or to have those thoughts or feelings revealed. Privacy of thought and feelings is different from privacy of the person, in the same way that the mind can be distinguished from the body.

6. **Privacy of location and space**: Is the right of individuals to move around public or semi-public space without being tracked, identified or monitored. This privacy type also includes a right to solitude and a right to privacy in spaces such as the home, the car or the office.

7. **Privacy of association (including group privacy)**: Is concerned with people's right to associate with whomever they wish, without any kind of monitoring.

Smart homes have high privacy and data protection impacts. The characteristic of connected things environment is the similar to the characteristics of smart devices, applications and sensors which collects a multiple stream of datatypes of data subjects as they move through such connected environments. The increasing number of interlinked smart devices and the possibilities to automatically identify objects is also leading to an automatic identification of persons that are related

to these objects. The increment in number of interlinked sensors the activities related with those sensors in the smart home could be a source of close, granular and intimate data on activities and behaviour of inhabitants and visitors. Organizations which are part of the smart home market, including both the startups and even the crowd funded efforts, are mostly to lack privacy expertise involved in the smart home market. By integrating the data that is available from different sources or services can also create new knowledge on data subjects that might not be revealed if separate examination is performed in the same datasets. This creates the issue of identity theft. An example for this problem can be found in implementations of using credit cards, in which the name and card number can be read without any authentication printed on the card. With this data it is possible for attackers to use the card to purchase goods with the identity of the card holder.

5.1 Threats to Privacy Presented By Utility Management Devices

It is asserted that most of the existing utility companies are not following the basic common sense guidelines in managing what private and/or confidential data they should reasonably collect from customers. In fact, it would appear that many utilities are collecting more information than the utility device necessarily need to work properly with no regard to the consumer. In this section we have selected smart meter as an example of utility management device to show what happens when we use the device and which type of privacy is being affected.

Scenario : Smart Meter: All smart meters allow the utility to remotely moni-

tor electricity consumption not just monthly or yearly but on a real-time basis. Depending on the meter, this is at least as frequently as hourly and often as frequently as every few minutes. The real-time monitoring can also occur by outlet, room, and by appliance, depending on the types of appliances in the home. Before smart meters, the only data gathered by utilities from electric meters was the total consumption of electricity on some interval (i,e. monthly) which is not as frequent as how smart meters do. In the case of the new smart meters, its mostly unclear which and how much information will be gathered however, data sent from the meter is personally identifiable.

Due to the fact that smart devices (including heating and cooling systems, refrigerators, toasters, hair dryers, computers, and home entertainment centers) account for sixty to ninety percent of residential energy usage, managing their energy consumption can greatly affect the energy load at any time of day. Manufacturers have begun to make more and more of these appliances grid-enabled-that is, smart appliances-by enabling them to communicate with smart meters. So if they are enabled, the appliances frequently send their energy usage to the smart meter labeled as consumed by that appliance. A resident can then view the home's detailed energy usage on an in-home display or on utility's website and make informed decisions on how to adjust energy usage. In addition, anyone with access to a resident's display or the website could review the load signature to determine what time the person arrives and leaves home, if the security system is activated, if one cooks with a microwave or the stove, the presence of certain medical equipment, how much and when the household watches television, if someone gets up in the middle of the night and uses the computer, which equipment is left on 24/7.

Devices like, smart meter collects statistics of usage of the device and environmental data and thus 'learn' the user's behaviour. This is stored within the unit and also uploaded to the cloud once it connects to a network. It also uploads system logs and software logs, which contains information such as the user's code, device settings, HVAC settings, and wiring configuration. Some times reports are shared with utility companies in order to generate energy more efficiently.

Effect: Through the use of smart meters, utilities typically collect thousands of times more data than required to generate a monthly bill and this exposes the data subjects to unnecessary privacy risks. The threats to privacy connected to smart meters lie primarily within the concepts of *the right to be left alone* within one's home and *the right to control personal information*, Smart meters can compromise both of these rights. Many smart meters are found within residents, and all of the meters, even those that are not located within in the home itself but adjacent to an outside wall of the house or somewhere on the home's property, record information about what happens within the home. Users don't want other people to be able to discern when they get up in the morning or when they go to bed. When people go on vacation, they don't want the ability for other people, no matter who they are, to be able to tell when (or confirm when) the house is either occupied or unoccupied. The unnecessary collection of the above information and data is considered by many as a clear invasion of privacy and a threat to both personal privacy, personal security and the security for the home and property.

- Since it's possible to aggregate data from different sources, individuals identity could be revealed.
- Smart meters will reveal the activities of people inside of a home by measuring their electricity, gas, or water usage frequently over time.

- Tracking Behaviour of Renters/Leasers: Usage patterns and behaviour could be monitored by renters who have same access to the device.
- Access to data use profiles that can reveal specific locations, and times of electricity usage in specific areas of the home can also indicate the types of activities and/or appliances used which leads to determination of personal behavioural pattern.
- The data could be (mis)used by companies to perform marketing, governments to tax specific activities and uses and persons to conduct activities with malicious intent.
- Smart meters will provide capability to track appliance usage. Appliance producers may want to get this information to know why, who, and how individuals used their products in certain ways. Such information could have impact on appliance guarantees. Insurance companies may also use this information to approve or decline claims.
- Access to near real-time energy usage data can reveal if people are at home, in which room they are, what they are doing, and so on. This not only bring a safety risk, with burglars and vandals using it to their criminal action, but it might also be used to do marketing and advertisement based upon home energy use behaviours.

5.2 Threats to Privacy Presented By Smart Wellness Monitoring Device

Smart wellness monitoring devices improves the quality of life, efficiency, and cost of healthcare. Even though smart health monitoring devices create a longer and

more enjoyable life, there are still challenges in the application of these technologies. In smart wellness monitoring system, portable Wearable's connected wirelessly to mobile Internet devices, and even embeddable sensors, will enable long-term continuous medical monitoring for many purposes. For instance, for patients with medical conditions, individuals seeking to change behaviours like (losing weight), physicians needing to quantify and detect behavioural aberrations for early diagnosis (such as depression), or athletes wishing to monitor their condition and performance. While smart wellness monitoring devices can improve quality of life and healthcare, they also generate new security and privacy issues. When data are continuously processed (collected, stored and shared), they can include information that data subjects want to recall later, but also some facts that users are not willing to store or to be reminded of later on. The processing of datas in such devices gives a record of everything we've done, day in and day out, and may be even some things we don't want to remember and to be reminded of'. Clearly, privacy is important in any healthcare information system. Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data[23].

Scenario: Wearables: are wearables really ready to be wear? this is the first question that comes to users concern in the case of wearables. The rapid pace of technological innovation today makes it difficult to predict what wearables will look like in even a few years, let alone to govern how they should collect, use and store information. In just a few years the wearables market has shifted from clip-on devices with basic accelerometers to flexible wristbands, chest straps and smartwatches with accelerometers, altimeters, gyroscopes, ambient light sensors and heartbeat sensors[25]. Future technological advancements may bring devices and sensors even closer to consumers: in the form of clothing, dermal patches, con-

tact lenses, tattoos, implants, and even 'swallowable' gadgets[3]. And obviously it highly carries different privacy risks. As wearable technologies collect huge amount of personal information, the privacy risk will also continue to arise. Many wearable devices collect information about users' health and fitness, for example, more than one type of quantified-self data exists, each with its own level of sensitivity and potential privacy impacts.

Effect: The fact that so much data can be collected through a wearable device, such as: smart watch, smart bracelet, a fitness tracker, or an activity tracker, implies that there are tangible risks involved. Smart wellness monitoring permits collection of huge amount of medical data about the patient, as many smart devices collect data continuously over extended periods of time. For instance, instead of a one-minute recording taken in the clinic every other week, it is possible to record electrocardiogram data continuously for weeks, throughout daily life. In using of smart wellness monitoring devices, it's not only the physiological data that is being collected rather, it allows much broader range of health-related informations to be collected, it could also collect information about patient lifestyle and activities including food habits and diet details, locations, physical activity, or social interactions. Smart health monitoring devices[23] also permit integration to a broad range of health-related applications: sharing data with your health provider, as in a traditional doctor relationship, also sharing data with an insurance company (e.g., to confirm compliance with a medication regimen), with lifestyle consultants (e.g., diet advisers), with sport coaches (e.g., sports teams or health-club trainers), or with family (e.g., to support a relative's recovery from surgery). In such settings, privacy is a complex issue: the patient needs subtle control over the collection, recording, dissemination, and access to their data.

Chapter 6

Associating The Impact of Smart Home Technologies on Privacy

6.1 Privacy Risk Assessment Methodology

The basic aspect of risk management is a risk model that enables the ability to identify critical risks. NIST has developed Privacy Risk Assessment Methodology (PRAM) called Privacy Risk Management Framework(PRMF). The framework [15] defines an equation and a series of inputs to enable the identification of problems for individuals and companies that can arise from the processing (collection, retention, etc.) of personal private information and the calculation of how such problems can it cause on individuals and in an organisation.These allows for prioritisation and resource allocation to achieve companies missions while minimising adverse events for individuals and agencies collectively.

Even though existing tools such as the Fair Information Practice Principles (FIPPs)

provide a foundation for taking privacy into account, they have not yet provided a away to measure privacy impacts on a consistent and repeatable basis. The PRMF provides the basis for the establishment of a common vocabulary to facilitate better understanding of and expressions about privacy risks and the effective implementation of privacy measures and principles.

In most of the cases, risk is always expressed as a function of the likelihood that the problematic data would occur multiplied by the impact of its occurrence [4]. Likelihood or probability is understood as a function of the threats to the system, the associated vulnerabilities that can be exploited, and the consequences should those vulnerabilities could cause [15]. Information privacy risk, therefore can be expressed as a function of the likelihood that information processing (collection, retention, sharing etc.)causes problems for individuals as well as organisations, and the impact of the occurrence of the problematic data that could occur. In simple terms, [4] expressed privacy risk as:

$$PR = LP \times IP$$

Where :

PR: Privacy Risks

LP: likelihood of problematic data action

IP: Impact of problematic data action

Data actions are information system operations that process personal information. "Processing" can include, but is not limited to, the collection, retention, logging, generation, transformation, disclosure, transfer, and disposal of personal information.

If this is true for each data action in an information system, then the unmitigated privacy risk for an entire system, R_u is given by

$$R_u = \sum_{d}^{D} \sum_{p}^{P} L_{dp} I_{dp}$$

Where:

L_{dp}: is the likelihood of privacy problem occurring in data action

I_{dp}: is the impact of privacy problem on the agency if it results from data

D: is the set of all possible data actions

P: is the set of all possible privacy problems

Mitigated or residual agency privacy risk for a system, R_R, is given by

$$R_R = \sum_{d}^{D} \sum_{p}^{P} (L_{dp} - C_{dp}^{L})(I_{dp} - C_{dp}^{I})$$

where:

C_{dp}^{L} : is the reduction in likelihood of privacy problem p occuring in data action d by employing control c.
C_{dp}^{I} : is the reduction in the impact of privacy problem p on the agency if it results from data action d by employing control c.

The mitigated risk calculation shows that, for any data action, a given control can minimize the likelihood of a privacy problem, the impact of that privacy problem should it cause, or both.

Using this new equations, agencies can calculate the privacy risk of a data action by assessing likelihood and impact of the data action becoming problematic. Likelihood is assessed as the probability that a data action will become problematic for a representative or typical individual whose personal information is being processed by the system. The PRAM demonstrates a step by step analysis of likelihood. According to PRMF, agencies can support the assessment of likelihood in a number of ways.

i) It is possible to use existing information on customer demographics to estimate likelihood.

ii) They may extrapolate from information available about privacy concerns in similar scenarios.

iii) They could conduct focus groups or surveys to glean more through and specific information from users about privacy concerns.

Impact is assessed as the magnitude of the problematic data action on the organisation if it occurs. The PRAM[4] reflects these framing processes with an impact analysis focused on four organisational impact factors. To calculate the total business impact that the risks cause here are the four organizational factors that should be considered.

1. *Non-compliance costs*: The impact caused by not complying with applicable laws, policies, contracts.
2. *Direct costs*: Direct impacts of the problem on the company related to achieving its mission and profit.
3. *Reputational costs*: The impact of the problem on public trust in the company.

4. *Internal culture costs*: The impact of the problem on the companies inside working culture.

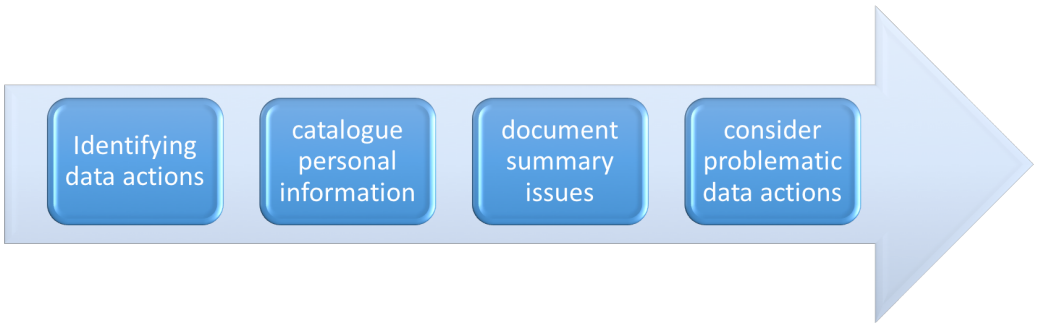

Figure 6.1: Inputs for PRAM

Figure[6.1], Shows the principal inputs for the risk analysis using PRAM which are: The data actions of the system, Personal information associated with a data action, and context, or the circumstances surrounding the data actions. Data actions are any information system operations that process personal information. Both context and associated personal information contribute to whether a data action has the potential to cause privacy problems. For each data action, we should identify the associated personal information and the risk of a data action which is also a function of context: the circumstances surrounding theăsystem's processing of personal information.

6.1.1 Privacy Risk Assessment Using Real Use Cases.

In this section we are going to perform privacy risk assessment for smart home products. We have performed privacy risk assessment for smart home solutions by using the privacy model called PRAM presented by NIST. We have tried to show the privacy risk that results from the processing of personal information using (PRAM) for anticipating and addressing in the case of smart home products. Using the equation provided by PRAM, we have calculated the privacy risk of a data action by assessing likelihood and impact of the data actions presented by smart home products.

For our assessment we have considered two cases: The first is, the Privacy impact of personal data being processed by different data controllers on individuals. The second case is, assessing the total business impact on companies (such as, smart home products developers and also service providers) which results in individuals being affected by using those products. In order to implement the equations presented by PRAM, we have considered companies with no privacy mitigation techniques in place so that there is no reduction to the likelihood of the occurrence of the privacy problem, the impact of that privacy problem should it occur.

The equation we have used is the unmitigated risk R_u is given by:

$$R_u = \sum_{d}^{D} \sum_{p}^{P} L_{dp} I_{dp}$$

Step 1: Problematic Data Action Identification

Following the steps provided by PRMF, the first step we have performed is iden-

tifying the problematic data actions and the personal information associated with a data action, and context, or the circumstances surrounding the data actions presented by two real use cases: Smart meters from energy management devices and wearables from health and wellness monitoring devices. The reason why we have considered this two use cases is while we were doing the scouting analysis of smart home products, we have identified the characteristics of most of the smart home products currently available in the market. By using those informations we have selected two of those devices which were critical to get most of the general problematic data actions that also presented by others smart home solutions.Thus, identifying the risks of this two areas were good enough to draw a generalised idea for others as well.

For assessment of the likelihood analysis to understand the probability that a data action will become problematic for a representative or typical individual whose personal information is being processed by the system, we have used the second option presented by PRMF which was mentioned in section 6.1: 'extrapolating from information available about privacy concerns in similar scenarios'. Based on this, we have tried to extrapolate data by creating different scenarios.

6.1.2 Use case1

Type of Device : Smart meter

Category: Utility Management Device

Description: smart meter is an electronic device that records consumption of electric energy in intervals of an hour or less and communicates that information at least daily back to the utility for monitoring and billing.

Features of The device:

- Energy control:
  - Smart meters provide accurate, near-real-time information about the energy we are using. We can use this information to control consumption habits and see direct evidence of the positive impact of your actions.
- Bill savings
  - Use the energy information we receive in order to make changes in consumption that can lower your bills.
  - Use this information to make energy efficiency improvements to our resident that may save us even more money.
  - Find out when energy is least expensive so we can change our usage.
- Environmental Responsibility

– The smart grid is able to accommodate renewable energy sources such as wind or solar.

Data Action1: *Detailed Collection of usage statistics of the device and environmental data*: Smart meter and home automation network data may track the use of specific appliances. Access to data-use profiles that can reveal specific times and locations of electricity use in specific areas of the home. It can also indicate the types of activities and/or appliances used. This could lead to determining personal behaviour patterns, habits, and activities taking place inside the home by monitoring electricity usage patterns and appliance use, including activities like sleeping, eating, showering, and watching TV and so on.

Data Action 2: *Granular energy data and appliance energy consumption profiles*: Patterns over time allows to determine how many people are at home and at what time, work schedule, sleeping routines, eating routines, vacation, health, or other lifestyle details and habits. Determine what appliances you use when, e.g., washer, dryer, toaster, furnace, A/C, microwave, medical devices, via granular energy data and appliance energy consumption profiles.

Data Action 3: *Performing Real-Time remote Surveillance*: Real-Time Surveillance Information Via real-time energy use data, determine if anyone is home, what they are doing, and where they are located in the home, determine when a home is vacant (for planning a burglary), who has high-priced appliances, and who has a security system. Endangering the physical security of life, family, and property and unwanted publicity and embarrassment (e.g. public disclosure of private facts or the publication of facts which place a person in a false light Near-real-time surveillance).

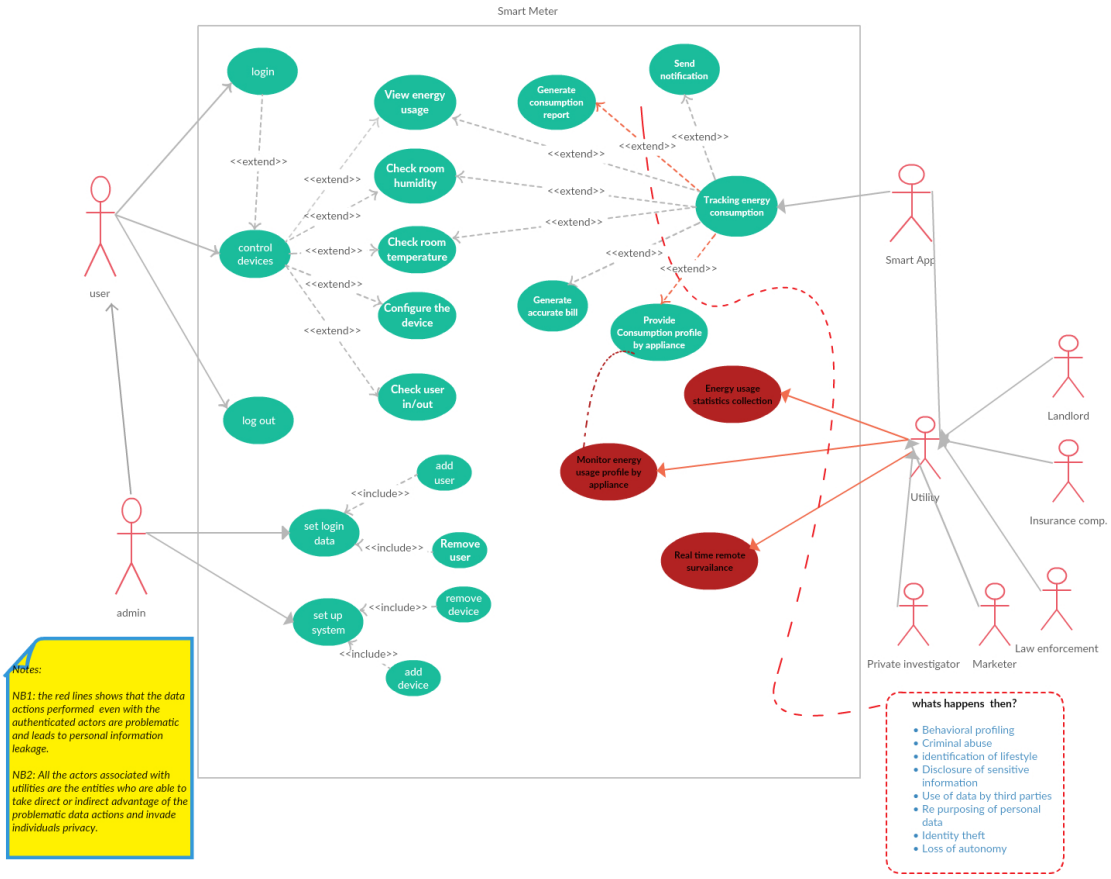

Figure 6.2: Smart meter use case diagram

Table 6.1: Privacy concerns related to smart meters

Entities potentially using collected data	Privacy Concerns
Utilities	Efficiency analysis and monitoring: demand-response, public or limited disclosure of usage statstics to promote conservation, energy awareness, etc.
Insurance Companies	Insurance company interpreting the data in a way that allows it to penalize customers. Determine premiums (e.g., specific behaviour patterns, like erratic sleep, that could indicate health problems[4].
Marketers	Marketers could obtainăinformation for targeted advertising. Use of individual or aggregated smart meter data to target advertising at specific household or individual.
Uses Law Enforcement	Identify suspicious or illegal activity, investigations, real-time surveillance to determine if residents are present and current activities inside the home[4].
Landlord/Lessor	Landlords can spy on tenantsăthrough an online utility account portal. Checking if their property is over occupied.
Private Investigators	Use of data for investigations, monitoring for specific events.
Creditors	Determine behaviour that seems to indicate creditworthiness or changes in credit risk.
Illegal uses	Identify the best times for a burglary, determine if residents are present, identify assets that might be present, commit fraud, identity theft, disrupt service, determine confidential processes or proprietary data.

6.1.3 Use case2

Type of Device: Wearable's

Category: Health and Wellness Monitoring

Description: Is a category of electronic technology devices that can be worn by a consumer and often include tracking information related to health and fitness. That are incorporated into items of clothing and accessories.

Features of The device: Fitness tracking, record heart rate, body fat composition, perspiration, blood pressure, blood glucose levels, health, temperature and muscle activity, sleep patterns and more all by just touching your skin as well as movement, distance and speed using GPS, accelerometers and gyroscopes.

Data Action1: *Analysis of Health of the patient by using Medical Sensors*: The sensors include heart rate monitor, oximeter, blood pressure sensor, ECG module, and thermometer. Each patient is monitored using the vital parameters from the sensors embedded on the patient as well as in the surroundings. Certain data types when combined could have critical implications, collecting personal data can also facilitate criminal abuse. These records can be used to correlate the current data received from the sensors for diagnosis.

Data Action2: *Real Time Health Advice and Action*: This service is designed to operate when the Emergency Response System fails to arrive or the patient is unattended.

Data Action 3: *Parent Monitoring Services*: Discrete Display of Confidential Information.

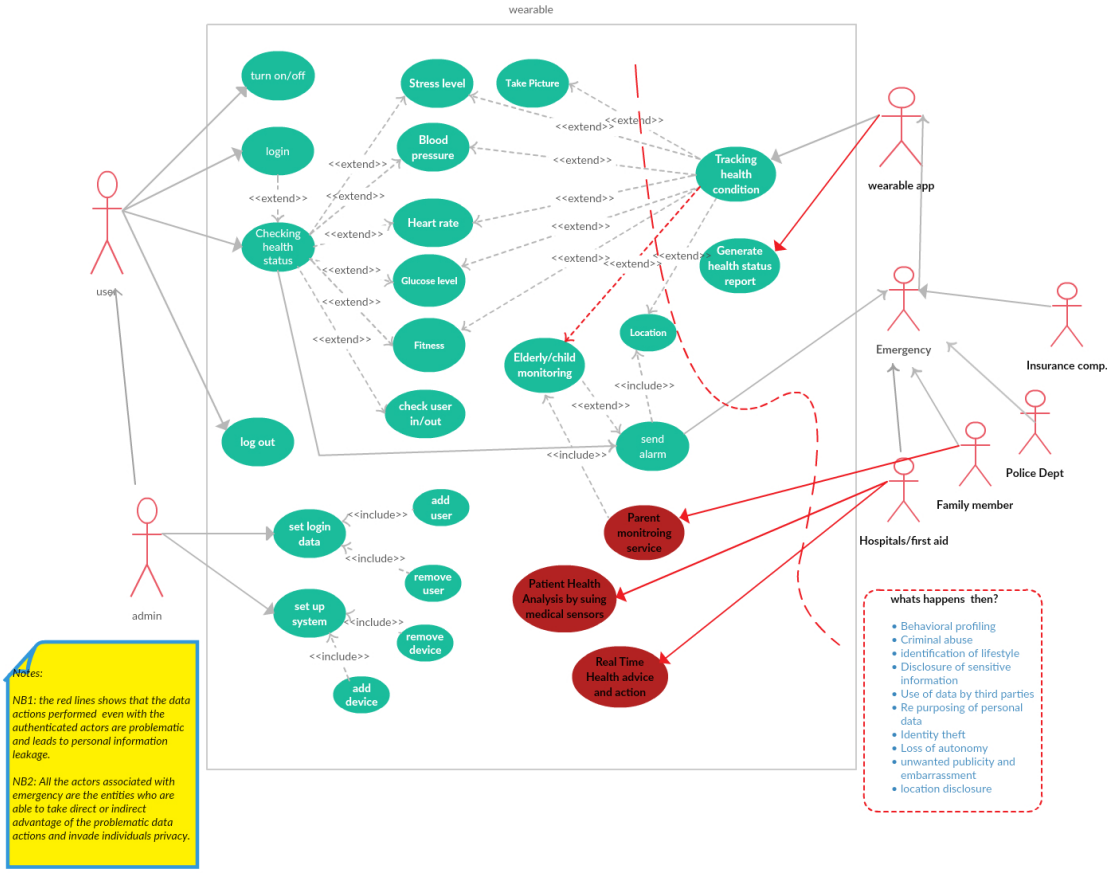

Figure 6.3: Wearables use case digaram

Table 6.2: Privacy Concerns Related to Wearable's

Entities potentially using collected data	Privacy Concerns
Hospitals	Wearable's will enable a broad range of health-related applications: sharing data with your health provider, it gives a record of everything you have done, day in and day out, possibly even some things you don't want to be reminded of.
Insurance companies	Wearable's will enable also sharing data with an insurance company (e.g., to confirm compliance with a medication regimen data from fitness wearables could be used to identify customers who are unhealthy or living a dangerous lifestyle and this could be taken into account by insurers when calculating a premium amount). Insurers can also penalize customers if they fail to disclose such risk factors and negatives, which brings up the important element of non-disclosure so wearable allow insurance company interpreting the data in a way that allows it to penalise customers.
Private investigators	Wearable device just knows when to take pictures of the epic moments, know if you're riding in your car so your friends and stalkers know where you are at all times of the day, know when you go to sleep, riding a car, or climbing a mountain.
Thieves and stalkers	Smart watches, often use a screen to display notifications. These notifications can include sensitive or confidential information, which is also accessible to people located close to the end user.

From the above tables[Table 6.2, Table 6.1] we have identified the following general risk associated with the use of smart meter and wearables. After finding out risks we have labeled the probability of their occurrence from low to high depending on the likelihood of their occurance and their related impact if they occur for each of the use cases. Here are the general risk terms selected to draw risk/impact graph:

R_1= Behavioral Profiling

R_2=Criminal Abuse

R_3=Identification of life style

R_4=Disclosure of Health Information

R_5=Disclosure of Sensitive Information

R_6=Use of data by third parties

R_7=Repurposing of personal data

R_8=identity theft

R_9= Unwanted publicity and embarrassment

R_{10}= Location disclosure

R_{11}=loss of Autonomy

Step 2: Probability/Impact Chart

Once we have extrapolated all the data that is necessary to estimate their scale of occurrence and impact they cause, we will draw the following graph to show the level of the impact they cause. Before performing the analysis of the likelihood and impact we have divided the cases of analysis in to two: individual and

business.

Case 1: Individual case: In this section the general focus of the analysis is to show the impact of smart home products on data subjects. In order to calculate the privacy impact, we used all the risks associated to the data actions we have identified in the two use cases and an estimation of scale based on what we have collected in the tables.

The probability matrix chart is scaled from 1-10. (to give on scale average for the probability and the risk) Based on the data available in the tables [6.2, and 6.1].

Likelihood: Is assessed as probability that a data action will become problematic for a representative or typical individual whose personal information is being processed by the system. It is scaled as:

Low - is if the probability of the occurrence of the risk is low.
Medium - is if the probability of the occurrence of the risk is medium.
High - is if the probability of the occurrence of the risk is high.

Impact: is assessed as the costs (physical, social, economical and psychological cost) to the individual of a data action if it became problematic for a representative or typical individual whose personal information is being processed by the system. It is scaled as:

Low - is if the impact of the occurrence of the risk is low.
Medium - is if the impact of the occurrence of the risk is medium.
High - is if the impact of the occurrence of the risk is high.

We have labled all the risk associated to all the data actions from R1 to R18.

Data Actions	Problems to individuals	Label Name	Likelihood	Impact
DA1	Behavioural Profiling	R1	9	9
	Criminal Abuse	R2	9	7
	Loss of Autonomy	R3	7	7
	Use of data by third parties	R4	7	5
	Identity theft	R5	8	5
	Identification of life style	R6	8	9
DA2	Behavioural Profiling	R7	8	9
	Criminal Abuse	R8	8	8
	Loss of Autonomy	R9	9	9
	Use of data by third parties	R10	7	8
	Identity theft	R11	8	4
	Identification of life style	R12	7	8
DA3	Behavioural Profiling	R13	9	9
	Criminal Abuse	R14	9	6
	Loss of Autonomy	R15	8	6
	Identity theft	R16	9	8
	Identification of life style	R17	8	9

Table 6.3: Smart Meter Problem Prioritization Table

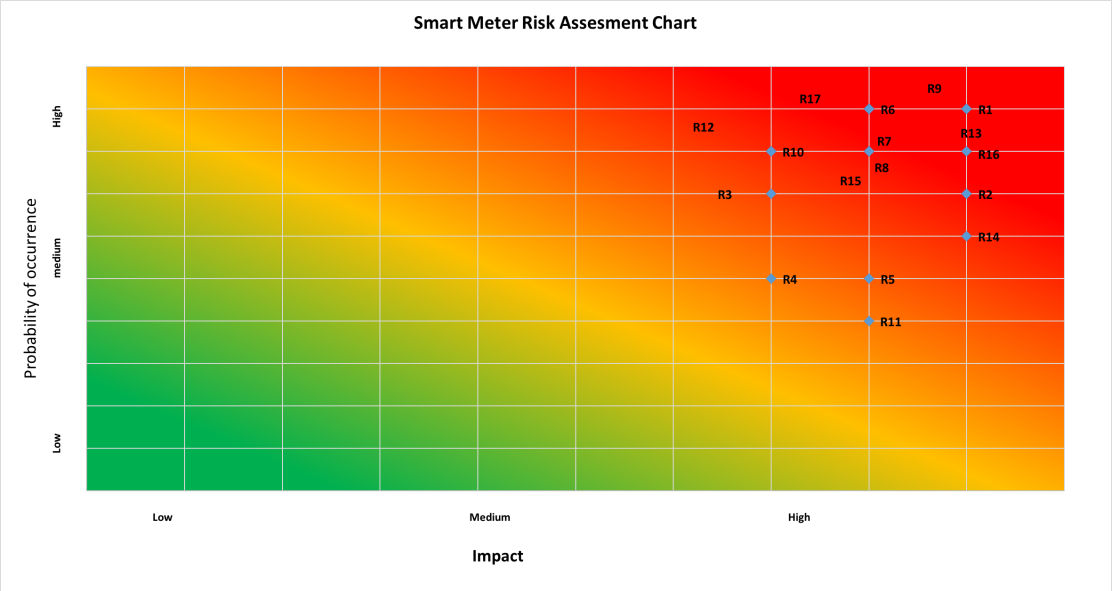

Figure 6.4: Smart Meters Risk Assesment Chart

Data Actions	Problems to individuals	Label Name	Likelihood	Impact
DA4	Disclosure of Sensitive Information	R1	9	9
	Criminal abuse	R2	7	9
	Behavioral profiling	R3	9	8
	Unwanted publicity /Embarrassment	R4	9	8
	Disclosure of Location	R5	8	9
	Identification of lifestyle	R6	9	7
DA5	Disclosure of Sensitive Information	R7	8	9
	Criminal abuse	R8	3	4
	Behavioral profiling	R9	7	6
	Unwanted publicity /Embarrassment	R10	6	7
	Disclosure of Location	R11	9	8
	Identification of lifestyle	R12	8	7
DA6	Disclosure of Sensitive Information	R13	9	8
	Criminal abuse	R14	8	6
	Behavioral profiling	R15	9	9
	Unwanted publicity /Embarrassment	R16	6	6
	Disclosure of Location	R17	9	4
	Identification of lifestyle	R18	9	6

Table 6.4: Wearables Problem Prioritization Table

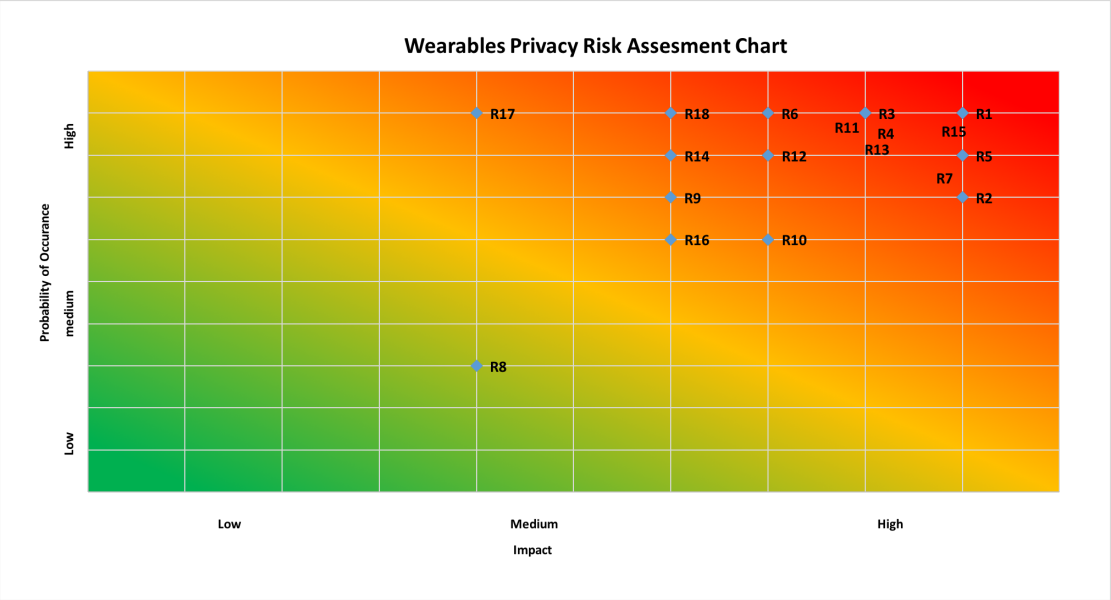

Figure 6.5: Wearables Privacy Risk Assement chart

As its shown in the figure 6.4 and figure 6.5 the corresponding plots of the probability and impact for the associated risks are all above the medium level. This shows that unless there is no any mitigation measure in place for the use of this products, it would rather be a high risk problem than the solution it provides. Misuse of personal data may lead to physical attack, financial loss, social discrimination, reputational damage and other harms.

Case2: Business Case.

After identifying the likelihood of occurrence of problematic action and their impact on individual's privacy we have then performed privacy impact assessment for companies which will be directly/indirectly affected by developing or deploying smart home products. As we did for the individual case, by identifying the problematic data actions of the two real use cases of smart home to calculate the associated likelihood of occurrence and impact, we have also followed the same step for the business impact calculation by considering the four organizational factor costs (non compliance cost, direct cost, reputational and internal costs) and we sum up the final impact they cause to draw their likelihood of occurrence vs total business impact chart.

We assigned on a scale from 1-10, the estimated expected rate of occurrence for each potential problem for individuals whose personal information is being processed per data action and for each associated business impacts.

The difference between this analysis and the previous one is that, the previous chart shows the impact of their occurrence on individual's privacy and this one shows the impact of the previous individuals risk occurrence in business. Understanding the business cost of privacy risk on companies could help them to consider the implementation of privacy by design before deploying the smart home solutions.

In order to show their business impact, we used the combination of both data actions presented by smart meters and wearables that have been identified for individual case and calculate their corresponding risks, if they happen to the users.

Likelihood: Is Probability that a data action will become problematic for the company when it affects the individual whose personal information is being processed by the system. It's scaled from 1-10.

Business Impact: Cost to the organization of a data action if it become problematic for a representative or typical individual whose personal information is being processed by the system. To understand the total business impact, we used PRAM framing process with impact analysis focused on the four organizational factors which are:

Non-compliance costs: Regulatory fines, litigation costs, remediation costs.

Direct costs: Revenue loss from customer abandonment, etc .

Reputational costs: Brand, damage, loss of customer trust, etc.

Internal culture costs: Impact on capability of organization/unit to achieve vision/mission.

Same as before, we are still considering companies with no any mitigation measures in place. Once we have the total business impact, we gave label name to all the associated Risk from A-II. So that it could be easy to plot them in the chart. We gave an estimated scale from 1-10 to the likelihood of their occurrence.

Table 6.5: Business Impact Factors

Data Action	Problems to Individuals	Non-compliance cost	Direct cost	Reputational cost	Internal cost	Total buisiness impact
Detailed Collection of usage statistics of the device and environmental data	Behavioral Profiling	8	6	9	4	27
	Criminal Abuse	9	7	9	6	31
	Loss of Autonomy	7	6	7	4	24
	Use of data by third parties	8	5	7	2	22
	Identity theft	5	6	8	6	25
	Identification of life style	4	6	8	5	23
Granular energy data and appliance energy consumption profiles	Behavioral Profiling	7	7	8	6	28
	Loss of Autonomy	5	6	5	4	20
	Criminal Abuse	9	9	9	9	36
	Use of data by third parties	7	6	8	5	26
	Identity theft	8	7	9	6	30
	Identification of life style	5	4	9	6	24
Perform Real-Time remote Surveillance	Behavioral Profiling	6	7	9	5	27
	Criminal Abuse	9	9	9	9	36
	Loss of Autonomy	6	8	9	5	28
	Identity theft	7	7	9	7	30
	Identification of life style	6	7	8	6	27
Analysis of Health of the patient by using Medical Sensors	Disclosure health informat	9	8	9	8	34
	Criminal abuse	9	9	9	8	35
	Behavioral profiling	7	6	8	5	26
	Disclosure of Location	7	5	8	4	24
	Unwanted publicity and En	9	5	9	7	30
	Identification of lifestyle	6	7	7	6	26
Real Time Health Advice and Action	Disclosure health informat	9	8	8	6	31
	Criminal abuse	9	9	9	9	36
	Behavioral profiling	8	7	8	6	29
	Unwanted publicity and En	9	9	9	7	34
	Disclosure of Location	4	6	7	5	22
	Identification of lifestyle	6	7	8	6	27
Parent Monitoring Services	Disclosure health informat	9	7	9	6	31
	Loss of Autonomy	6	5	7	5	23
	Behavioral profiling	5	7	6	6	24
	Unwanted publicity and En	9	8	8	8	33
	Disclosure of Location	5	5	5	5	20
	Identification of lifestyle	5	5	8	6	24

Table 6.6: Problem Prioritization Table

Data Action	Problems to Individuals	Label name	Liklihood	Total buisiness impact
Detailed Collection of usage statistics of the device and environmental data	Behavioral Profiling	A	9	27
	Criminal Abuse	B	7	31
	Loss of Autonomy	C	7	24
	Use of data by third parties	D	5	22
	Identity theft	E	5	25
	Identification of life style	F	9	23
Granular energy data and appliance energy consumption profiles	Behavioral Profiling	G	9	28
	criminal abuse	H	9	36
	Loss of Autonomy	I	8	20
	Use of data by third parties	J	8	26
	Identity theft	K	4	30
	Identification of life style	L	8	24
Perform Real-Time remote Surveillance	Behavioral Profiling	M	9	27
	Criminal Abuse	N	6	36
	Loss of Autonomy	O	8	28
	Identity theft	P	8	30
	Identification of life style	Q	9	27
Analysis of Health of the patient by using Medical Sensors	Disclosure health information	R	9	34
	Criminal abuse	S	7	35
	Behavioral profiling	T	9	26
	Disclosure of Location	U	9	24
	Unwanted publicity and Embarrassment	V	8	30
	Identification of lifestyle	W	9	26
Real Time Health Advice and Action	Disclosure health information	X	8	31
	Criminal abuse	Y	3	36
	Behavioral profiling	Z	7	29
	Unwanted publicity and Embarrassment	AA	6	34
	Disclosure of Location	BB	9	22
	Identification of lifestyle	CC	8	27
Parent Monitoring Services	Disclosure health information	DD	9	31
	Loss of Autonomy	EE	8	23
	Behavioral profiling	FF	9	24
	Unwanted publicity and Embarrassment	GG	6	33
	Disclosure of Location	HH	9	20
	Identification of lifestyle	II	9	24

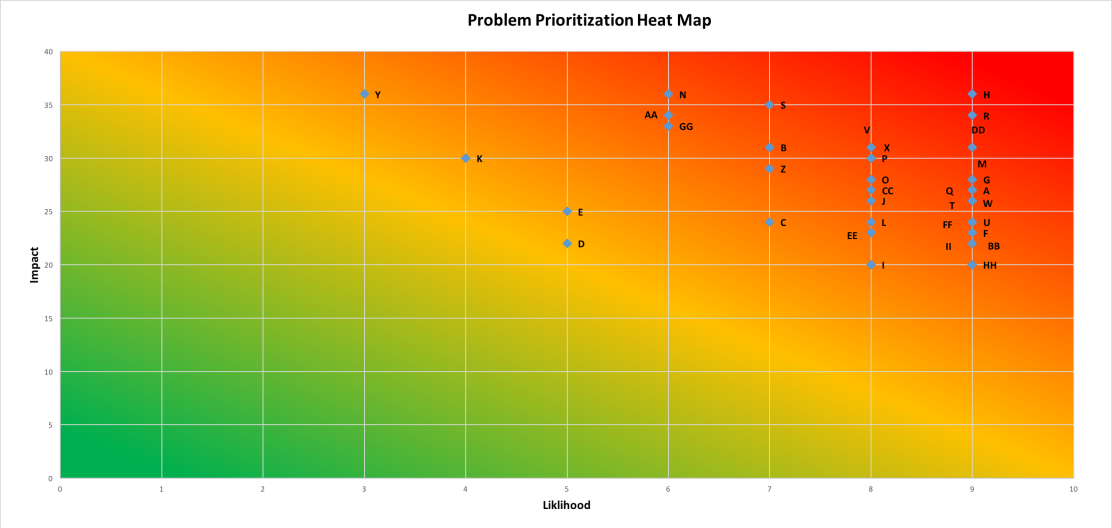

Figure 6.6: Problem Prioritization Heat Map

Chapter 7

Conclusion and Future Work

Data collection and processing are the main critical components of smart home technologies. Privacy issues are thus of utmost importance to smart home researchers, designers, service providers, and users. By Simply providing or offering strong security does not solve privacy issues. Privacy plays an important role in human relationships, enabling us to create interrelation, as well as in personal development and supporting decisional autonomy.

Many people wish to control and personal information flows about themselves, but they often differ widely about what kinds of information they want to control. In this study, we have tried to identify the main privacy issues while using smart home solutions and motivate key concept in personal privacy that should influence the design and implementation of what we would call privacy-aware smart home solutions, and other systems that take the the activities of our everyday life into account and try to prevent unintended personal border crossings. We mainly focused at raising awareness regarding the products used in Smart Home environments in protecting the privacy of the inhabitants.

We have shown that, despite the usage of secure encrypted wireless communications in Smart Home environments, relevant personal information such as users' presence, location and behaviour pattern can be leaked. Even though we are yet far from presenting technical implementations of these concepts, we nevertheless believe that a proper analysis of such non-technical aspects will provide beneficial to the overall system design in the field of Smart home.

To build privacy-aware or privacy-compliant smart home technologies, we need to understand the nature of privacy, its social and legal realities, and the technical tools at our disposal. We introduced those aspects in detail. While there is a long way to go to build smart devices and applications that are actually privacy-intensified, this work brings insight in clarifying the privacy concerns, the associated risk about smart home products, aiding to devise better solutions in the future.

The paper is not intended to show the disadvantages of this technology rather its intended to show the limitations so that it will keep moving up with less impacts on stakeholders. As we understood from the analysis we saw that it creates a high impact so we recommend that companies deploying smart home services should place countermeasures by using different existing frameworks, and guidelines in order to mitigate the risk of such privacy leaks so that they can also reduce the impact on individual as well as the business itself.

For future work, we would like to focus on developing a privacy guideline in which companies could consider in their design while planning to provide smart home

services to their customers, and afterwards creating Privacy Manager interface, to help non- expert users of smart devices which define and administrate their privacy preferences, offering different applications to control related aspects of personal privacy.

Bibliography

[1] ZigBee Alliance. Ieee 802.15. 4, zigbee standard. *On http://www. zigbee. org*, 2009.

[2] Shui Bin, Li Jun, and Global Buildings Performance Network. *Building Energy Efficiency Policies in China: Status Report*. Global Buildings Performance Network, 2012.

[3] Paolo Bonato. Advances in wearable technology and applications in physical medicine and rehabilitation. *Journal of NeuroEngineering and Rehabilitation*, 2(1):2, 2005.

[4] Sean Brooks, Ellen Nadeau, Michael Garcia, Naomi Lefkovitz, and Suzanne Lightman. Privacy risk management for federal information systems. 2015.

[5] Marie Chan, Eric Campo, Daniel Estève, and Jean-Yves Fourniols. Smart homes - current features and future perspectives. *Maturitas*, 64(2):90–7, Oct 2009.

[6] Marie Chan, Daniel Estève, Christophe Escriba, and Eric Campo. A review of smart homes—present state and future challenges. *Computer methods and programs in biomedicine*, 91(1):55–81, 2008.

[7] Paul Darbee. Insteon: The details. *Smarthome Technology*, pages 1–64, 2005.

[8] Scott Davidoff, Min Kyung Lee, Charles Yiu, John Zimmerman, and Anind K Dey. Principles of smart home control. In *UbiComp 2006: Ubiquitous Computing*, pages 19–34. Springer, 2006.

[9] Nigel Davies and Marc Langheinrich. Privacy by design [from the editor in chief]. *IEEE Pervasive Computing*, (2):2–4, 2013.

[10] Paul De Hert and Vagelis Papakonstantinou. The proposed data protection regulation replacing directive 95/46/ec: A sound system for the protection of individuals. *Computer Law & Security Review*, 28(2):130–142, 2012.

[11] Liyanage C De Silva, Chamin Morikawa, and Iskandar M Petra. State of the art of smart homes. *Engineering Applications of Artificial Intelligence*, 25(7):1313–1321, 2012.

[12] W Keith Edwards and Rebecca E Grinter. At home with ubiquitous computing: Seven challenges. In *Ubicomp 2001: Ubiquitous Computing*, pages 256–272. Springer, 2001.

[13] Rachel L Finn, David Wright, and Michael Friedewald. Seven types of privacy. In *European data protection: coming of age*, pages 3–32. Springer, 2013.

[14] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors*, 12(9):11734–11753, 2012.

[15] Smart Grid Interoperability Panel Cyber Security Working Group et al. Introduction to nistir 7628 guidelines for smart grid cyber security, 2010.

[16] Jason I Hong, Jennifer D Ng, Scott Lederer, and James A Landay. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In

Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques, pages 91–100. ACM, 2004.

[17] Kamrul Islam, Weiming Shen, and Xianbin Wang. Security and privacy considerations for wireless sensor networks in smart home environments. In *Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on*, pages 626–633. IEEE, 2012.

[18] Nikos Komninos, Eleni Philippou, and Andreas Pitsillides. Survey in smart grid and smart home security: issues, challenges and countermeasures. *Communications Surveys & Tutorials, IEEE*, 16(4):1933–1954, 2014.

[19] John Krumm. *Ubiquitous computing fundamentals*. CRC Press, 2009.

[20] Delfina Malandrino, Andrea Petta, Vittorio Scarano, Luigi Serra, Raffaele Spinelli, and Balachander Krishnamurthy. Privacy awareness about information leakage: Who knows what about me? In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, pages 279–284. ACM, 2013.

[21] Brent A Miller and Chatschik Bisdikian. *Bluetooth revealed: the insider's guide to an open specification for global wireless communication*. Prentice Hall PTR, 2001.

[22] Vittorio Miori, Luca Tarrini, Maurizio Manca, and Gabriele Tolomei. An open standard solution for domotic interoperability. *IEEE Transactions on Consumer Electronics*, 52(1):97, 2006.

[23] Vivian Genaro Motti and Kelly Caine. Users' privacy concerns about wearables. In *Financial Cryptography and Data Security*, pages 231–244. Springer, 2015.

[24] Michael Angelo A Pedrasa, Ted D Spooner, and Iain F MacGill. Coordinated scheduling of residential distributed energy resources to optimize smart home energy services. *Smart Grid, IEEE Transactions on*, 1(2):134–143, 2010.

[25] Jody Ranck. The wearable computing market: a global analysis. *Gigaom Pro*, 2012.

[26] Rosslin John Robles and Tai-hoon Kim. Applications, systems and methods in smart home technology: a review. 2010.

[27] Lalitha Sankar, S Raj Rajagopalan, Soheil Mohajer, and H Vincent Poor. Smart meter privacy: A theoretical framework. *smart grid, IEEE transactions on*, 4(2):837–846, 2013.

[28] Vijay Srinivasan, John Stankovic, and Kamin Whitehouse. Protecting your daily in-home activity information from a wireless snooping attack. In *Proceedings of the 10th international conference on Ubiquitous computing*, pages 202–211. ACM, 2008.

[29] Samuel D Warren and Louis D Brandeis. The right to privacy. *Harvard law review*, pages 193–220, 1890.

[30] Alan F Westin. Privacy and freedom. 1970.

[31] Di Zhang, Nilay Shah, and Lazaros G Papageorgiou. Efficient energy consumption and operation management in a smart building with microgrid. *Energy Conversion and Management*, 74:209–222, 2013.