An Exploratory Study of the Security and Privacy Issues Affecting the Adoption of the Internet of Things

Cathal Enright

A dissertation submitted to the University of Dublin
in partial fulfilment of the requirements for the degree of
MSc in Management of Information Systems

1st September 2016

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: _____

Cathal Enright

1st September, 2016

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics,
Trinity College may lend or copy this dissertation upon request.

Signed: _____

Cathal Enright

1st September, 2016

Acknowledgements

I would like to specially thank my supervisor, Patrick Joseph Wall for his advice and helpfulness. PJ has been an excellent mentor and has provided invaluable guidance, encouragement and expertise.

I would like to thank my family Aine, Oisin and Caoimhe for their love and support. I would also like to thanks my girlfriend Rachael who has been very helpful, caring and patient at times! I would like to thank my friends who have supported me the past two years.

Finally, I would like to thank the participants that took part in this research without them this research would not have been possible.

Abstract

Every now and then a new technology is introduced to the world that becomes a prominent feature of our lives. Weiser (1991) envisioned that "*the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it*". The Internet of Things (IoT) has the capability of doing just that as it is "*set to be the next big revolutionary technological change, it will change the way we live our lives"* (Singh, Tripathi et al. 2014). IoT is the next "*technological revolution*" (Tan and Wang 2010).

With the rise world-wide of smart technologies and 'smart' device ownership, IoT has emerged as one of the major trends shaping the future of technology. Everyday items such as TVs, cars, watches, light bulbs and refrigerators etc. are already being connected to the internet and many more are in development stages.

Although the IoT will add to the convenience in our lives, it will also create additional risks. Like all new developments, there is a potential for both increased opportunities and threats for users. According to an array of academic research papers ((Skarmeta and Moreno 2013) (Das 2015)), security and privacy are key concerns for IoT technology and its expansion into widespread use.

This paper aims to address the issue of IoT security and privacy by interviewing a group of IoT users about their concerns and perceptions on the subject. The paper highlights how existing approaches to ensure security in IoT are incomplete, and that many weaknesses and threats to its end users exist. The study will discuss the challenges and provide analysis for future research work to enable a more secure IoT environment.

Table of Contents

List of Figures

List of Abbreviations

BYOD	Bring Your Own Device
CIO	Chief Information Officer
CPS	Cyber Physical Systems
CPM	Communication Privacy Management
DNSSEC	DNS Security Extensions
DPD	(The EU) Data Protection Directive
FTC	Federal Trade Commission
ICT	Information and Communication Technology
IDOT	Internet Data of Things
IEEE	The Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IS	Information Systems
IST	Information Systems Theory
ITU	International Telecommunications Union
M2M	Machine to Machine
NFC	Near Field Communication
OWASP	Open Web Application Security Project
PET	Privacy Enhancing Technology
PIR	Private Information Retrieval
PMT	Protection Motivation Theory
RFID	Radio Frequency Technology
TCD	Trinity College Dublin
TLS	Transport Layer Security
T2T	Thing-to-Thing
SC&C	Smart Cities and Communities
SG20	Study Group 20
VPN	Virtual Private Networks
WSN	Wireless Sensor Networks

Chapter 1: Introduction

1.1 Context and Background

The term, "IoT" (Internet of Things), was used for the first time by Kevin Ashton at the MIT Auto-ID centre in 1998 (Ashton 2009). According to Ashton IoT has the potential to change the world even more than the internet has done. The MIT Auto-ID centre presented their IoT vision in 2001 (Brock 2001). Later, IoT was formally introduced by the International Telecommunication Union (ITU 2005).

IoT was originally referred to in relation to supply change management (Gubbi, Buyya et al. 2013, p.2). In its early stage, IoT used RFID tags, and thereafter, the concept has changed little by little up to the point of the current ubiquitous computing environment (Lee 2016).

In the past the majority of internet connections were devices operated and controlled by people, but this is changing. The basic idea of IoT is attaching embedded devices to everyday objects, turning them into ‘smart’ devices. As a growing number of objects can be connected via the internet, the number of connected “things” will be greater than the number of “people” (Tan and Wang 2010). The idea of connecting physical objects to the digital world is not a new concept, it is only recently however that the development and acceptance of radio frequency identification (RFID) and wireless sensor network (WSN) technologies have made the IoT a feasible technology.

IoT has become one of the largest growing technologies in recent times. Gartner states that the number of wireless devices is set to hit 25 billion by 2020. Sundmaeker (2010) goes further and estimates there will be between 50 and 100 billion connected devices by 2020.

Billions of IoT devices will require large distributed networks and also a process of transforming raw data into something more meaningful (Singh, Tripathi et al. 2014). IoT is going to change the way we live our lives by simplifying day-to-day tasks (Weber 2016). Coetzee (2011) explains that the technology advancements in IoT will lead us to an “always connected paradigm”. There is no stopping IoT, with market research showing an

increase in sensor deployments over the past decade. This growth is predicted to continue into the future (Perera, Zaslavsky et al. 2014).

This rise in connected objects will inevitably lead to a rise in vulnerabilities, there will be more ways for systems to become compromised. "*IoT technology will be a challenge to social, economic and legal norms. Specifically IoT technologies raise a variety of privacy and safety concerns*" (Thierer 2015) IoT is in its infancy, and the true security and privacy risks have yet to be fully discovered and mitigated.

1.2 Research Questions

The following primary research question will be examined in this study:

“Will Security and Privacy Threats Prevent IoT Adoption?”

This research paper aims to address users’ privacy and security concerns when using IOT devices. It is a very topical subject in the academic and business community at present. The other research elements presented by this study focuses on these key questions:

- Which are the IoT devices most commonly used by consumers?
- Are users aware of the private information they share when using IoT devices?
- What are technology users’ general security perceptions?
- Are users willing to share private information?
- Do users have any thoughts about if the data on these devices are stored safely and where?
- Do users have any opinions on the risks in using IoT objects?

1.3 Importance of the Research

The IoT is a relatively new concept and an emerging area for research in the IT community. According to Dijkman (2015) IoT is a vision of a global infrastructure of networked physical objects, and it is growing dramatically. "*The number of connected things has increased threefold over the past five years*" (Dijkman 2015). It will allow devices to communicate to one another (M2M) and will turn everyday items into "smart objects".

According to a new forecast from International Data Corporation (IDC), the IoT has made a huge impact on the IT industry and is set to grow substantially over the next years (MacGillivray 2015). All of the key players in technology such as Apple, Microsoft, Google and IBM are investing in this growing market, which is set to reach a value of $235 billion in 2016, according to Gartner (van der Meulen 2015).

Evans (2011) enforces the idea of IoTs' importance on the world today it will change everything and it represents the next evolution of the Internet. It is envisioned that the Internet of Things will revolutionise how individuals and corporations interact with the digital and physical world (Xu, Wendt et al. 2014). IoT is clearly an influential technology, on which extensive research is needed to ensure its success. This paper will add to that research.

This study will focus on the security and privacy aspect of IoT which many researchers believe to be a major concern (Weber 2010, Roman, Zhou et al. 2013, Da Xu, He et al. 2014). According to Woods (2016) "*by 2020, addressing compromises in IoT security will have increased security costs to 20% of annual security budgets, from less than 1% in 2015"* . Gartner identified that IoT security is a top ten priority for every organisation looking to adopt IoT technologies within the next two years, and also predicts that spending on IoT security is expected to reach $547 million in 2018(Van der Meulen 2016). The US Intelligence Community put IoT as a major cyber technology threat stating that it "*can threaten data privacy, data integrity, or continuity of services*"(Clapper 2016)

A study on how the security and privacy challenges affect end user adoption of the IoT technology is useful for the academic community and also IoT technology companies. This thesis will be one of the few qualitative studies done on the IoT and the privacy implications to its users.

1.4 The Scope of the Research

This research aims to explore the impact of the underlying security and privacy issues within the IoT. The study will conduct in-depth semi-structured interviews with a range of interviewees (18 years and over) who are users of IoT devices. The study will specifically focus on the privacy and security implications associated with using IoT technology.

The initial analysis will be devised from the interviews using an inductive approach. The findings will arrange the responses into key themes. The study will observe how the Protection Motivation Theory (PMT) and Communication Privacy Management Theory (CPM) are underlying theories and form a basis to the participants rational.

1.5 Chapter Structure

The chapters of this dissertation are structured as follows:

Chapter 1 - Introduction

This chapter presents the context and background information on the research topic. The research questions are presented and the importance of the study is discussed.

Chapter 2 - Literature Review

This chapter critically reviews and examines the relevant literature to the research question. The chapter defines the IoT and its impact on technology. The chapter then discusses the relevant enabling technologies of IoT. The benefits of the IoT are outlined and its importance. The security risks are discussed in great details. Finally, the privacy, governance and legal issues are discussed.

Chapter 3 - Methodology

This chapter defines the methodological approaches available. The philosophies, approach and research strategies are presented and then the research choice is justified. The time horizon, population and sampling are then discussed. The ethical considerations are explained. Finally the limitations to the methodological approach and the lessons learnt are outlined.

Chapter 4 - Findings and Analysis

This chapter presents the analysis and findings of the data collected during the research. The qualitative research is analysed and then the themes and finally the theories that emerge are discussed.

Chapter 5 - Conclusions and Future Works

This chapter concludes the dissertation. The answers to the research questions are discussed. The key findings of the research are presented. Finally, the limitations and future works are considered.

Chapter 2: Literature Review

2.1 Introduction

The aim of this chapter is to present a comprehensive review of the literature relevant to IoT and also to highlight the key themes and trends to emerge from current studies on the topic. The chapter provides theoretical content of previous research carried out in the field of IoT. The literature review includes journal articles, conference papers, books and edited volumes. The research goes in depth to focus on the privacy and security issues around this technology. Relevant literature was identified by searching databases for terms such as “Internet of Things”, “IoT”, and ”security and privacy”.

This literature review examines the research under the following topics:

• An introduction to IoT

• What is IoT?

• IoT enabling technologies

• The importance of IoT

• IoT security

• IoT privacy, governance and legal issues

2.2 What is IoT?

The Internet of Things (IoT), is a new wave of technology devices. In basic terms, they are everyday objects which connect and communicate over the internet. There are in fact more objects connected to the internet than there are people in the world today (Evans 2011).The term IoT first appeared in a technical report by ITU (2005).

IoT devices are usually called “smart devices”, and have a wide variety of uses and functionalities (Leo, Battisti et al. 2014). A smart device can be defined as a device with the following characteristics: a) a physical presence b) communication facilities c) unique identification d) the ability to sense and interact with its environment (Fisher and Hancke 2014). By embedding electronics into everyday objects, making them ‘smart’, a global cyberphysical infrastructure is created (Issarny, Georgantas et al. 2011).

In the world of IoT, everything real becomes virtual, which means that each person and thing is locatable and addressable, and is a readable object on the internet. IoT promises extending computing to “*anything, anyone, any service*” (Desai 2016). These “things” can range from objects and environments, to vehicles and clothing. IoT devices will even have “*the ability to sense, communicate, network and produce new information, becoming an integral part of the Internet*”(Revell 2013).

Figure 1: IoT Global Connectivity. Source: (El Kaliouby 2015)

There have been quite a number of definitions for the term Internet of things since its first use by Kevin Ashton in a presentation titled “Internet of Things”(Ashton 2009). However, the literature on IoT does not yet provide an exact definition that is universally agreed by scholars. The definition of IoT is a subject of some debate, due to the influence of several contributing trends, as well as various interpretations of the phrase (Uckelmann, Harrison et al. 2011).

Minerva (2015) who is an author at The Institute of Electrical and Electronics Engineers (IEEE) created a paper to address this issue. This study will use the same definition Minerva used: “*IoT is a network that connects uniquely identifiable ‘Things’ to the Internet. The ‘Things’ have sensing/actuation and potential programmability capabilities. Through the exploration of unique identification and sensing, information about the ‘Thing’ can be collected and the state of the ‘Thing’ can be changed from anywhere, anytime, by anything*”. This definition is used because it is a concise and clear explanation of how to identify an IoT object.

Another key definition describes it as follows: “‘Internet of Things’ semantically means ‘a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols’” (Bassi and Horn 2008). Borgohain (2015) explains the IoT term as “the concept of free flow information among the various embedded computing devices using wireless communications such as the internet as the mode of intercommunication”.

Finally, Chen (2014) describes IoT as follows, “It is an extension and expansion of Internet-based network, which expands the communication from human and human to human and things or things and things. In the IoT paradigm, many objects surrounding us will be connected into networks in one form or another. RF identification (RFID), sensor technology, and other smart technologies will be embedded into a variety of applications”

For this research paper, IoT will refer to “smart” objects such as devices or sensors - other than computers, smartphones or tablets, that communicate information through wireless technologies mainly across the internet.

2.3 IoT Enabling Technologies

The advancements in communication technologies have helped in creating the IoT landscape. This section will provide a brief overview of IoT enabling technologies and their importance. As noted by Atzori (2010) "*actualization of the IoT concept into the real world is possible through the integration of several enabling technologies*".

IoT's advancements through communication channels have been a big factor in its adoption as devices are enabled by wireless technologies. The following technologies are some of the key enablers: Bluetooth, radio frequency identification (RFID), Wi-Fi and NFC. Yan (2008) believes that "*IoT has stepped out of its infancy stages and is on the verge of transforming the current static Internet into a fully integrated Future Internet*".

IoT devices should be context aware, i.e. they are capable of sensing an awareness of their physical environment and the situation in order to be able to act and answer in a proactive and intelligent way (Abowd, Dey et al. 1999, Hong, Suh et al. 2009). IoT is the concept of Cyber Physical Systems (CPSs) which are technologies that monitor data from sensors via cellular networks (Rajkumar, Lee et al. 2010).

The advancements to the enablers of IoT is what is driving its growth within companies. Goldman Sachs Global Investment Report (Jankowski, Covello et al. 2014) states the following key advantages to IoT: 1) Cost of sensors significantly dropping to an average of 60 cents down from $1.30 in the past 10 years. 2) Processing costs have declined by nearly 60 times over the past 10 years enabling devices not only to be connected but also to know what to do with all the new data being generated. 3) The cost of bandwidth has declined enormously, by nearly 40X over the past 10 years. These all factored into the rise in IoT and its popularity. An overview of IoT's enablers is presented below.

2.3.1 RFID (Radio Frequency Identification)

RFID (Radio Frequency Identification) is often thought of as the prerequisite to IoT technologies. An RFID system consists of tags (responders and receivers). The tag has a microchip connected with an antenna, which can be attached to an object as an identifier of the object (Jia, Feng et al. 2012). RFID can be defined as an "*automatic technology and aids machines or computers to identify objects, record metadata or control individual target*

through radio waves" (Jia, Feng et al. 2010). RFID enables the identification of objects from a distance, and unlike earlier bar-code technology it does so without line of sight (Finkenzeller 2003), this is very useful in the context of the IoT.

The IoT is made possible when RFID readers are connected online, the readers distributed throughout the world can track and monitor the objects attached with tags globally, automatically, and in real time (Jia, Feng et al. 2012).

Figure 2: RFID Tag, Source: (Ogden 2014)

2.3.2 WSN (Wireless Sensor Networks)

Wireless Sensor Networks (WSN) also have a huge role to play in the development of IoT. Akyildiz (2002) defines WSN technologies as "*tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes.*" The usefulness of this technology can be attributed to the recent advancements in sensors, they have become a lot more feasible due to their ability communicate untethered over short distances, they are low-cost to produce and use up little energy (Akyildiz and Vuran 2010).

WSN allows IoT devices to share information across platforms in order to develop a common operating picture (COP)(Gubbi, Buyya et al. 2013). Atzori (2010) explains that

WSN are of a high radio coverage and communication paradigm, which does not require the presence of a reader.

Gubbi (2013) commented on the technologies as follows, “with the growing presence of WiFi and 4G-LTE wireless Internet access, the evolution towards ubiquitous information and communication networks is already evident”. WSN makes the ‘always connected’ feature of IoT devices a reality.

Figure 3: WiFi chip, Source: (Tangient)

2.3.3 NFC (Near Field Communication)

Near Field Communication (NFC), is a bridge between the physical and virtual world for devices. NFC is a short-range communication standard where devices are able to engage in radio communication with one another when touched together or brought into close proximity to one another (Whitmore, Agarwal et al. 2015). The NFC technology has allowed everyday objects such as credit cards to become IoT enabled by allowing wireless transactions.

Figure 4: NFC tag, Source: (Kef 2015)

2.3.4 Bluetooth

Bluetooth is a small, low-cost silicon implementation that can be used as a low powered electronic tag. These tags can operate up to one year on a lithium coin cell battery (240-mah capacity) (Want, Schilit et al. 2015). Bluetooth provides an advantage with its low cost to functionality ratio, it is already used in everyday items like smartphones and now in a variety of IoT devices such as health wearables.

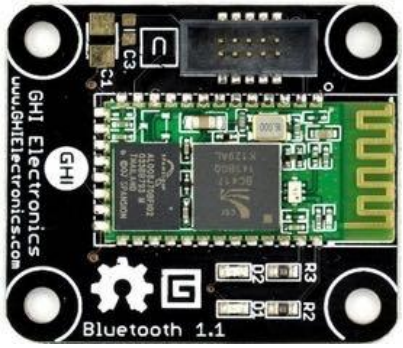

Figure 5: Bluetooth module, Source: (Electronics 2003)

2.4 The Importance of IoT

IoT will help to improve a wide range of industries; this section will provide an overview of its usefulness and how it will have an impact on everyday life. "*IoT should not be seen as a simple extension of the current internet rather as a set of new independent systems that operate their own infrastructures*" (Garrido, Miraz et al. 2010). IoT will not only improve the industries listed below, but also a wider range; the full extent of its capabilities is not yet known.

2.4.1 Healthcare

IoT will have an impact on healthcare, and can be used in assisted living situations. Sensors are placed on health monitoring equipment used by patients. The information collected by these sensors is made available online to doctors, family members and other interested parties in order to improve the quality of service (treatment, responsiveness etc.) (Dohr, Modre-Opsrian et al. 2010). According to Korhonen (2003), health monitoring within smart homes is needed to support independent living for the elderly, and the monitoring IoT tools should compensate functional impairments. An interesting paper by Pantelopoulos (2010) establishes that the advancements in wearable sensor technology will transform healthcare by enabling proactive personal health management and ubiquitous monitoring of a patient's health condition. "*Automatic continuous surveillance of vital parameters enables patients with chronic diseases to leave their hospital ward. Most importantly they are able to live in their own homes*." (Barnickel, Karahan et al. 2010)

2.4.2 Smart Homes

"IoT Technologies are being used in homes and offices that are equipped with sensors and actuators that track utility consumption, monitor and control building infrastructure such as lights and HVAC systems, and conduct security surveillance" (Darianian and Michael 2008). IoT technologies can also improve cities by making traffic control more efficient, monitoring car park space availability, evaluate air quality and provide notifications when waste containers are full (Schaffers, Komninos et al. 2011).

2.4.3 Wearables

An important sub-section of IoT is wearable devices, “clothing and electronics have traditionally been separate industries but now they must work together” (McCann and Bryson 2009, p.25). Wearable computing can be defined by the following categories: smartwatches (Pebble and Apple watch), wrist sensors (FitBit), augmented eyewear (Google Glass) and wearable textiles (Swan 2012).

“Wristband sensors are a predecessor to smartwatches, one of the first examples was using accelerometers to measure steps in products like Nike Fuelband, Jawbone UP wristband and iPhone app, the Adidas MiCoach” (Swan 2012).

2.4.4 Automated Vehicles

The IoT will effect transportation and self-driving cars are beginning to be introduced to the market. Google has developed one and so has Tesla. According to Gerla (2014) “*The Internet of Vehicles will be a distributed transport fabric capable to make its own decisions about driving customers to their destinations. They will have communications, storage, intelligence, and learning capabilities to anticipate the customers’ intentions*”.

2.4.5 Big Data

There is a correlation between IoT and Big Data. Gudivada (2015) explains that over 90% of the world’s data were produced in just the past two years, and that the growth is on track to continue accelerating as we shift towards giga-bit networks, gigapixel cameras, and a data-intensive Internet of Things (IoT). While the data volume collected by devices and sites continue to increase, companies will try to utilise this to gain a competitive advantage in the market.

In a paper published in MIS Quarterly, Awad (2006) examines the relationship between information transparency and consumer willingness to partake in personalisation. Awad(2006) concludes that privacy has become an issue of strategic importance for companies, and that in order to provide consumer-driven personalised service, firms must target consumers who are willing to provide information.

2.5 IoT Security

2.5.1 IS Security and Privacy Threats

Threats to users' security and privacy concerns have been long-standing issues when it comes to Information Systems (IS) and how they are used. Information security manages the way a person or company protects assets from unauthorised disclosure, modification, disruption or destruction (Sattarova Feruza and Kim).

For many years now companies have been investing large amounts of revenue into getting top of the range firewalls, antivirus software, email spam filters and also sophisticated security networks. Gordon (2002), carried out some research in the field of creating a optimal level of resources that companies should invest in their IT security systems. He concludes that "*the amount to spend on information security is an increasing function of the level of vulnerability of such information*". What this means is that the greater the risk, the higher the investment costs needed to protect from the vulnerabilities. Ponemon (2015) conducted a study on the 'Costs of Data Breach', the study found that the average costs of a data breach to a company increased from $3.52 million in 2014 to $3.79 million in 2015.

A huge amount of companies and users have been hacked in recent years; Version(2016) conducted a study on the area of IT security, and found so far in 2016 "*there are 100,000 incidents of which 3,141 were confirmed data breaches*". Hacker groups such as Anonymous are taking on large organisations and costing companies millions of dollars in losses. For example, they cost Paypal 3.5 million in losses in 2012 (Sandra 2012).

Cybercrime is in the top tier of the National Security Strategy of many EU states e.g. France, the Netherlands and the UK. It is becoming the number 1 threat above organised crime and fraud generally (Armin, Thompson et al. 2015). In recent times, various independent surveys have discovered that between 36% and 90% of organisations reported security breaches in the past year (Schatz and Bashroush 2016). The frequency of IT incidents is on the rise at an astonishing rate (Spanos and Angelis 2016).

Not only companies need to be vigilant, but everyday users do as well. While organisations can make investments to train employees on the appropriate security

precautions to take when using technologies, individual home users must take the initiative to educate themselves (Anderson and Agarwal 2010). Credit card fraud online, identity theft, Trojans and malware are a few of the everyday security vulnerabilities that users face when connected online. While the internet has been around for many years, threats to personal security and privacy are huge threats to users. How will a new technology, such as the IoT, mitigate against these attacks & risks?

2.5.2 IoT Security and Privacy Overview

Privacy and Security are identified as major issues in the IoT technology (Desai 2016) (Mayer 2009), (Srinivasan, Stankovic et al. 2008). Both Roman (2011) and Sicari (2015) state that traditional security protection mechanisms and countermeasures are not enough to protect IoT devices, as different standards and communication features are needed. IoT can be viewed as a "*fusion of heterogeneous networks*" according to Zhao (2013) that brings not only the same security challenges as other networks, but also privacy problems, authentication issues and access control challenges. Uckelmann (2011) lists the key societal needs for the Internet of Things as follows: open governance, security, privacy and trustworthiness.

According to Skarmeta (2013), "*IoT security, privacy and trust need to be considered as fundamental designs of sensor systems*", this is due to "serious multi-dimensional problems that face the IoT paradigm". A recent IoT security survey by Brophy (2016) from IOActive revealed that nearly half of all security professionals surveyed felt that less than 10% of all IoT products on the market provide adequate security.

2.5.3 IoT Security Vulnerabilities

The following section outlines a brief overview of the many security vulnerabilities in IoT devices and eco-systems. The level of security of a device is the chance or risk that it will be compromised, the damage this would cause, and the time and resources needed to achieve a level of protection (Mulani and Pingle 2016). OWASP (Open Web Application Security Project) who are an online community of security professionals and researchers created a 'Top Ten' list of IoT security issues (Miessler 2014) . OWASP is a recognised group that highlights IS security issues and aims to raise awareness on them. They are recognised by FTC, Defense Information Systems Agency, PCI DSS and MITRE. Miessler

(2014) devised this 'top ten' list of security vulnerabilities in IoT devices: Insecure Web Interface, Insufficient Authentication, Insecure Network Services, Lack of Transport Encryption, Privacy Concerns, Insecure Cloud Interface, Insecure Mobile Interface, Insufficient Security Configurability, Insecure Software/Firmware and Poor Physical Security. Some of these security issues are detailed below.

Attack vectors

Providing security in IoT devices is a challenge, as IoT architectures need to deal with billions of objects which interact with each other and other entities, and all these interactions must be secured somehow (Roman, Zhou et al. 2013). By its nature, IoT increases security risks – Leo (2014) explains that widespread sensors will have the ability to communicate and process autonomously; this in turn increases the exposure of the devices to a cyber-attack. According to Roman(2013), the number of attack vectors available to malicious attackers might become staggering, as global connectivity ("access anyone") and accessibility ("access anyhow, anytime") are key features of IoT.

Attacks spread quicker

Atzori (2010) identifies that everyday devices generate more security risks, and the IoT could distribute those risks far more widely than the internet has to date. Rose (2015) affirms this view by observing that IoT devices' interconnected nature means that every poorly secured device that is connected potentially affects the security and resilience of the internet globally. The FTC (2015) report describes how IoT devices can facilitate attacks on other systems at a high rate.

Limited resources

IoT devices generally have limited resources, this creates challenges especially considering that IoT sensors have merger resources but need to have "cryptographic primitives and security protocols" (Skarmeta and Moreno 2013). This makes it very difficult to achieve high level security.

IoT Password Limitations

IoT devices are limited in their user interface, many devices do not have keyboards to type a password onto or even screen displays. This means that passwords become a weak security link in these devices, as many devices for example have "default" admin

passwords, weak passwords, and not encrypted data are being sent between devices and open ports (Desai 2016).

A common issue is the use of default passwords on devices, which users are not required to change when setting them up. One website has claimed to find 73,000 webcams accessible over the internet using a known default password (C.Tofel).

Data Integrity

A key issue with IoT described by Abie (2012) is data integrity, which involves authentication, access control and secure communication. The following questions need to be answered (i) How do you trust the data our sensors are sending?, and (ii) How do we even know it is a sensor that is sending data at all, and not a bot or piece of malware?

According to Leo (2014) security should not be thought of only as an add-on of a device, but actually requires an integrated approach across all layers. This means that not only should an IoT device be secure, but the devices it connects to and the network it runs across must also be protected.

Lack of Encryption

In today's internet, wireless communication is typically made more secure through encryption. Encryption is also seen as key to ensuring information security in the IoT (Whitmore, Agarwal et al. 2015). However, to allow IoT devices to be encrypted, algorithms need to be made more efficient and less energy-consuming, and efficient key distribution schemes are needed (Bandyopadhyay and Sen 2011, Roman, Najera et al. 2011).

Eavesdropping

Abie (2012) identified that IoT devices can be attacked easily because communication is mostly wireless and can therefore be eavesdropped, it is usually unattended so can be physically attacked.

2.5.4 IoT Enabling Technologies Vulnerabilities

In section 2.3 the enabling IoT technologies were discussed. These technologies are not without many weaknesses, and the IoT devices also inherit these vulnerabilities. Airehrour (2016) explains that there are many network communication security vulnerabilities which IoT devices must learn to cope with.

Bluetooth - has many location privacy issues because the device is a permanent identifier, making location tracking easy (Wong and Stajano 2005). Hager (2003) created a paper on the known vulnerabilities in Bluetooth technologies. Firstly 'spoofing-through-keys' also known as the man-in-the-middle attack, is when identification and encryption keys are stolen before the start of a session and then used to impersonate or eavesdrop on communications (Jakobsson and Wetzel 2001). Secondly, Hager (2003), identified the 'Pin Length' as another vulnerability; most devices have extremely short (usually four-decimal) pins. The third security flaw found was that each Bluetooth connection has a unique address. Once a device ID is associated with a user of a device, an intruder can change their address to impersonate the user of the spoofed address (Hager and MidKiff 2003).

RFIDs - also have several security and privacy concerns. Firstly, RFIDs respond to reader interrogation without alerting their owners, therefore where the range permits the clandestine scanning of tags is a threat (Juels 2006). When a tag is combined with personal information (e.g. credit card details), marketers can identify the profile of a consumer and target him with advertisements based on what he has purchased (Juels 2006). Abie (2012) found the pervasiveness of RFID tags and readers an issue in IoT because it is possible to collect large amounts of data in order to infer sensitive information. Another issue raised is with authentication; misbehaving readers can gather information from well-behaving RFID tags (Juels 2006). Basic RFID tags are settable to simple counterfeiting attacks (Westhues 2005).

WSNs - have many vulnerabilities also, which IoT devices must mitigate. Firstly the sensor nodes in WSN have limited resources; typically they are limited due to two constraints - limited energy and size, which makes providing security very difficult (Shi and Perrig 2004). WSNs are susceptible to eavesdropping and packet injection by an adversary (Kavitha and Sridharan 2010). WSNs are also vulnerable to attacks when

information is in transit by providing wrong information to the destination (Wang, Attebury et al. 2006).These are just a few of the many attacks and vulnerabilities possible on WSN that IoT must also deal with.

NFC - too has its own security weaknesses and vulnerabilities; these are similar to the other weaknesses already listed. Chattha (2014) identified that they are prone to 'eavesdrop attacks' (the attacker uses a stronger antenna than the IoT device to pick up the communication). Furthermore, 'data corruption' can occur, where the attacker changes the communication data of the device to an unrecognised format (Chattha 2014). Finally, 'data insertion' is possible, where the attacker's rogue data are inserted by the attacker when two devices are exchanging information.

2.5.5 IoT Security in Wearables, Smart Home, Smart TV and Cars

Wearables' security risks

Wearable technology requires a high level of trust. Trust does not only have to exist between user and device, but also among connected devices. As more consumers purchase wearable and IoT devices they unknowingly expose themselves to potential security breaches. Hence, their data may be used by companies legally without the users ever knowing about it. Barnickel (2010) comments that "*some commercial systems have no clear security and privacy specification at all and rely on security by obscurity by claiming security features without disclosing how they are achieved*".

In a recent analysis by Rahman p.449 of the IEE Computer Society, a large number of security design flaws were identified in common fitness trackers. The study outlined the following attack methods: "1. Inspect attacks: the adversary listens to the communications of trackers, bases and the web server" (Rahman, Carbunar et al. 2016, p.449) "2. Inject attacks: the adversary exploits solution vulnerabilities to modify and inject messages into the system, as well as to jam existing communications." (Rahman, Carbunar et al. 2016, p449) "3. Capture attacks: the adversary is able to acquire trackers or bases of victims".

Rahman's (2016, p.451) study looked in depth at the Fitbit Ultra and Gammon Forerunner 610 and found many vulnerabilities, for example "*during the initial login via*

Fitbit client software, user passwords are passed to the web server in cleartext and then stored in log files on the base".

Wearable devices that are compromised do not only put the end users' personal information and reputation at risk but their health as well (Canada 2014). For example, eavesdropping and impersonation of a wearable device charged with regulating insulin could result in dire consequences for the individual's health (Li, Raghunathan et al. 2011). Another reference to security issues in wearables by Soh (2015) states that "information describing a user's health status has to remain secure and not be allowed to disclosed to anyone but the system's wearer and supervising physicians, this is a challenge due to the large number of sensors and devices" Mulani (2016) has views on the seriousness of the security threats with IoT, he illustrates this by giving an example of a traffic control operator or a person with an implanted IoT medical device who cannot risk their IoT devices being hacked.

IoT security risks in the Smart Home

The Smart Home is another security vector to be looked at when it comes to the IoT. Smart home devices can record information about the number of people who live in a home, details about their daily habits as well as changes in their routines (Canada 2016). An interesting paper by Lin (2016), states there are many threats and vulnerabilities arising from IoT in a Smart Home, for example confidentiality breaches in home monitoring systems can lead to the release of private health data. Another example given by Lin (2016) is that unauthenticated system status alerts might confuse a house controller into thinking that there is an emergency and therefore to open doors and windows to allow emergency exit.

IoT security risks in Smart TVs

Smart TVs are popular IoT devices already used in many households, however they also pose a risk to users' security. Security vulnerabilities in TVs could put sensitive information stored on them at risk, such as financial account information and passwords, and they could be used for identity theft or fraud (Barcena, Wueest et al. 2014).

IoT security risks in self-driving cars

Self-driving cars are another aspect of IoT which will change how users drive their cars. Recently however it was reported in the media how a Tesla self-driving car crashed

and killed its passenger, which has led to a federal investigation of the technology (Thielman 2016). It is not the first time this has happened either, Google's self-driving car also crashed back in February this year (Lee 2016). These examples convey how new IoT technologies need to be vigorously tested before hitting the market to consumers.

2.5.6 IoT Security Recommendations

The following is an overview of the privacy and security requirements needed to improve the IoT ecosystem as recommended by experts.

Firstly the devices need to have more 'resilience to attacks': "*the system has to avoid single points of failure and should adjust on node failures*" (Weber 2010). Secondly they must provide 'data authentication': "*retrieved address and object information must be authenticated*". Thirdly, IoT devices must provide 'access control' "*providers must be able to implement access control on data provided"*. Finally, IoT devices should provide 'client privacy': "*only the information provider should is able to infer from observing the use of the lookup system related to a specific customer, inference should be very hard to conduct*" (Weber 2010).

According to Bandyopadhyay (2011), there are three key elements needed to prevent IoT attacks: "(a) securing the architecture of IoT– security to be ensured at design time and execution time (b) proactive identification and protection of IoT from arbitrary attacks (e.g. DoS and DDoS attacks) and abuse, and (c) proactive identification and protection of IoT from malicious software."

Zheng (2011) recommends that lightweight ciphers are created, a robust security service to handle key management similar to cloud systems, privacy preservation and anonymity, domain and event based security management and finally standardisation.

Also, IoT users need be made aware of the security risks and best practices when it comes to the IoT and IS. The main objective of security awareness is based on the argument that "*there are some central information security issues that every citizen using IT should be aware of. These issues are no less relevant than 'normal security issues'*" Siponen (2001). Furnell (2007) also conducted research in this area and found that 29% of all users are either not confident or worried about the security of their PC. With a better IS

security education, it is hoped that IoT users should be better able to understand the importance of information security and their own security responsibilities.

2.6 IoT Privacy, Governance and Legal Issues

2.6.1 Privacy in IoT

This section will discuss in-depth how the IoT poses a privacy risk to its users. Firstly, privacy can be defined in terms of control as "..*the claim of individuals to determine for themselves when, how and to what extent information about themselves is communicated to others*"(Westin 1968).

User privacy is very important in IoT and there is a challenge in protecting individuals' privacy. Privacy has been identified as one of IoT's "*most sensitive subjects*" due to the fact that its data can contain confidential information of a personal nature and therefore it is important to protect it (Roman, Najera et al. 2011). According to Article 8 in the Charter of Fundamental Rights of the European Union (2010) "*Everyone has the right to the protection of personal data*". Privacy is an important right because it is necessary for the condition of other rights, such as personal autonomy and freedom (Britz 2010). Privacy will be an essential factor for the IoT because it will help determine user acceptance and widespread use of the technology (Da Xu, He et al. 2014).

Privacy protection in the IoT environment is more difficult than the traditional ICT environments because the number of attack vectors on IoT entities are much greater (Da Xu, He et al. 2014) (Roman, Najera et al. 2011). The more objects that become traceable through IoT, the larger the threat to privacy (Whitmore, Agarwal et al. 2015). Mulani (2016) emphasises that the "*respect for privacy rights is integral to ensuring trust in the Internet*" he goes on to further explain that IoT devices challenge traditional expectations of privacy.

IoT devices collect large amounts of data on consumers and therefore carry privacy risks. IoT relies on the principle of processing large amounts of data through sensors, thus large volumes of data can be collected and stored. IoT device data are usually stored in the cloud, and the use of predictive analytics tools can potentially allow companies or malware to have detailed profiles on users (Desai 2016). As IoT devices are increasingly being used as personal health trackers and in the homes of consumers, private information is inevitably stored and collected (Hwang 2015). The FTC (2015) report describes how IoT devices enable *"unauthorised access and issue of personal information"* (Clapper 2016).

As a worst case scenario dystopia is possible, because there is a fear that "users would have access to an unprecedented number of personalized devices, all of which would generate considerable data, and the environment itself would be able to acquire information about its users automatically" (Roman, Najera et al. 2011). This is a big brother type view of the world and its surroundings. Context neutrality is another issue, individuals' right not to be linked with places, people, locations and preferences in daily life will be near impossible to hide because of sensor networks (Marias, Barros et al. 2012). Weber (2015) adds to this view by observing that individuals' data and behavioural patterns may become identifiable. This is due to the fact that as the devices are used in day-to-day life, a greater amount of private data is stored and collected.

Marias (2012) alludes to the fact that in an IoT network it is possible for "unsanctioned invasion of privacy by the government, corporations or individuals to get our personal information such as age, address, movement or even sexual preference". In fact, this year the US Intelligence Agency have even mentioned that IoT might be used in future "for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials" (Clapper 2016).

Consumers leave a large data foot print when using IoT devices. Bandyopadhyay (2011) identifies the following main causes for concern in relation to IoT privacy "*(a) control over personal information (data privacy) and control over individual's physical location and movement (location privacy), (b) need for privacy enhancement technologies and relevant protection laws, and (c) standards, methodologies and tools for identity management of users and objects.*"

IoT will affect its users' privacy in many different sectors such as appliances, vehicles and smart cities. In automobiles, drivers can share their driving behaviour with insurers to get lower rates (Power 2016). Patients' health data are now being stored by physicians, hospitals and insurance companies (Power 2016). In relation to health wearables they can be uniquely identified and traced back to their users (Soh, Vandenbosch et al. 2015). Laplante (2016) affirms that in relation to IoT and healthcare, the systems must allow for sharing private information while at the same time ensuring privacy, because patients expect private information to remain confidential as there are legal obligations to protect private information in healthcare systems.

If the privacy threats are not addressed there could be backlash from consumers. For example, CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) set up a campaign against Benetton who decided to put RFID tags on the clothing they were selling to their customers to track more analytics on them (CASPIAN). Boycotting IoT services and devices may become more prevalent in future, as the full information on how much is being tracked is passed on to the average consumer.

To deal with these privacy issues the development of a 'privacy broker' might be needed, this guarantees the provider only obtains the necessary information on the user (Lioudakis, Koutsoloukas et al. 2007). Also there is a need to create a digital forgetting system that deletes information periodically when it is no longer of use for the purpose it was collected (Atzori, Iera et al. 2010). Studies into digital forgetting are ongoing (Baetens 2010). It is clear that privacy remains a huge challenge to be addressed in the IoT.

2.6.2 IoT Governance

Another issue in IoT is the lack of governance around the technology. IS governance can be described as how IT decision-making rights and responsibilities are distributed among stakeholders, and it defines the procedures and mechanisms for making strategic IT decisions (Peterson 2004). There have been issues defining security, privacy, trust models and a governance framework for IoT (Weber 2010, Roman, Zhou et al. 2013). Xia (2012) further explains how *"IoT alludes to the organised interconnection regular items in practice which are frequently furnished with pervasive knowledge."* IoT will require innovative approaches to ensure its safe and ethical use (Roman, Najera et al. 2011). There is no control or standard on what IoT devices are coming into the market, so there are varying levels of security in these devices.

The accountability in IoT governance is considered very important (Weber 2010). According to Zheng (2011) the EU and the IoT industry stakeholders have tried to establish framework principles, and norms and scope for international IoT governance. He specifically mentions that "*the IoT Eco-system requires a secure platform that helps users understand the risks and control their privacy settings".*

Copie (2013) identifies the need for governance in IoT when it comes to storing, processing and aggregating information. He recommends a solution of combining cloud and IoT governance to tackle the scalability of the IoT as it grows and grows with more connected devices.

2.6.3 Legal Framework

There are many legal implications that need to be taken into account when it comes to IoT technology as its still in its infancy state. According to Weber (2011), legal frameworks should be established in order to have accountability in IoT and to protect the development of new services. Weber (2015) alludes to the fact that a single legal description for IoT cannot be easily developed, and that more specific data protection and privacy laws must be considered.

The basic legal questions that need to be answered are as follows: “Is there a need for (international or national) state law or are market regulations of the concerned business sufficient?”, “If legislation is envisaged: Would existing/traditional legislation be sufficient or is there a need for new laws?”, “If new laws are released: Which kind of laws are required and what is the time frame for their implementation?”(Weber 2010). These questions have not yet been answered and both the EU and the American government are still reviewing the legal aspects of the IoT. The next section provides an overview of the EU regulation efforts so far when it comes to the IoT.

2.6.4 EU IoT Regulation

In order to deal with IoT legal regulations in Europe, the Article Working Party on the Protection of Individuals with regard to processing their information (WP29) released a paper on legal recommendations for the IoT when it comes to a legal framework (WP29 2014).

The WP29 report (WP29 2014) sets out the following advice: Firstly, Privacy Impact Assessments (PIAs) should be performed before any new application is launched in the IoT, which are outlined under the assessment framework for RFID applications (industry). Secondly, WP29 recommends that personal information collected on IoT devices must be deleted when no longer necessary for the purpose it was collected.

Thirdly, IoT devices should have privacy by design which means the amount of collected data is limited to what is required to provide the service. Fourthly, the WP29 recommends 'self-determination of data', this means that users must exercise their rights to be "in control" of their data. Fifthly, non-IoT device owners should be protected through the creation of IoT systems that inform individuals of their data being captured. Finally, they recommend the use of 'user friendly consents' which means users should be offered the right to refuse IoT privacy policies, and such policies should be made user-friendly.

While this is a welcomed attempt by the EU to deal with the legal issues, it is not detailed sufficiently or adequately enough to deal with the complexity of the IoT (Ryan and Glynn 2014).

2.6.5 USA IoT Regulation

The US identifies rights to privacy through interpretation of the First, Third, Fourth, Fifth, and Ninth Amendments (Folk 2015) however nothing specifically aimed at IoT technology. Instead, the US has chosen to adopt a similar approach as the EU in relation to the legal aspects of IoT regulations and has created non-binding guidance for the IoT when it comes to data collection. In January 2015, the Federal Trade Commission (FTC) released a report on the IoT which sets out recommendations for IoT device manufacturers (FTC 2015).

The following is the list of recommendations set out by the FTC: Firstly, adopting IoT "security by design" - the devices should have built in IoT security. Secondly, IoT companies should do a privacy or security risk assessment on the collection and retention of consumer information. Thirdly, IoT companies should incorporate the use of 'smart defaults', this means getting users to change default passwords on their devices. Fourthly, companies should train staff on the importance of good security practices. Finally, companies should adopt a 'defence-in-depth' strategy for security risks, which means they should ensure there are multiple security layers. While the above report is a step in the right direction for managing the IoT it is not enough, and the recommendations stand no legal grounds.

2.6.6 IoT Self-Regulation

Rather than establishing a legal framework for the IoT, self-regulation is a strong possibility (Weber and Weber 2010, p.26). Self-regulation is "*law which is responsive to changes in the environment and which develops and establishes rules independent of the principle of territoriality*" (Johnson and Post 1996).

Weber (2010, p.23-24) believes that IoT is too important not to be regulated and also that '*state law*' is not appropriate for a global system due to its '*territorial limitations*'. There should be an '*independently managed de-centralised multiple-root system*' (Weber 2009).

The following advantages come with self-regulation (Weber 2010, p.24-25): Firstly, the rules created are more efficient because they respond to real needs. Secondly, it provides the opportunity to adapt the legal framework to changing technology. Thirdly, it can be implemented at a reduced cost. Finally, self regulation can induce the concerns of people to be open to a permanent consultation process when developing rules.

The ITU (International Telecommunication Union)(ITU 2016), the United Nations' agency specialised in the field of telecommunications, created Study Group 20 (SG20) that is looking into standardising the requirements for IoT (ITU-T). As mentioned previously, the term IoT first appeared in a technical report by the ITU (2005). The SG20 group aims to standardise the requirements of the IoT, with an initial focus on smart cities and communities (SC&C). The ITU-T released 21 technical reports on smart cities in May 2015 which can be accessed here: (ITU-T 2015).

Also, Atzori (2010) identified IoT standardisation as being sought by the European Commission and European Standard Organisations like the ETSI (European Telecommunication Standards), as well as by their international counterparts ISO (International Organisation for Standardization), and by other standard bodies (IETF, EPCglobal) etc. There is much more work needed in the field of standardising the IoT's products and services. The future outlook for the technology is that the legal framework will be established mainly through self regulation. It is unlikely that an intergovernmental regulation body will be founded in the near future (Weber and Weber 2010).

2.7 Summary

This section has covered a broad outline of IoT from the literature review conducted. The literature has provided the background to IoT and its development and how it is evolving. The literature has also shown what technologies have enabled IoT to come into being. The literature outlines the severe threats to privacy and security associated with IoT devices. Finally the literature has identified the need for a self regulation to create standards to govern this technology and its distribution.

Chapter 3: Methodology

3.1 Introduction

The following chapter answers the research question by outlining an overview of the different research methodologies and the broad research design, and then justifying the methods and techniques selected. This chapter also includes the conceptual framework that shapes the paper.

The chapter provides a detailed explanation of how the research was conducted and the manner in which the data were collected. In addition, there will be details of the main strengths and weaknesses associated with the chosen approach.

Research can be defined as "an activity that involves finding out in a more or less systematic way, things you did not know" (Walliman 2011). Methodology can be described as "the philosophical framework within which the research is conducted or the foundation upon which the research is based" (Brown 2006).

3.2 Purpose of the Research

This research aims to understand users' privacy and security concerns and or apprehensions when it comes to new technologies, in particular the IoT. The research examined users' perceptions of security and privacy issues of IoT smart devices. The purpose is to find if users are concerned about their private data being stored and shared on IoT devices. The intention of the research is to identify what IoT companies and manufacturers need to implement to assist in a more secure technology and also to help future research in the area.

The research will answer the following key questions. Does privacy or security matter to users, in particular that of their personal information? Does privacy or security matter to users when using devices that connect to the internet (IoT devices etc.)? How much control do users believe they have over the personal information stored on their devices?

The goal in this research is to understand the perspectives and behaviour of people and the context in which they act, hence a social science approach to the research was deemed appropriate. This social research approach means that the process followed was to develop a research question or statement and then gather data on that phenomenon in other to draw upon conclusive answers (Quinlan, Babin et al. 2011). The social science concept was originally developed by August Compte in the 1800s and then developed in the 1900s by the sociologists Emile Durkheim, Max Weber and Karl Marx (Quinlan, Babin et al. 2011). Information systems have been interpreted in the form of social studies many times in the past (Walsham 1993)

3.3 Research Philosophies

3.3.1 Empirical and Theoretical Research

Empirical and theoretical research are the two main categories of academic research (Remenyi and Williams 1995). Theoretical research involves finding a result predicted by a theory, while empirical research focuses on data gathering and analysis. This research paper will apply an empirical research method.

3.3.2 The Research 'Onion'

A popular cited work by (Saunders 2011) introduced the 'research onion' as a representation of research philosophy. This divides the research process into a number of different subsections which helps to decide a valid research methodology. There are six distinctive layers in the research onion as follows: philosophies, approaches, strategies, choices, time horizons and procedures. The onion is a way of depicting the choices for your data collection methods and aid in creating a research design (Saunders 2011). This paper will follow this research structure and each of Saunders' (2011) layers will be explained in depth.

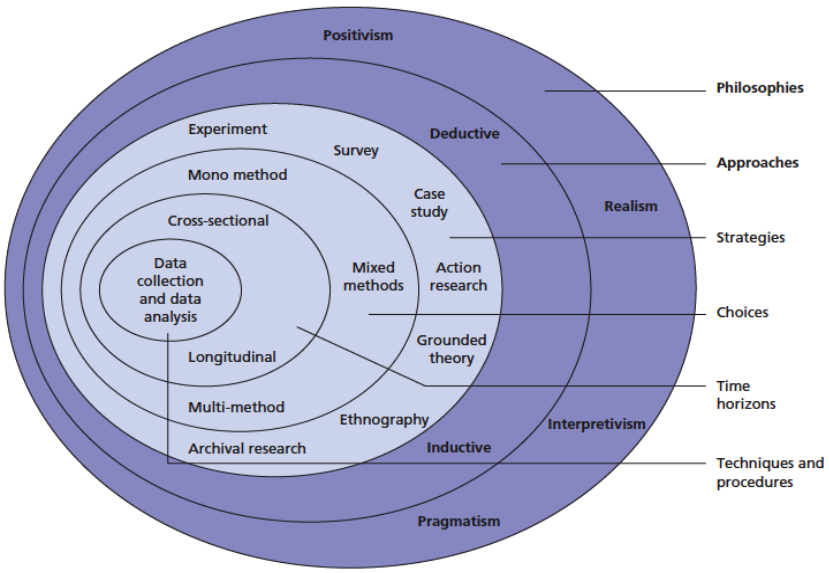

Figure6: The research onion Source: (Saunders 2011)

3.3.3 Philosophy

The research philosophy forms the foundation to any research question. It is an explanation of a belief or an idea on the collection, interpretation, and analysis of data collected (Levin 1988). Saunders (2011), further explains that the researcher will maintain a specific study to reflect important assumptions about his opinions and views on the world. Klenke (2008) enforces the idea that it is important to choose the correct philosophy, as a researcher's psychological assumptions are critical in framing the research process.

There are many different research philosophies, the following section gives an overview of the most common philosophies used when conducting research that were considered during the research phase of this study.

3.3.4 Ontology

Ontology is an important part of a researcher's approach because it describes his beliefs about reality. Different kinds of research are founded on different beliefs, based on what the researcher believes is the truth. Klenke (2008) emphasises that it is important to address the question "What is the nature of reality?" because a philosophic question about reality affects the way we do our research. Two main ontologies were considered for this research.

Objectivism

Objectivisim is the position that implies social phenomena confront us as external facts that are beyond our reach or influence (Bryman 2012, p.32). It portrays that social entities exist in reality, and are external to social actors concerned with their existence (Saunders, Lewis et al. 2009). This is the more common scientific conception of reality, which means that we as learners assimilate, "*learners are told about the world and are expected to replicate its content and structure*" (Jonassen 1991). This is a view that things - computers, organisations etc - have a nature, an essence separate from human beings.

Constructivism

The other ontological view is called constructivism (also known as subjectivism/constructionism). This is a belief that while things like computers physically exist, their nature, their essence is determined by the perceptions people have of them, and the ways in which people use them. Constructivism is the belief that "*social*

phenomena are formed by perceptions and actions of social actors concerned with their existence" (Bryman 2003). The mind is instrumental in interpreting events, objects, and perspectives on the real world, and those interpretations comprise a knowledge base that is individualistic (Jonassen 1991). It distinguishes that social phenomena are formed by perceptions and actions of social actors concerned with their existence.

This research paper will follow this constructivist view, as the research is not concerned with numbers and statistics but with social situations and the manner in which individuals view them (Quinlan, Babin et al. 2011)

3.3.5 Epistemology

Epistemology addresses the second paradigmatic question "How do we know what we know?" Saunders (2011) explains that "*Epistemology concerns what constitutes acceptable knowledge in a field of study*". It also deals with the researcher's belief system about the nature of knowledge such as certainty, structure and sources of knowledge.

It refers to ways of knowing and how to understand the reality through three main philosophical paradigms. These paradigms, positivism, interpretivism, and realism, are outlined below.

Positivism

This is the collection of data allowing the testing of hypotheses which are generated by quantifiable means and gathering of facts (Saunders 2011). Positivists see the world as having one reality which we are all part of (Quinlan, Babin et al. 2011). Researchers generally have the philosophical stance of "*natural scientists*" (Saunders 2011). Remenyi (1998) helps to explain positivism as a way of "working with an observative social reality and the end product can be law-like generalisations similar to those produced by the physical/natural scientists". The researcher is concerned with observable facts gathered from social reality.

Realsim

This is a philosophy of scientific enquiry. It adopts a scientific approach similar to 'positivism'. "What the senses show us as reality is the truth: that objects have an existence independent of the human mind. The philosophy of realism is that there is a reality quite independent of the mind" (Saunders 2011).

There are two types of realism, critical realism and direct realism. (Saunders 2011) states that direct realism is "*what you see is what you get: what we experience through our senses portrays the world accurately*", and that critical realism is "*what we experience are sensations, the images of the things in the real world, not the things directly. Critical realists point out how often our senses deceive us*".

(Saunders 2011) also emphasises the following important point: "The direct realist perspective would suggest the world is relatively unchanging: that it operates, in the business context, at one level (the individual, the group or the organisation). The critical realist, on the other hand, would recognise the importance of multi-level study (e.g. at the level of the individual, the group and the organisation). Each of these levels has the capacity to change the researcher's understanding of that which is being studied."

Interpretivism

Interpretivism takes the opposite approach to that of positivism, it argues that human behaviour cannot be quantified and measured the same way as physical sciences. Interpretists take the view that the subject matter of social sciences (people and institutions) are fundamentally different from the natural sciences (Bryman 2012, p.28). Saunders (2011) defines it as having a "focus set to social actors where the researcher takes a more empathetic stance entering the social world of the research subject and understanding it from that point of view". Walsham (2006) also complements this perspective and states that our knowledge of reality is a social construction by human actors.

Pragmatism

The pragmatic philosophy is the view that there maybe more than one way to answer a research question and that the most important determinant is the research question itself(Saunders 2011). Pragmatists often use a mix methods approach (both qualitative and quantatative approach)(Morgan 2007).

3.4 Research Approach

3.4.1 Quantitative (Deductive) vs Qualitative (Inductive)

The Research Approach is the second layer of Saunders et al. research onion. There are two main types of research approaches used in IS research, the inductive and deductive approach (Blaikie 2009). A qualitative, or inductive approach was utilised in this research paper. The following section outlines the differences between qualitative and quantitative approaches.

Quantitative research is a deductive approach that considers collecting measurable, quantifiable data through structured questionnaires or surveys to support or develop an existing theory (Wilson 2014). Quantitative data produce characteristics and other variables in numerical form which are analysed through the use of statistics and illustrated in diagrams, charts or graphs to identify trends (Hair, Celsi et al. 2011). In a 'deductive approach', a theory is tested through a series of propositions with the final goal of deducing conclusions. It involves the development of a theory that is subjected to a rigorous test. According to Saunders (2011) it is characterized by "*searching to explain causal relationships between variables as well as by enabling facts to be measured in a quantitative way*".

In contrast, qualitative research is an inductive approach that concerns understanding and interpreting reasons, opinions and underlying motives, to create new ideas and develop a new theory (Hair, Celsi et al. 2011). Qualitative data are developed from interviews, focus groups, observations and case studies, and analysed as narrative text rather than numerical values (Wilson 2014).

Moreover, qualitative research aims to get the reality of the situation to understand the nature of the problem better. It is a theory based on observations of a problem. *"The approach concentrates on using literature to identify theories and ideas that the researcher will test using data*" (Al Zefeiti and Mohamad 2015). As described by Gray (2013) this approach firstly makes a plan for data collection, then this information is analysed to see if any patterns emerge that suggest relationships between variables. Through observations it is possible to construct some generalisations, relationships and possibly theories. Qualitative approaches are used when the researcher wishes to study issues that are not

easily partitioned into discrete entities, or to examine the dynamics of a process (Kaplan and Maxwell 2005).

3.4.2 Rationale for Research Approach

The literary review highlighted that IoT technology is a relatively new technology and is growing at a substantial rate. A challenge to the successfulness of this technology is the security and privacy issues surrounding it. There is a clear lack of research done on the opinions and thoughts of end users and consumers.

This research paper was designed to identify users' opinions on security and privacy when it comes to IoT devices. A range of research approaches were considered, however, the literary review clarified a clear lack of qualitative research when it comes to IoT systems, in particular in the field of security. A plethora of surveys have been conducted in relation to IoT and security (Zhao and Ge 2013, Barcena 2015, HP 2015, Whitmore, Agarwal et al. 2015, (OWASP) 2016) however, there are not many qualitative data available in this field.

The research follows an interpretivist belief that reality and the individual who observes it cannot be separated (Weber 2004). So, one individual's views on IoT security and privacy perceptions could be completely different to another individual's views.

There is a strength and power in the interpretivist approach that lies in the ability to address the meaning and complexities of situations (Black 2006). There is no straight forward quantifiable way to address why certain people have particular privacy and security feelings towards technologies, instead these need to be investigated in a qualitative way.

As explained by Kaplan (2005), qualitative studies aim to understand how people feel about something and why they think that way, what their perspectives are, and what a technology means to people. The IoT concept is quiet new to people, so their judgements and feelings towards it need to be recorded and analysed which this study aims at doing.

It is hard to measure a feeling or a perception in a statistical manner. As the research question is looking for meaning to users' feelings, a qualitative interpretivist research approach was deemed to be the appropriate method.

3.5 Research Strategy

3.5.1 Strategy Overview

Research strategy is the third layer of Saunders' research onion. In order to choose the correct strategy, an extensive view of well recognised works were reviewed on research methods. Saunders (2011) listed the following that were considered: survey, case study, action research, experiment, grounded theory, ethnography and archival research. The bottom half of the figure below was followed as the research methodological choices.

As the research follows a constructivist, interpretivist, inductivist and qualitative approach, semi-structured interviews were chosen as the appropriate research strategy.

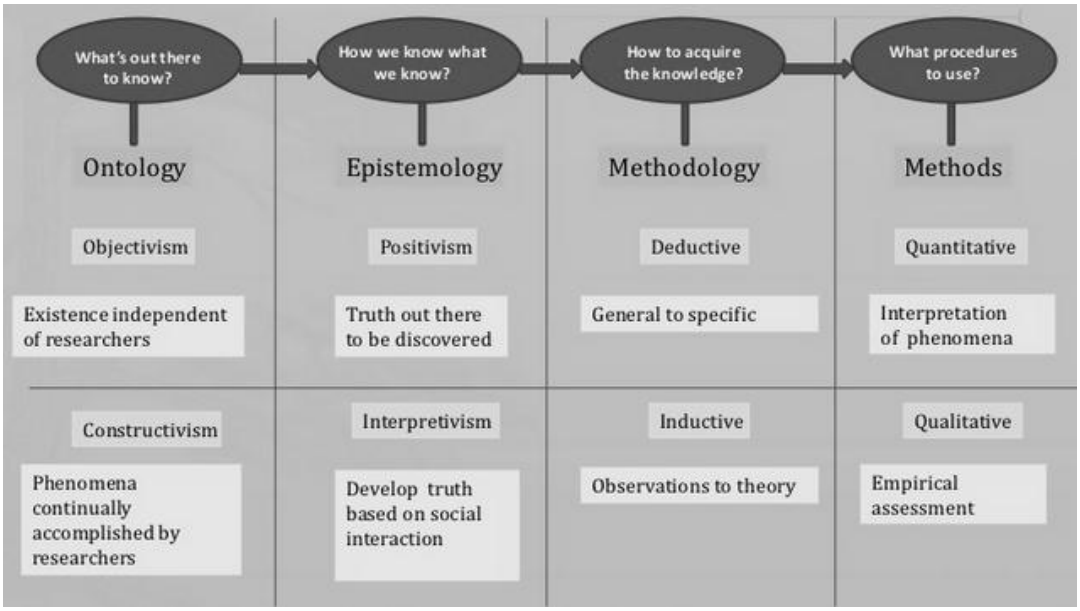

Figure 7: Chosen Methodology Source: (Yeong 2011)

3.5.2 Semi-structured Interviews

This research paper adopts a qualitative approach by using semi-structured interviews to collect primary data. A semi-structured interview is defined by a pre-set question guide that aims to provide in-depth findings through informal discussions with participants (Collis and Hussey, 2003).

Semi-structured interviews allowed the researcher to probe participants to elicit additional information and tacit knowledge which provided insight into the privacy and security concerns for users, if any. An inductive research approach was selected as the research method because of the qualitative method of data collection. It is appropriate to use interviews as the research method because the aim is to gain an understanding of the participants' experiences and interpretations on a specific topic. Easterby-Smith (2012) describes how semi-structured interviews provide flexibility to elaborate on any subject that the researcher feels is pertinent during the interview. The interprevist philosophic approach is a useful way of measuring the responses to the interviews. "*Simply observing and interviewing do not ensure that the research is qualitative, the researcher must also interpret the beliefs and behaviour of participants"* (Janesick 2000).

The reasons for conducting this research strategy were as follows: Firstly, there was less of a chance for potentially ambiguous questions. Additional questions may be required to explore your research question and objectives given the nature of events within particular organisations (Saunders 2011, p.320). Secondly, the researcher may omit some questions in particular interviews, given a specific organisational context that is encountered in relation to the research topic (Saunders 2011, p.230). Finally, the order of questions may also be varied depending on the flow of the conversation (Saunders 2011, p.230).

In-depth understanding is much more difficult to attain through structured questionnaires, which are objective and result in quantifiable data. A more detailed understanding can be found through language and observations (Saunders, Lewis et al. 2009). Qualitative methods are less structured, which allows the author flexibility to take the "interpret" approach to primary data collection (Saunders, Lewis et al. 2009).

3.5.3 Advantages of Research Approach

There are several advantages and disadvantages to semi-structured interviewing. There is a big advantage in utilising probing as a method to keep interviewees on topic *"this approach provides more depth than a classic survey interview"* (Brannen 1992). The participants can give much greater insight into their personal experiences on a subject rather than simple 'yes' and 'no' answers.

Interviews provide the researcher with the opportunity to resolve seemingly conflicting information because the researcher has the chance to ask directly about apparent conflicts (Harrell and Bradley 2009). In the case of IoT research there is a conflict between the growing popularity of IoT devices and the rising security vulnerabilities.With semi-structured interviews, questions can be asked out of order because of the natural flow of conversation (Harrell and Bradley 2009). This way, the interviewees can finish their line of thought on the subject without being confined to answering a particular question then and there.

When the respondent is answering questions the interviewer can practice ‘active listening’, which means listening carefully to the respondent’s answers and evaluating them. The interviewer can then try to interpret what is being said and seek clarity by using follow up questions (Guion, Diehl et al. 2001).

Finally the interview is generative, which means new knowledge or thoughts are likely (Legard, Keegan et al. 2003). There is a chance at some stage or during the course of the interviews that the participant will be directed down avenues of thought that he has not explored before.

3.5.4 Disadvantages of Research Approach

Semi structured interviews have a number of disadvantages (Bryman 1992). The interviewer must come up with questions as a result of the responses produced by the interviewee (Opdenakker 2006). This can be explained as the interviewer needing “double attention" which means the interviewer must be actively listening to what the participant is saying while also taking notes and making observations.

There is a fixed length of time so it can be difficult to make sure all your questions get answered with the correct amount of detail needed while at the same time trying to understand what the respondent is saying without trying to rush them (Wengraf 2001).

The interviews must flow around different modes of questions and answers while limiting the amount of time on discussing personal contexts (Ritchie, Lewis et al. 2013).

There is limited probing so the more detailed material are likely to come from the more confident and articulate people. The in-depth data of qualitative research is hard to achieve (Ritchie, Lewis et al. 2013)

3.6 Time Horizon, Population and Sampling

3.6.1 Time Horizon

Time horizon is an inner layer of the 'research onion' by Saunders. There are two types of time horizons - longitudinal and cross-sectional. For a longitudinal study the researcher observes the phenomenon for a period of time, in cross-sectional studies the time is limited (Saunders 2011).

A cross-sectional time horizon was selected due to the time constraints to conduct this research. Each interview was approximately 45 minutes in length and each informant was interviewed once and then contacted later if any further questions arose.

3.6.2 Population and Sampling

The research population is the total number of individuals or objects that are the main focus of the study (Arcury and Quandt 1998). This study involved interviewing nine participants.

Sampling in quantitative studies typically are large groups of people and are collected at random, to confidently generalise the sample to the population it represents (Patton 2005).

For qualitative methods, sampling focuses on relatively small groups to permit inquiry into and to understand the phenomenon in detail (Patton 2005).

For this research the sample audience was identified beforehand following the qualitative methodology. The target subjects for this study were users of IoT devices. Subjects were identified by the researcher beforehand and some additional interviewees were identified through the use of snowballing techniques.

3.7 Ethical Considerations

The ethical considerations are considered at each stage of this research. Ethical considerations are important because they establish protection and safety for the study participants. The application for ethical approval was submitted to TCD School of Computer Science and Statistics on 28th April 2016.

Every participant was given a brief outline of the purpose of the study and what it involved. Once the researcher received confirmation that the participant would like to take part in the study, the participants were each presented with the participant information sheet and the informed consent form which were signed before commencement of the interviews.

3.8 Methodology Limitations

Qualitative research approaches in general suffer from the following weaknesses: firstly, the context, events, conditions and interactions cannot be replicated. Secondly, the time required for data collection, analysis and interpretation is lengthy. Thirdly, the researcher's presence may have an effect on the subjects of the study. Finally, confidentiality and anonymity present issues when selecting the findings (Hughes 2014). According to Saunders (2011)semi-structured interviews specifically suffer from quality of data collection issues such as reliability, bias and validity. The limitations of the chosen methodology are as follows,

Sample size - The research utilised a semi-structured interview approach. This approach is more time consuming in nature than other research techniques such as questionnaires. Therefore it was taken into account that the sample size would be smaller, however it is hoped that the information is more in-depth and relevant. A larger sample size of participants may have been beneficial for data analysis as it would be more representative of the average consumer.

Interviewer Bias- Interviews are potentially subject to bias, and this was kept in mind when creating an outline of the interview questions and topics to be discussed.

Sample population - The majority of interviewees were known to the interviewer prior to conducting this research; maybe a more random sample would yield a better generalisability of the research findings. However, random sampling was not possible in this circumstance given the financial and time constraints.

Confidentiality and trust issues - The participant might feel uneasy about disclosing certain private information which may impair the interview process and the determined outcomes. The risk of this happening was mitigated by keeping participants' responses anonymous and allowing participants to skip any questions they did not feel comfortable in answering.

Data validity - To reduce the risk of data errors the interviews were audio recorded and also notes were taken during each interview. The audio recordings were then later transcribed in order to reduce the risk of inaccuracies.

3.9 Lessons Learnt

Throughout the research process a number of barriers were faced and overcome.

A mock interview was created initially in order to judge the responses to the proposed questions and to see if ambiguities had arisen. This was useful because any bias in the initial draft of some of the questions could be removed, also probe questions were thought of that were also noted. From the themes raised in the mock interview additional questions were added for future interviews.

Some of the interviews could not be conducted face-to-face as the participant was quite busy and unavailable to meet up. This meant that phone calls were used for three of the interviews. The disadvantage of this was that the facial expressions were lost so it was harder to interpret the data. Also, as one of the interviewees was using public transport at the time of the interview, that interviewee's answers were much shorter and more concise than those of the other respondents.

Significant time was lost in waiting for Ethical Approvals for the study before interviews could be conducted, it took around three months from the initial submission to the actual approvals, which put an enormous pressure on the researcher to conduct the interviews as quickly as possible and begin to analyse the results.

As interviews can be quite time consuming, it was difficult to ascertain a large number of participants'. The follow up analysis is also time consuming, as it involves transcribing the interviews and then searching for themes and meanings. If more time had been available, it would have been possible to collect more thoughts and opinions from IoT users.

3.10 Summary

In conclusion, the chapter has outlined the various academic research methodologies. This research paper will follow a constructivist ontology; interpretive epistemology and inductive methodology will also be used.

Chapter 4: Findings and Analysis

4.1 Introduction

This chapter presents the analysis and findings of the data collected during the research. The data were collected through semi-structured interviews. The guideline for the conversations to follow consisted of 24 questions, however the interviews were allowed to flow beyond the pre-defined questions to obtain further insights and relevant information. In this chapter the results of the interviews will be analysed around the following key questions:

- How does privacy or security matter to end users and their personal information?

- Does privacy or security matter to users, when using (IoT) devices that connect to the internet?

- What steps have users taken to protect their personal information while using IoT devices?

The analysis of interviews began by reading through the interview transcripts and reducing the data. Next, a themed analysis was made in which the major patterns were extracted and subjects or themes arising from the interviews were noted. Finally, any patterns that emerged were compared to current IS theories. The aim was to gain a conceptualisation of underlying security and privacy patterns.

4.2 Themes and Observations

4.2.1 Themes

From analysing the interview recordings, common trends and observations began to emerge. Some themes related across to all participants. The themes were developed based on common comments or points that came up during conversations with the participants. Detailed data collection was conducted through the semi-structured interviews. Nine interviews were conducted, each between forty five minutes and an hour in length. The three main themes were personal security and data privacy, attitudes towards IoT technologies, and data collection, analysis and protection.

4.2.2 Observations

The researcher interviewed nine participants in total. The participants' information will remain anonymous. As some of the questions related to their security behaviour it would not be safe to disclose their identities, instead they will be referred to as Participant followed by a letter of either 'A,B,C,D,E,F,G,H or I'.

While the participants will remain anonymous, this section will give a brief overview of their background. The participants' ages ranged between early twenties to mid-forties. A large proportion works in the IT sector or has an interest in technologies. Participant A - is a systems administrator for a large law firm, Participant B is an experienced IT professional in a large company, Participant C is a software engineer, Participant D is a tech enthusiast but works in the retail sector, Participant E is a project manager, Participant F is a server support engineer, Participant G is a computer science student and finally Participant H is a reformed hacker who now works as a systems administrator, Participant I is a systems administrator.

The initial impression after each interview was that each participant had concerns with IoT and its security and privacy, however it was not enough to stop them from adopting this technology. Each participant had his own unique ways of protecting his data to his own level of security satisfaction. The concerns for personal information security were felt across the board with each participant. These observations are described in more

detail in later sections of this paper. The following diagram is an overview of each participant's job description and also the age group of the participant.

Participant ID	Job Description	Age Group
A	System Admin	30-40 years old
B	System Admin	30-40 years old
C	Programmer	30-40 years old
D	Retail Employee	20-30 years old
E	Project Manager	40-50 years old
F	System Admin	30-40 years old
G	Student	20-30 years old
H	System Admin	30-40 years old
I	System Admin	40-50 years old

Figure 8: Participants' Overview

4.3 Usage and Attitudes towards IoT Theme

4.3.1 IoT Knowledge

The participants were first asked to describe IoT and what it means. This was to establish competency to see if the interview was relevant to them. All participants were IoT devices users, some even had multiple IoT devices and they were all familiar with this emerging technology. They each gave detailed definitions and examples of IoT technologies and how the devices can be used. Surprisingly, all participants had heard of the technology. Also, each participant defined IoT in a logical detailed way. Participant A said that IoT is "*a way of connecting various devices through the web*" He gave examples of smart fridges, smart watches and smart TVs. Participant E said he had read many media articles about IoT and that "*anything and everything*" will have an IP address and be connected online.

4.3.2 IoT Usage

All participants used IoT devices and smart devices, this was a requirement to participate in the research. Some of the participants used devices like their smart watch to track their heart rate, sleeping patterns and general health data. However, participants F, H and I were completely against the idea of using tracking with this technology. This conflict will be described in a later section.

A breakdown of the participants' devices can be seen in the table titled Figure 9 on the next page, the majority of participants had several IoT devices.

ID	Devices	Device Description
A	1. Smartwatch 2. GPS Tracker	1. Polar m400 2. Garmin 520
B	1. Health tracker 2. Smart TV device	1. FitBit 2. Google Chromecast
C	1. Smart TV device 2. Security System	1. Baidu Android TV box 2. Xaomi central security
D	1. Smart TV	1. Samsung 3D Smart TV
E	1. Smartwatch 2. Smart TV device 3. Smart Security System 4. Health tracker	1. Apple smartwatch 2. Google Chromecast 3. ICam Alarm 4. Polar m400
F	1. Smart TV device 2. Smart Wifi Radio	1. Chinese Android Media Player 2. Wifi Radio
G	1. Smartwatch 2. Google cardboard 3. Smart TV device	1. Bluetooth Chinese non branded smartwatch 2. Virtual reality smart device adapter 3. Non branded Android Media Player
H	1. Smart TV 2. Smart TV device	1. Nvidia Sheild TV 2. Google Chromecast
I	1. Smart TV	1. Samsung smart TV

Figure 9: IoT Usage

4.3.3 Future IoT purchases

The participants were asked about what devices they would like to own or purchase in the future. This question was asked in order to better understand the demand for IoT and what sort of market is out there for new products in this field.

All participants were planning on buying IoT products in the near future. Participant A was open to buying more IoT products, he would be happy to purchase an IoT heating system, he also mentioned a washing machine "*if you have a load in the morning that you forgot to turn off you could set it as well*".

The question on future IoT purchases was followed up asking if the participants felt there was any device that should never be connected online, as Khan (2012) explained in his paper that advancement in technology, especially IoT, will lead to a society of everything and everyone connected all the time.

Participant A felt that house security systems connecting online were a huge danger which he felt "wary" about. He said he would only use open sourced software "I would use open sourced software that I know is safe. So that I have full control over and not allow a third party to spy on my house." Participant B was much more open to the idea, stating "I think all devices will be connected to the internet. You will eventually be IoT enabled yourself! Your passport, even how you pay for things, everything will be IoT". He had no apprehensions about converting his house alarm to an IoT enabled system.

4.4 Personal Security and Privacy Theme

In this research analysis section, the key personal security themes found will be explained in more detail. Personal security is an important subject and theme that emerged when conducting the interviews. Participants were asked a series of questions around their security habits and behaviour.

4.4.1 General Security and Privacy Opinions

The participants were asked if security and privacy mattered to them in relation to their personal information. The participants generally all felt that they would like to keep their personal data private, and a key point was that they felt their personal information was a valuable asset.

Respondent D stated that “Of course, I try to be as secure as possible with my personal information. With my passwords and accounts I have even set up 2-step verification on most things. Occasionally I have set up VPNs (Virtual Private Networks) just to secure myself”.

Respondent E simply stated that “*of course, it absolutely matters to me*”. This feeling of importance around the users’ information was echoed in all of the participants’ responses. Respondent F gave a more detailed reasoning “*personal information can be used to get at your financial information easily, through phishing etc*”.

Finally, Respondent H said that “Yes, for various reasons. I know what can be done with that information. It can completely destroy your life, a tiny bit of personal information can do massive damage if hackers get their hands on it or enemies that are also tech savvy.”

4.4.2 Online Security and Privacy

Each participant was asked if privacy and security mattered to them when connecting online. All participants felt that when connected online or using smart devices their personal security is important to them. Especially when connecting online they felt that there were dangers out there, such as hackers, and that precautions were needed to keep their data as safe as possible.

Respondent A described himself as very cautious when online. He gave the example that while on Facebook he likes to go through the settings, and set them to his own preference level. "*I like the way how on certain things, like android devices, now when you're downloading apps you can attach certain permissions to things instead of a blanket yes which was the way before. You're beginning to have more power in saying e.g. no I don't want this app to have access to my camera. The more options you get the better. When it is a blanket lockout, either agree to these terms or don't use the product, otherwise you end up just agreeing to the terms even though you're not totally satisfied with it."*

Respondent C minimised what data he put online, he said "I avoid putting detailed information online. My LinkedIn isn't updated. I rarely use social media. I only use it for news information."

Respondent G felt that yes online security and privacy is important to him, his smart watch connects to his phone via Bluetooth which then connects to the internet. He said that "*it is easy for people to get your information, .. It is a concern of mine*".

4.4.3 Identity and Access Management

In order to gain an understanding about how the devices are treated on a daily basis, participants were asked if their devices were ever left unattended, and to describe a typical day of their smart device usage. There were mixed answers to this topic, some participants such as F leave their smart TV on all the time, while Participant H turns everything off when not in use. Participant F stated that "when I leave my house I don't want my devices getting hacked because there is a greater risk for devices that are always connected".

4.4.4 Device Encryption

All participants were asked about their level of security behaviour, more specifically if they ever encrypt their IoT devices. Participant E said he encrypts everything he can, even his smartwatch. He stated that Apple devices are encrypted by default in fact. Participant G also follows the best practice of encrypting every device he can, pointing out that "*I don't want anyone else to access them (IoT device), I want to keep them safe*". Participant H also valued encryption, he described how all his devices are encrypted

including his tablet, he felt that "..*it would be better if all smart devices came with the option to encrypt*". Participant A was concerned for his Garmin , stating encryption was not possible, he gave the example that if he lost the device and someone picked it up "..*they will have all my data, unfortunately there are no lockdown features*".

4.4.5 Password Management

One of the more personal questions of the interview related to password management of IoT devices and the interviewees' behaviour in this respect.

Increasing password length and complexity should aid an increase in security levels and is generally considered good practice (Allan 2004). Users should consider using stronger authentication methods, rather than increasing the length and complexity of passwords for more sensitive and vulnerable data. It was not appropriate to ask the participants what their actual passwords were but it was possible to get a description of how complex each participant's passwords were and if they followed guidelines regarding having separate usernames and passwords for different devices and accounts. Common guidelines for strong passwords are,

- Minimum of eight characters on the password length
- Lowercase and uppercase characters
- Numbers and symbols
- Avoid using dictionary words, names, dates and letter\number sequences
- Different passwords for different devices and accounts

The participants' answers were quite varied, and each had their own idea of what was a safe password management practice to follow. The majority of interviewees felt they followed a "secure" password management system. Participant E uses what he called 'best practice' password complexity management for all devices and systems. He uses a different password for all his devices, he tends not to use the password manager applications because they are what he described as a "single point of failure". All of his passwords are a minimum of ten characters in length.

Participant C on the other stated that "I have too many passwords so I don't have different passwords for everything. I'd say I have five to six passwords that I use for everything". He felt that his devices could be open to "brute force attacks".

4.5.6 Privacy Policies

As a foundation question the interviewees were asked if their IoT devices displayed any privacy policy that must be agreed to when they were first powered on. They were also asked about their opinions on terms and conditions in general when it came to technology devices and utilisation. Most participants revealed they never read the terms and conditions before they started using IoT devices or a website in general. There was a feeling of it being too time consuming and pointless.

4.5 Data Collection, Analysis and Protection Theme

4.5.1 Information Stored on IoT Devices

The participants were asked if they thought that personal information about them might be stored on their smart devices. This was to get an end user perspective on what data might be saved on these machines and how aware they are of the technology and its uses. Everyone felt that their personal information was getting tracked and logged on some, if not all, of their devices.

Participant B felt that his FitBit is tracking the heart rates of its users, tracking how they sleep and measuring how active they are, this was stated in the terms and conditions of the device.

Both respondents F and H felt so concerned about their personal information getting online that they went to the extremes of setting up fake email accounts to use in the event of needing to login to sites or apps that require personal data.

4.5.2 Health Data vs Location Data

An intriguing argument came about in the interviews on the topic of “do they have different concerns for different types of personal data”. They were each asked which data are more valuable to them to keep private, health or location data. The responses were split down the middle; half of the participants felt location data were really important because they reveals things like your home address and daily routines, while the other half of the interviewees felt that health data were more important because they can be used by hackers to gain a full profile on you. “Hackers could use the health data to impersonate you”, according to Participant H.

4.5.3 M2M Communications

IoT is broad and M2M communications can be described as a sub-section, but it is also an independent concept. M2M stands for Machine to Machine, it is when the ‘smart’ machine(s) use network resources to communicate with the infrastructure for a wide variety of purposes such as monitoring and control. Often this interaction is independent of

the end user. The fact that machines can now handle tasks automatically based on environmental factors is one of the biggest advantages of IoT and has led to it becoming very popular in industries such as manufacturing. However, it is also a security risk: if the machines are compromised they will pass on operations without the end user's knowledge. I asked the participants how they felt about the concept of their IoT devices communicating independently and carrying out automated tasks, the responses were varied widely.

Participant H was completely against the idea, detailing as follows: "Yes, I am aware and I don't like that. Because if one is breached, then the others will be breached because it can automatically jump from that device to the other device." Participant F felt a similar way, stating that "There's definitely danger to that sort of thing. The simplest example is if your status is being posted online that says you're out of the house you're more likely to get burgled if someone sees that for instance. There are always dangers to personal information about you being published and if that information is published automatically without your knowledge then that's very worrying."

Interestingly, participant B felt that it was frustrating " …that would be deeply communicating with a device that I don't want it communicating with and that would annoy me. I think it's sneaky, if I didn't have control over the device I just wouldn't buy it." He went on further to acknowledge that is may be an inevitability in future IoT products "I normally do a lot of research into a device before I buy it, but maybe in the future it will be unavoidable".

In contrast, Participant E who is an avid IoT user said "Things have occurred over the last number of years that have made me more comfortable with that. For example I'm embedded in the Apple eco system. I have an Apple phone, tablet, laptop and watch. The beauty of that is I'll go about my day taking photographs of my kids. With my phone and it uploads by itself. Days of me having to bring that phone to the computer and having to click upload and then put them into an app for managing them, those days are long gone. It just happens and I assume now that when I open my laptop the photos are there for me to sort or edit the way I want. You make a tradeoff for privacy and convenience." He is more focused on the benefits the technology provides rather than any associated security risks.

I then asked participants a follow on question to see would they disable these features if they had a choice. Participant F said - "*Yes I would disable those settings if I didn't think there was any benefit. But sometimes I would be too lazy and not have the time*."

While Participant H would disable them, he did suggest a solution for giving the choice back to the end user "I should always get a notification 'do you want to connect?'. I need the choice to say yes or no, I come in the range of my other device and it will just connect. I would rather have the device ask me yes or no, it needs to give the option to the user."

4.5.4 Security Updates

An important part of any technology is mitigating the threats, this is helped by security updates on devices. Each participant was asked about the value of security updates, if they feel they are necessary or if they add unnecessary bloatware to their devices and provide IoT manufacturers more rights to data then needed. Again the perceptions were very diverse.

Participant D felt the need to install them whenever they became available, however he was concerned about what permissions and changes the supposed security updates make "*…I like to check what the update actually includes before I do though, because a lot of times they change back settings. For example Windows 10 sets your device to Microsoft's preferred settings rather than your own*."

Participant A had a mixed opinion towards them saying that "Usually I update my devices. If I hear of a security patch I usually update but not straight away, these things need to settle down. I don't want to break a device because I have put in the latest update. I wait a week or two. Usually they make things more secure but they tend to break things at the same time." He echoed the general opinion of most of the interviewees in saying that "*I think the way they sell the updates is for the new features. The way its bundled together is quiet smart to get people to do security and software updates*".

4.5.5 Companies Data Usage

A key theme which arose several times during the interviews was to what degree the participants trust private companies to keep their data secure? And do the participants feel companies are recording their personal information? There was a definitive hint in the interviewees' answers that Big Data is used by companies to record their users. Big Data refers to "enormous amounts of unstructured data produced by high-performance applications falling in a wide and heterogeneous family of applications" (Cuzzocrea, Song et al. 2011). Companies are interpreting these vast amounts of data in order to better understand their customers. However, the feeling of being tracked was not welcomed, it was expressed earlier also during the questions of what data are stored on your IoT devices. Participant B felt that "*companies are collecting a lot more data then I would like them to*".

There was a mystery among the participants as to where exactly their personal information is stored. Some believed their data were stored in the cloud, some believed in server farms, and others that their data were only stored locally on their IoT devices. No participant was able to confidently describe where his personal information was stored or how companies are using it. Participant C asserted full trust in companies stating "*It doesn't bother me too much, I think my uploaded data are very limited. I trust people easily*". All participants felt their data were being collected, and the majority of them, although acknowledging this, felt it was acceptable to a certain extent and chose to ignore it to gain the "benefits" of using the IoT technology.

4.5.6 Companies Re-Selling Information

A lead on question from the previous section was how companies use the data they are collecting, and if end users feel like there is a value to their personal information. This was asked to gauge an understanding of whether consumers feel like their data are assets? And if so, how can companies use them to their advantage?

All interviewees expressed a sense of value towards their data and personal information. Participant G was certain that "by law, once you use a company's site or device, they are allowed to use your data. It states this in the terms and conditions on Facebook for example when you upload pictures".

Participant E went into greater detail explaining that “I would assume they re-sell my personal information. That’s something that’s changed in this generation, it used to be that you manufactured a thing and the cost of making that was from various supplies and when you sold it you tried to recoup that investment. That whole business model has completely changed. The cost of making a thing is immaterial because it will continue to deliver value as long as it’s used. As long as it has access to personal information that personal information has a value attached to it and that can continue to be sold.”

The participants were also asked if they felt companies are re-selling their information to third parties and other companies.

4.5.7 Company Transparency

An intriguing topic emerged on IoT and technology companies’ transparency in how they use their consumers’ data. There was widespread confusion among participants, with no one really definitive on what information exactly is being collected by companies.

Everyone that was interviewed agreed that companies need to be a lot clearer in their use of personal data. Participant H felt strongly on the subject “*Yes always, because I feel like the data is mine and not theirs. I don’t think any company out there does a good job of this, that’s why they get hacked left and right. My solution would be keep the data more secure, use encryption and don’t keep it in one location.*”

Participant G stated that “*I think all companies should have their terms and conditions in big print*.” He was also of the opinion that companies keep their real intentions with our data hidden deep in pages of jargon.

4.6 Data Analysis

The interview data collected will be analysed by using IS Theories as a method for finding a patterns to the responses of the participants and to expanding on the usefulness of the theories. The aim is to interpret the data to reveal a greater insight and understanding into the participants' responses. The study will observe how the Protection Motivation Theory (PMT) and Communication Privacy Management Theory (CPM) are underlying theories and form a basis to the participants rational in their responses.

4.6.1 IS Theory

The Information Systems Theory (IST) aims to make a connection between mathematical systemic formalism and information technologies to develop a constructive systemic model, revealing information regularities and specific information code for each object (Lerner 2007). The results of the interviews in this research paper will be qualitatively analysed by a number of IS theories to explore the possibilities of finding a deeper meaning to the results and to answer the research question.

This research will utilise an inductive approach to compare to observational theories - the PMT (Protection Motivation Theory) (Rogers 1975) and also CPM (Communication Privacy Management Theory) (Petronio 1991). Both of these theories are recognised by researchers and academics and have been used in a number of studies. PMT was used in the IS field by Johnston (2010) to introduce the idea of how fear appeal influences end users to take security actions against threats. CPM was used by Child (2009) to research a theory based measure of blogging privacy management, it was later used by Child (2011) to research the 'Challenges of Blogging and Relational Communication on the Internet' it was also used by Xu (2011) to find a link between individuals' perceptions and institutional privacy assurances.

4.6.2 Protection Motivation Theory (PMT) Overview

In IS security and finding the security gap, people primarily consider whether a threat is preventable in the first place ((Boer and Seydel 1996); (Wu, Stanton et al. 2005)). Protection motivation theory ((Rogers 1975)) incorporates controllability factors (locus of

control and self-efficacy) from social cognitive theory ((Bandura 1977)) in this cognitive assessment.

PMT is a theory that explains how individuals are motivated to respond to 'fear appeals', these are warnings about threats or dangerous behaviour. In interpreting such messages, individuals use a cognitive process to weigh their response to the threat (Vance, Siponen et al. 2012). The Protection Motivation theory was first discussed by Rogers (1975).

Previous research that used PMT found it useful in predicting individuals' computer security behaviour, both at home and in organisations ((Lee and Larsen 2009); (Ng, Kankanhalli et al. 2009); Anderson and Agarwal, 2010). The results from the interviews have many elements of PMT theory in the answers of the respondents.

4.6.3 Communication Privacy Management (CPM) Overview

Privacy is a longtime issue within the information systems field, and much research has gone into ways of measuring it (Bélanger and Crossler 2011). There are many information privacy theories, Li (2012) conducted research and discovered fifteen established theories, one of which, CPM, was chosen for this research. Communication Privacy Management (CPM) is a general theory used in understanding how people reveal and conceal private information. CPM was first developed by Petronio (1991).

The CPM theory proposes a dialectic relationship between privacy and disclosure, suggesting a unique way to understand the dynamics of the tension between concealing and revealing private information (Petronio and Altman 2002). CPM is a shift from the perspective focusing on "self-disclosure" ("purposeful process of revealing information about oneself to others," (West and Turner 2010, p.171)) to a more comprehensive view (Petronio, Durham et al. 2008). CPM is a way of discovering boundaries in how users reveal private information, the theory states that the boundaries can range from complete opens to complete secrecy (Margulis 2011, p.12)

Petronio (2002) presents five basic principles of CPM: (1) individuals or collectives believe they own their private information; (2) people feel they have the right to control the flow of private information to others; (3) people utilise privacy management rules to determine the ranges of privacy boundaries; (4) people presume co-owners (shareholders

of the information) will follow existing privacy management rules; and (5) turbulence occurs when the privacy boundary is violated.

The interview data conducted on IoT privacy concerns will be analysed in the next section using the CPM theory to understand how users reveal their private information when using these devices, and any issues they have in revealing their personal information to IoT systems.

4.7 PMT: Protection Motivation Theory

4.7.1 Data Analysis relationship to PMT

There are six key points in the PMT theory, and some of the interview answers collected alluded to these. PMT proposes that motivation to protect one's self from risks comes from the following factors - perceived severity, perceived vulnerability, and the perceived response efficacy (Rogers 1975). To explain failure to engage in protective behaviour, the model was modified to include three cognitive appraisals - self-efficacy, response costs and rewards associated with risky behaviour (Maddux and Rogers 1983). The diagram below outlines the theory of PMT and it will be explained in greater detail in the sections that follow

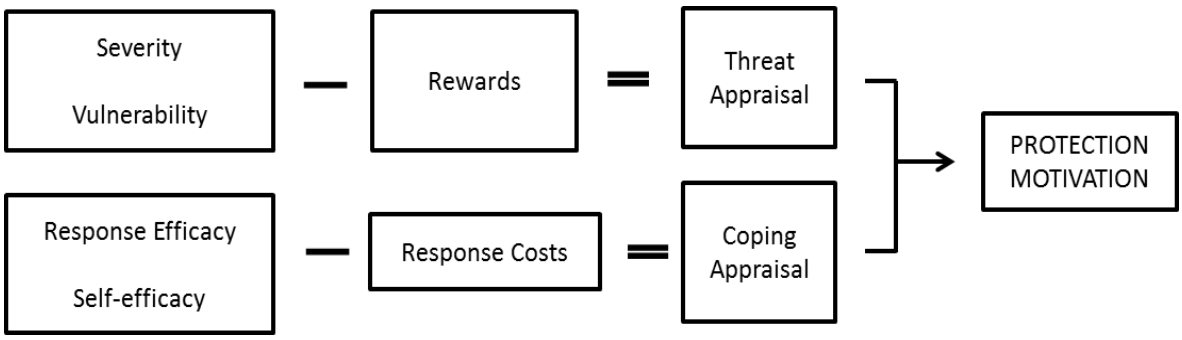

Figure 10: Cognitive process of PMT, Source: (Maddux and Rogers 1983, Rogers and Prentice-Dunn 1997)

4.7.2 Security Threat Appraisal

Security Threat Appraisal is similar to the perceived risk, which can be explained as uncertainty and consequences (Crossler 2010). In a study investigating online privacy behaviour of teenagers online, the perceived risk led to a lower willingness to provide information to websites. Those who did not provide personal information to websites were also more likely to practice other coping behaviour, such as providing false or incomplete information (Youn 2005).

Perceived Severity

Perceived severity refers to judgement of the severity of the consequences resulting from a threatening security event (Larose, Rifon, Liu, & Lee, 2005). The greater the perceived severity and seriousness of the threat, the more likely online consumers adopt protection (Larose et al., 2005). Research suggests that perceived severity impacts decisions of home wireless network users to implement security features (Crossler, 2010) and influences the intentions to use anti-spyware software (Chenoweth, Minch, & Gattiker,2009).

The question on perceived severity related to the consequences of the users' IoT devices being hacked, and what information could be collected on the users. In general the data collected on the devices were believed to be everything from personal information like date of birth, name and address to credit card information. The participants were feeling anxious about this data collection in general if it got into the wrong hands.

ID	Perceived severity	Level
A	"I treat any data that is online about me as public data. I wouldn't be surprised if something online comes back to haunt you in a few years". "All information belongs to Google because I'm on an Android phone" "weight, height, heart rate, GPS - are stored on my IoT devices"	Low
B	"I wouldn't like stuff about me posted online, in general I don't want my data online""If I was a bank robber I might care about being tracked whereas I don't really care about it." Your device knows "health, location, height, name, age"	Medium
C	"I think the data uploaded about me is very limited" "However, I wouldn't want to expose health or location data. It makes me uncomfortable"	Medium
D	"I don't want other people having access to my data or stealing my data. I think companies have too much access" "My address, credit card numbers etc are tied to my IoT devices"	High
E	"I don't share anything on my IoT device to a social media site that I consider private. There's a limit to what I share online" "My banking information is a concern, I am more cautious with that data"	Medium
F	"If someone has access to your IoT account (Google Play) they can easily get access to your credit card if thats linked. They could use your email account to get access to the other accounts that are linked"	High
G	"Not concerned about my personal data on my smart devices" "everything resets itself on my smartwatch when it gets turned off, the information is only stored on the watch"	Low
H	"I know what can be done with personal information. It can completely destroy your life"	High
I	"My personal details, date of birth, location data are at risk. My biggest concern is you don't see what information is being stored and how, the ones listed previously are just the tip of the iceberg"	High

Figure 11: Perceived Severity of participants'

Perceived Vulnerability

Perceived vulnerability is the degree to which an individual believes a threat will affect them (Lee, Larose et al. 2008). When it comes to virus protection, Lee(2008) found that people who perceive a threat of the likelihood of a virus attack are more likely to engage in virus protection. Increases in the number of internet virus vulnerabilities will increase an individual's intentions to adopt antivirus software. Another study by Dinev (2004) found that the perceived vulnerabilities related positively to privacy concerns. The perceived vulnerability helps to explain why some people backup their computer data.

The interviews conducted found that the users who perceived the threats of losing information privacy through IoT devices were more concerned about protecting their private information. The participants were asked questions such as "does privacy or security matter to you in relation to your personal information?"

The users who perceived the threats of losing information privacy through IoT devices are more concerned with protecting their private information. This is evident in the responses from Participant F, H and I. When asked "does privacy or security matter to you in relation to your personal information?" Participant F stated that "Yes, because your personal information can be used to get at your financial information easily". Participant F practices high levels of security by setting up fake email accounts when using IoT devices and has different passwords for all of his devices. Participant H has similarly high levels of perceived vulnerabilities when it comes to IoT, he stated that "I know what can be done with personal information. A tiny bit of personal information can do massive damage if hackers get their hands on it". He also practices using fake email accounts for all his IoT devices and uses different passwords for each device.

When it came to newer IoT technologies, for example smart cars that users do not yet own, the vulnerability perceived among the participants was much higher. Participant B stated "People can shut down the cars remotely, I have seen it on the news. I would be reluctant to use an automated car in the next 10 years. Maybe when security gets better. I wouldn't at the moment." Participant C had a similar view "For smart cars people need to monitor it more. The auto pilot part I wouldn't trust it 100% so I would keep a close monitor on it while using it."

ID	Perceived vulnerability	Level
A	"For whatever reason I have never thought of security on my wearable device"	Low
B	N/A	
C	"If burglars know your location they can break into houses however I don't think there are many high tech thieves out there"	Low
D	"When it comes to IP cameras, I think they are vulnerable to attacks. I've seen videos of hacked IP cameras posted online many times" "Theres always loopholes and backdoors in software" "I don't think anything is 100% secure"	Medium
E	"I make informed decisions about the maturity of technologies and how well the infrastructure is around it." "I would never leave a device on its own and walk away, even in work.. For theft reasons"	High
F	On your IoT device "..your personal information can be used to get at your financial information easily"	High
G	"I never leave my devices unattended, If I'm not in the room the device is switched off"	High
H	"I know what can be done with personal information. A tiny bit of personal information can do massive damage if hackers gets their hands on it"	High
I	"I hear stories all the time of phishing and fraud attacks, there seems to be a massive amount of that going on" "I'm concerned to protect my devices as much as I can by using pinches, passwords etc"	High

Figure 12: Perceived vulnerability of participants'

Maladaptive rewards

Rewards refer to the expectations of benefits to continue based on the behavioural choices (Lee, Larose et al. 2008). Among consumers, individuals decide to participate in a social contract when they perceive that benefits outweigh the risks associated with information disclosure and this decreases the motivation for privacy protection ((Phelps, Nowak et al. 2000); Sheehan & Hoy,2000). Adolescents aged 14–18 are more willing to provide personal information to a website when they perceive benefits in return (Youn, 2005).

"*When individuals perceive the benefits on social media sites like getting connected with others or playing games, they may consciously expose their personal information toward attaining these benefits*" (Mohamed and Ahmad 2012).

In IoT devices the maladaptive rewards are very evident, and the interviewees' information on why they use these IoT devices alluded to this. For example, users provide personal information such as health data and location data, ignoring any privacy concerns they have, to get the benefits of using wearable IoT devices. Users liked the fact that their smart TVs can now show Netflix to them and tell them when new episodes of their favourite TV shows have been released.

ID	Rewards
A	"With my Garmin 520 I can track my GPS and monitor my vital stats such as heart rate" "I am able to track my cycles and share data with other guys on my team with Strava"
B	"Track my heart rate and runs"
C	"With my IoT security system I can monitor my house when I am away from home via a handy app on my phone"
D	"I use my smart TV to watch my favourite shows on Netflix, which I can't do on a standard TV"
E	"With my IoT alarm system I can login to an app and see my pets while Im out and about. Anytime there is movement in the house or the property is broken in to the cameras can record the activities" "My polar m400 can track my health data"
F	"My smart TV box allows me to watch my tablet screen on the TV"
G	"My IoT android TV box allows me to do anything I could do on my phone, on my TV" "My Bluetooth smartwatch allows me to record my sleep patterns and record how many steps I have taken" "My smart TV box tells me when my favorite TV shows come out"
H	"I have tried numerous IoT devices but after a while I no longer use them"
I	"I use the smart TV just for the Netflix app that's it"

Figure 13: Rewards

4.7.3 Security Coping Appraisal

The security coping appraisal consists of security self-efficacy, response efficacy and prevention cost. In the coping appraisal a person's response efficacy and self-efficacy must outweigh the response costs for engaging in the protection motivation.(Lowry 2015).

Perceived response efficacy

Response efficacy is an "*individual's confidence that a recommended behaviour to prevent or to mitigate the threatening security event*"(Crossler 2010). In other words, this is the belief that a recommended coping response is effective in protecting from a threat (Woon, Tan et al. 2005). Mohamed (2012) found that in relation to social media, individuals who believe that a protective action can be taken to avoid consequences of losing information privacy are more likely to be concerned with privacy. Participants were asked about their perceptions on security updates, and as to whether they aid or hinder their IoT devices in preventing security threats. The answers to these questions allow an understanding to the perceived response efficacy of IoT users.

ID	Perceived response efficacy
A	"Usually security updates makes devices more secure"
B	"Yes in general, they do"
C	"I don't pay particular attention to them, only when I get a message saying to update"
D	"I like to think if its a specific security update it will actually make things more secure"
E	"Yes, its going to make things more secure" "I tend to update with every patch"
F	"Yes, updates help security and usability, they normally make things faster"
G	"I would make sure all security updates are installed on my devices where possible but I pick smart devices based on best apps. I wouldn't be concerned with security as a first priority"
H	"Yes they make things more secure, as sib as a security update is out I will install straight away"
I	"Yes, I think updates increase security and get released for a reason"

Figure 14: Perceived response efficacy of the participants'

So in general participants were very positive towards there perceived response efficacy when it came to IoT devices. From the findings here it alludes to the fact that IoT devices need to be regularly updated and the vulnerabilities found need to be mitigated against by IoT companies software updates.

Self-efficacy

Security self-efficacy is “an individual’s confidence in his/her own ability to perform the recommended behaviour to prevent or mitigate the threatening security event” (Crossler 2010). The previous research conducted in PMT points to low self-efficacy leading to omission of security measures, and related research into omissive security behaviour finds support for this theory (Pahnila, Siponen et al. 2007), (Woon, Tan et al. 2005).

Research in related areas supports similar predictions, for instance, people who have higher self-efficacy are more effective in learning how to implement IS security measures than those who have lower self-efficacy (Gathegi and Workman 2005). Within the context of the interviews conducted it was found that individuals who believe they have the ability and control to protect their information on IoT devices will be more concerned with privacy. Consequently, they will also most likely enable privacy measures on their IoT devices. Hence, it is hypothesized that users with high self-efficacy in using privacy measures on their IoT devices have higher concerns with their information privacy.

Each participant was asked “how much control do you believe you have over the information on your smart device?” and “what steps do you take to protect your private information?”

ID	Self-efficacy	Level
A	"whenever I see the options to disable privacy tracking I do, for example Google Ads" "all information on my smart devices belong to Google"	Low
B	N/A	N/A
C	"For certain IoT apps I disable privacy and security data, I do this when I feel its not necessary for apps to have this information".	High
D	"I have little control, so I try to keep the amount of information stored on my IoT devices to a minimum."	Low
E	"Very little, I know my information gets stored on Apples servers"	Low
F	"Very little, companies that own IoT apps and devices have the access." To combat this the participant sets up fake email accounts for each IoT device which is seperate from any other system.	High
G	"Everything is stored on my watch. Theres nothing stored externally" "I disable certain settings, theres noway for another IoT device to connect to mine without me knowing about it"	Medium
H	"I believe I have full control over my IoT devices" this participant created fake email accounts when using different IoT devices and he also setup different passwords for different devices.	High
I	"I feel there's no control." "I don't think I'll ever be in the market to buy other IoT devices, my issue is that there is no information available to me about what these companies are storing about me"	Low

Figure 15: Self efficacy of the participants'

Response cost

The response cost in PMT hypothesises that "*as the response cost goes up, the likelihood of preforming the adaptive coping response goes down*"(Crossler 2010). This is in line with other IS security models (see (Karabacak and Sogukpinar 2005)) which means that users directly or subconsciously measure the likelihood of the threat occurring and the expected consequences of the threat versus taking preventative measures. This is evident in how the participants didn't view security updates as a priority in their buying decisions of their IoT devices. Participant B felt that "It wouldn't be a criteria I would base my purchase

on" and Participant G said he bases IoT purchases on "*the devices with the best apps and security is not a first priority*". There is more evidence of this in the device purchases of some of the users opting for Chinese or non-branded IoT devices that don't get security updates but provide the same entertainment features at a reduce cost - Participant F has a Chinese android media player and wifi radio, Participant G has a non-branded smartwatch. When security updates are included in IoT devices (see *Perceived response efficacy)* the participants all responded positively which shows that if there is a low response cost they will take the necessary security actions. However, when there is a cost involved even an intangible one like the time spent to read privacy policies and investigate if they really agree to what is shared, users where unwilling to do so.

4.7.4 PMT Summary

It has been found that while they feel concerned for the privacy and security risks, the users are not going to stop using the IoT devices they have already adopted. The participants generally would like security updates for their devices. It has also been found that the degree of the intent to adopt protective behaviour depends on the amount of protection motivation of an individual. Participants F, H and I have shown they value their private information highly and are willing to go take extra steps to protect those data, for example by setting up fake email accounts and using different passwords for every device they own. The research correlates to Lee's (2008) statement that "*through the cognitive processes, a greater protection motivation leads to greater intentions to carry out protective behaviour".*

4.8 CPM: Communication Privacy Management

4.8.1 CPM and Interviews Data

In the past CPM was originally used to describe the tradeoff between costs and benefits associated with interpersonal disclosure, however the mental calculus is similarly performed when determining whether to disclose electronic information (Dinev and Hart 2006). The interviews were mainly focused around security and privacy questions. CPM was chosen as the framework to follow based on the themes that emerged from the interviewees' answers, there was a strong concern among IoT users about their private data.

The interviews are analysed below and compared to the CPM theory to see if any patterns emerge in the participants' data and responses. CPM utilises the idea of privacy boundaries for disclosing information, these boundaries can range from complete openness to complete closure. Open boundaries reflect granting full access to private information through disclosure or view of information, while closed boundaries represent that information is concealed and protected (Margulis 2011).

CPM stipulates five principles about privacy management that give a route to better understand both when access to the information is granted and when access is denied (Petronio and Altman 2002). These five principles are discussed below and the interview data are analysed in reference to them.

4.8.2 Individuals or collectives believe they own their private information

The first principle of the CPM theory states that individuals believe they own their personal information in the same way they own possessions (Child, Pearson et al. 2009). Throughout the interviews it became very evident that participants were the owners of their private data. When asked about company transparency, participant H expressed that personal data belong to him "*Yes always, because I feel like the data are mine and not theirs.*"

One of the interview questions stated - "*Does privacy matter to you in relation to your personal information?*" The responses to this question were very coherent, all participants seemed to value their personal information. Participant A responded "*Yes,*

usually big time", Participant C said "*Yes, I avoid providing detailed information online*", Participant D simply stated "*Of course, I try to be as secure as possible…*", Participant E "*It absolutely matters to me*".

Interestingly Participant H compared personal information to being similar to a financial value, he responded that "*Yes, because your personal information can be used to get to your financial information easily*". He then went on to explain how phishing attacks for example is a tactic used by hackers pretending to be a company or person they are not who the end user trusts, asking for personal details. Personal information has a value, and while some respondents did not know the exact value of that information, they were all able to identify it as being valuable, especially to companies who create IoT systems and devices.

4.8.3 People feel they have the right to control the flow of private information to others

The second principle of CPM is privacy control, this means that when users share private information with an IoT device they still believe the personal information belongs to them and they should be able to control it. Petronio (2013) describes it as follows "*...because individuals believe they own rights to their private information, they also justifiably feel that they should be the ones controlling their privacy. This assumption stands true even after giving access to authorised others.*" The concept of privacy control originates from Westin (1968) and Altman's (1975) theories on general privacy.

When participant A was asked about "Do privacy or security matter to you when devices connect to the internet?", he immediately began to explain how he is cautious, for example when on Facebook he likes to go through the settings and change the privacy levels. He also stated he does the same when it comes to IoT apps, stating "*I like the way there is more permissions nowadays on Android than before when you said a blanket yes to everything…the more options you get the better*".

The interviewees were asked "*How much control do you believe you have over your personal information stored on your smart devices*?" The respondents had strong feelings towards this question; there was a clear lack of control on privacy when it came to using IoT devices. Respondent I who was the oldest participant summarised it as follows "*I feel there's no control. I don't know all the different kinds of information that is being stored about me by the device provider*". Later he went on to state that "*I feel companies should*

be more transparent with my data. I don't feel comfortable supplying data to companies…if they were more transparent it would give more control. Individuals can then make choices but they can't do it without information". Participant D echoed these thoughts and felt there was "*very little control*", he went on to state that it is why he tends to "*keep the amount of information stored to a minimum*".

Participant H began by stating that he has full control, but then went on to say "… even if you give the command to delete information from these services (referencing IoT), you don't know if it is actually deleted."

4.8.4 People utilise privacy management rules to determine the ranges of privacy boundaries

The third principle perceives that people develop and use privacy rules to control the flow of information to others (Petronio 2008). People use privacy rules based on personally important criteria to control the distribution of information (Margulis 2011). Individual privacy rules are based on cultural values, gender orientations, motivational needs, contextual impact and risk-benefit ratio (Margulis 2011). This feeling is true for IoT users also, they still believe that they should retain the rights and responsibilities to regulate how much information is shared with others. By others this refers to other third parties but also other devices.

To one of the interview questions asked, "*Do you leave location data on, on your IoT device?*" Participant E stated that "*never, in fact it's one of my pet hates*" when installing an app for his Apple watch he described the options as "*1. Never share location data to the app, 2. Only share while app is active, 3. Always share*", he felt so strongly on the subject that he "*actively deletes apps that don't ask for permission to use those data. I'm always thinking of the principle of granting the least access needed*". In this answer the respondent clearly shows how he likes to control his private information when using an IoT device, he wants the control of that private information to be under his discretion and any change to that leads to a conflict. He has a criterion that is "*least access needed*" this means that he feels permissions to IoT apps should only be given when needed to perform a particular function and not be granted at all times.

Participant C has a similar usage method, he said that “for certain apps I would disable privacy and security data, I do this when I feel it’s not necessary for certain apps to have this information. For example location data, I stop this being shared”.

The interviewees were asked “Do you have any apprehensions about your devices connecting automatically without your interaction?” and then subsequently asked “Would you disable it if you had the opportunity?”

4.8.5 People presume co-owners (shareholders of the information) will follow existing privacy management rules

The forth proposition is that once private information is shared, a collective privacy boundary is formed and the receivers of the private information become co-owners (Margulis 2011). This is evident with IoT companies and their consumers, the participants believe that their private information is secure when known to IoT and technology companies.

For example, the interviewees were asked “do you think that companies are using your data from these connected device securely?” Participant C felt that “...it doesn’t bother me too much, I think the data uploaded are very limited”.

Participants were also asked “*How much control do you believe you have over your personal information stored on your smart devices?*” Participant A began by stating that Google and Android know everything about him based on all of his smart devices information, however he was not that concerned about that because he considered Google a big company. He said that “...they are just using the information internally to make their own products better”. He went on to state that he is more worried about smaller companies.

4.8.6 Turbulence occurs when the privacy boundary is violated

The fifth and final principle of CPM is when privacy rules are not co-ordinated between the original owner and the co-owner, there is a possibility of boundary turbulence. Boundary turbulence occurs when co-owners fail to effectively control the flow of private information to third parties (Margulis 2011). This can be explained in the feedback in relation to companies passing on private information to third parties. Participant D felt that

IoT companies have too much access “I think they have too much access, I don’t think anything is 100% secure. I have seen this in the past with password leaks, credit card leaks, playstation network leaks etc”. Participant I said that “I don’t think I’ll ever be in the market to buy other IoT devices, my issue is that there is no information available to me about what these companies are storing about me”.

Turbulence was also evident in the answers of the participants gave on one of the probing questions “*would you adopt a self-driving car?*”. Participant B stated that “*people can shut down cars remotely I have seen it on the news. I would be reluctant to use an automated car in the next 10 years*”. Participant C said “*for cars people need to monitor it more*”. Both participants answers indicated privacy boundary violation occurred in self driving cars as they had read in the news of how they had been hacked (see (Hern 2016)).

According to CPM, people who have experienced privacy turbulence will have stricter privacy rules in managing their private information (De Wolf, Willaert et al. 2014). This is true with the interviewees; Participant H had strong privacy concerns and conceals his information wherever possible from IoT companies. He suffered many examples of turbulence, for example one of his Facebook accounts was hacked in the past; this led him to take IT security more seriously.

4.8.7 CPM Summary

IoT is a new technology phenomenon and this study on how the CPM theory can relate to IoT and its uses is the first attempt. CPM has only recently been used in the IS field to aid in explaining how social networking privacy is managed (Child and Petronio 2011). The CPM theory is still in its infancy and so is IoT. While some of the principal traits of CPM relate to the privacy answers derived from the interviews, the theory needs to be adopted more towards Information systems in the future.

4.9 Summary

This chapter presented the analysis from the data collected as part of the research. The data source used in this study was semi-structured interviews with a total of nine participants.

The participants were asked to explain their IoT device usage and understanding. General security and privacy behaviour were discussed in order to get a view of each individual's perceptions and concerns.

The data collected were analysed, and initial themes and observations were noted. Finally, two theories were discussed as the data collected showed a link to these theories.

Chapter 5: Conclusions and Future Work

5.1 Introduction

This thesis has investigated the privacy and security concerns of IoT device users. The study was undertaken after reading the increasing number of articles, both academic and in the media, on the subject of IoT and its security risks.

From the literature review conducted in Chapter 2 the IoT age of technology is upon us and the number of devices is set to grow substantially. While many privacy and security risks associated with the technology remain, researchers and developers must work together to tackle these threats as they have already done with many other technologies.

During the research methodology stage investigated in Chapter 3 it was determined that a constructivism ontology, an interpretive epistemology, an inductive methodology and a qualitative method would be used. It was therefore decided to use semi-structured interviews for data collection in order to discover in-depth or hidden meanings in the participants' answers.

The research outcomes were presented in Chapter 4. Initially the key themes and observations of the interviews were discussed. Then it emerged that the answers taken from the interviews could be analysed by security behaviour theories. The two theories chosen were the Protection Management Theory (PMT) and the Communication Privacy Management Theory (CPM). The outcomes from the research suggest that users are worried and uncomfortable about their privacy being breached, and generally try to protect as much information as possible. Users feel that IoT companies should being doing much more for them in terms of security and private information collection transparency. While these issues remain at large among IoT users, they remain active users of the technology which suggests that the cost-risk benefit ratio is towards continued use of the technology.

This chapter will illustrate further the outcomes of the research and explain how the research question has been answered. It will then discuss the limitations to this research paper and the any future work that can be investigated around IoT.

5.2 Answering the Research Question

"Will security and privacy threats prevent users from adopting the Internet of Things?"

The simple answer to this question is "No", the rate of IoT adoption is growing substantially, and the participants follow this trend. The majority of participants (with the exception of the oldest) plan on buying more IoT devices in future. Common devices such as wearables, smart TVs and fitness bands have already made a huge impact on people's lives and will continue to do so. While newer IoT technologies that are considered a "high risk" (the smart car: may take much longer to penetrate the market), it is believed that once they have been established as safe and secure users will begin to use these also.

As represented in the graph below, the estimated number of smart devices is set to reach 50 billion by 2020, and the privacy and security concerns are not envisioned to prevent this. The year is displayed on the bottom of the figure and number of devices (in billions) is on the left side.

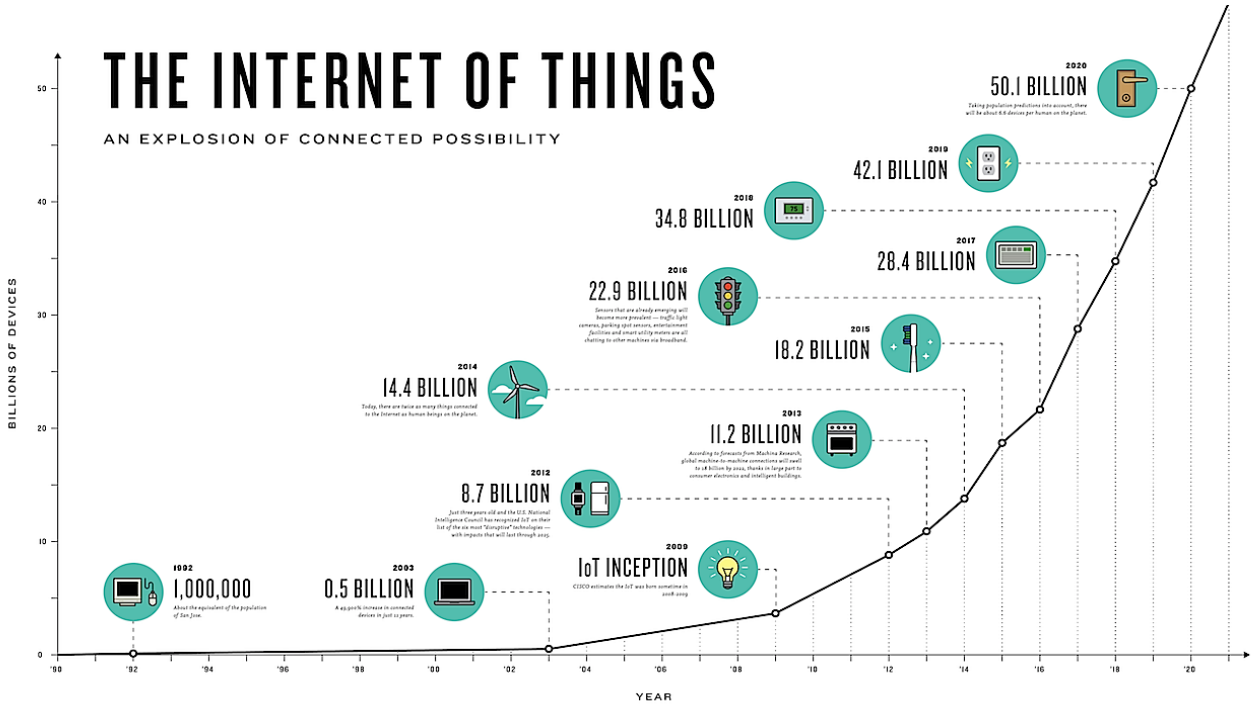

Figure 16: The Internet of Things - Source: (Ncta 2014)

The sub questions raised in section 1.2 have now also been answered and can be summarised below,

“What are the IoT devices most commonly used by consumers?” Currently it appears wearables, smart watches and smart TVs are the most common IoT devices used.

“Are users aware of the private information they share when they use IoT devices?” In general they are not aware of what private information is shared when using IoT devices. The majority of participants suspected that much more personal information is gathered than they would have liked.

“What are the general security perceptions of users when using technology?” Generally users trust technologies that they will provide a level of security to their private information. The well-established technology companies such as Apple and Google are viewed as safe device providers who follow general industry best practices for security.

“Are users willing to share their private information?” At the moment users have tentatively agreed to share some of their private information with IoT tech companies, however they are not happy about the lack of transparency of IoT companies. They agreed that the privacy policies are convoluted and it is difficult to decipher what exactly is being agreed to.

“Do users have any thoughts about if the data on these devices are stored safely and where?” As the interviewees were generally from an IT background they had an understanding of how their data might be stored in the cloud or in a server farm owned by the IoT company, however they did not feel comfortable with the lack of information around the subject. They would like IoT device manufacturers to be clearer in future as to where data are kept and stored and for how long.

“Do users have any opinion in relation to risks and the use of IoT objects?” The interviewees had not thought fully about the security risks when using their IoT devices. The devices users have bought and use on a daily basis are safe in the eyes of consumers. They enjoy the benefits and entertainment values the devices provide over any concerns or perceptions.

5.3 Findings

5.3.1 Privacy Concerns

There is definitive concern about private information stored on IoT devices. Many participants feel that the IoT companies have full control over their private information so they have been reduced to creating false email accounts and disabling usage tracking where possible. This study has found that individuals who have been exposed to or the victim of personal information breaches have a stronger concern regarding the privacy of their information on IoT devices. This finding is in line with Smiths'(1996) findings. Technology companies as a whole need to be more transparent to their users and return more privacy controls to the end user.

5.3.2 Privacy Risk Vs Benefit

Privacy risk can be described as a measure of the potential loss of private information (Dinev and Hart 2006), while privacy benefit is the associated benefit of disclosing private information. Concern and trust were two key variables when it came to considering the costs and benefits involved in privacy disclosure, which is in line with what (Dinev and Hart 2006) and (Gefen, Karahanna et al. 2003) discovered also. This study found that in general IoT users take into consideration the privacy risks when using IoT devices, but they feel the benefits to be obtained are much greater in return. Participant B sums this feeling up in saying that "*companies are collecting a lot more data than I want them to but not enough to put me off using IoT devices*". Participant D felt a similar way, by saying "*I continue to use these devices even though I don't like the privacy risk, for connectivity, entertainment purposes and the amount of things you can do with them (IoT devices)*".

While the literature review has pointed to a large number of vulnerabilities in the privacy and security of IoT devices, they are still being used and bought by consumers. The perceived benefits of using the devices outweigh any concerns or threats to personal information. This discovery was also made by Adams (Adams 1999) research, i.e. that new technologies are often considered acceptable if the invasion of privacy is not personally faced, even if the technology has major potential privacy risks.

5.3.4 Privacy Policies

IoT privacy does matter to users, however, as suggested in the findings from PMT, the users' involvement with privacy issues and their perceptions of their own ability to protect privacy affect their behaviour. In the interest of the general users' protection, IoT devices should display more clear and conspicuous information about their information practices, including explicit warnings of the risks they pose to their users. IoT companies and manufactures need to be much more transparent with the information they collect on their users and how this information is stored and used.

5.3.5 IoT Security

The literature review found a large number of security vulnerabilities in IoT technologies. There are more vulnerabilities with this new technology than with more established technologies because of the interconnected nature of the IoT devices. These security vulnerabilities need to be urgently addressed and mitigated. There is a need to educate all IoT users on the dangers of using IoT devices and that they have the same dangers as connecting online in general.

5.3.6 IoT Adoption

With this group of participants the study found that the younger the end users, the more open to new technologies they will be. Perhaps this is due to their frames of reference (see (Orlikowski and Gash 1994)). For example, the youngest participant 'G' listed owning five IoT devices and the oldest participant 'I' owned only one IoT device. The younger participant was open minded to owning more IoT devices while the oldest participant saw them as merely unnecessary gadgets.

5.3.7 Research Contributions

The research findings have provided academic researchers and industry analysts with insight into the security and privacy perceptions of IoT users. They provide a baseline for future research work to develop a more secure and private IoT environment. They will also aid in enabling IoT technology companies to understand that their users require more controls of their privacy when using IoT devices.

5.4 Limitations of Research

There are a few limitations to this research paper. The main focus of the study was on the understanding of IoT devices among their users, so because of this the interviewees may have had a reasonably positive stance towards IoT technologies to begin with.

The majority of the participants came from an IT background, either working in the field or studying that field, so their knowledge and understanding on the subject would be more technical than that of the average user. So a future study on a set of subjects from a non IT background would be useful.

Due to the small sample size used in this study, the results are not representative of the wider population. The results in this study from the CPM framework have not uncovered the full range of issues influencing boundary opening and closure. In particular, future research that focuses on unique and distinct segments of the population (e.g. older IoT users, younger IoT users, non IoT users etc.) may find a substantially different mix of motivations and priorities concerning privacy regulation.

The results from this study are interpretive and hence based on the personal experiences of the participants. Perhaps using a different research philosophy such as a quantitative philosophy would yield different and more generalised results.

As IoT is a quickly evolving technology this should be taken into account when reading the paper, as in the future many of the issues raised will have been addressed and answered.

5.5 Future Work

This section outlines some of the future areas of research based on the information discovered while conducting this thesis.

IoT technologies are still a relatively new concept, and while a huge amount of technical research has been done on the security and privacy issues posed by the IoT, there has been very little research on the end users' opinions or qualitative analysis on the subject. More qualitative research and analyses need to be done to fully understand the privacy perceptions of IoT users and how the technology can be advanced to protect them.

Based on the literature review IoT has a very complex nature, and developments in IoT security standards and perhaps a governing body are needed to manage the quality of produced IoT devices.

The research could also be conducted using the IUIPC (Internet Users' Information Privacy Concerns) theoretical framework (Malhotra, Kim et al. 2004). This framework is a way of finding individuals' beliefs and behavioural intentions when it comes to internet usage, this could be modified to reflect on their thoughts on IoT.

This research was conducted using the opinions of people based in Ireland, a broader geographical location base would be of interest to see if the findings are similar or different. Also, it would be possible to conduct the research in a poorer area where the population might not yet have experienced IoT technologies to see how their opinions differ.

5.6 Conclusion

This research paper has discovered several interesting findings of how IoT users perceive privacy and security. The research established that while IoT adoption is growing and the trend is set to continue, the growing privacy and security perceptions must be addressed.

While users would prefer a more secure and private IoT environment, in practice they compromise these concerns for the benefits and enhancements the technology brings to their lives. However, a major security data breach or privacy threat could change these opinions drastically.

IoT users would like more transparency from companies on how their data is being collected and the purposes for which it might be reused. They would like additional controls to be granted to them to protect their private data.

These findings and existing literature will lead to a more secure IoT environment for both users and private companies. The results can be built upon in future IoT research studies.

Appendices

Appendix 1 - Ethics Application and Supporting Documentation

- obtain continuous feedback from participants about ethical issues;
- periodically review the ethical strategy in the light of feedback received; and
- if required, update their ethical procedures;
- retain copies of consent forms signed by the participants.

Composition of the SCSS Research Ethics Committee
The Committee will consist of a Chairperson/Convenor appointed by the Director of Research and two other experts – a member of the School's academic staff and external advisors. The internal and external members will be selected from a panel approved by the Director of Research from time to time. Members will be selected on a case by case basis by the Chairperson subject to their availability. Researchers will be precluded from the Committee considering ethical approval for their study.

School of Computer Science and Statistics
Research Ethical Application Form

Part A

Project Title: **The Internet of Things - A Study of User Security and Privacy**

Name of Lead Researcher (student in case of project work): **Cathal Enright**

Name of Supervisor: **Patrick Joseph Wall**

TCD E-mail: **caenrigh@tcd.ie** Contact Tel No.: **0863662413**

Course Name and Code (if applicable): **Masters in The Management of Information Systems**

Estimated start date of survey/research: **17/05/2016**

I confirm that I will (where relevant):

- Familiarize myself with the Data Protection Act and the College Good Research Practice guidelines http://www.tcd.ie/info_compliance/dp/legislation.php;
- Tell participants that any recordings, e.g. audio/video/photographs, will not be identifiable unless prior written permission has been given. I will obtain permission for specific reuse (in papers, talks, etc.)
- Provide participants with an information sheet (or web-page for web-based experiments) that describes the main procedures (a copy of the information sheet must be included with this application)
- Obtain informed consent for participation (a copy of the informed consent form must be included with this application)
- Should the research be observational, ask participants for their consent to be observed
- Tell participants that their participation is voluntary
- Tell participants that they may withdraw at any time and for any reason without penalty
- Give participants the option of omitting questions they do not wish to answer if a questionnaire is used
- Tell participants that their data will be treated with full confidentiality and that, if published, it will not be identified as theirs
- On request, debrief participants at the end of their participation (i.e. give them a brief explanation of the study)
- Verify that participants are 18 years or older and competent to supply consent.
- If the study involves participants viewing video displays then I will verify that they understand that if they or anyone in their family has a history of epilepsy then the participant is proceeding at their own risk
- Declare any potential conflict of interest to participants.
- Inform participants that in the extremely unlikely event that illicit activity is reported to me during the study I will be obliged to report it to appropriate authorities.
- Act in accordance with the information provided (i.e. if I tell participants I will not do something, then I will not do it).

Signed: Cathal Enright Date: 27/04/16

SCSS Research Ethics Application Form September 2011

Part D

If external ethical approval has been received, please complete below.

External ethical approval has been received and no further ethical approval is required from the School's Research Ethical Committee. I have attached a copy of the external ethical approval for the School's Research Unit.

Signed: ..... Date: .....
Lead Researcher/student in case of project work

Part E

If the research is proposed by an undergraduate or postgraduate student, please have the below section completed.

I confirm, as an academic supervisor of this proposed research that the documents at hand are complete (i.e. each item on the submission checklist is accounted for) and are in a form that is adequate for review by the SCSS Research Ethics Committee

Signed: PJ Wall PJ WALL Date: 27 April 2016
Supervisor

Completed application forms together with supporting documentation should be submitted electronically to research-ethics@scss.tcd.ie Please use TCD e-mail addresses only. When your application has been reviewed and approved by the Ethics committee hardcopies with original signatures should be submitted to the School of Computer Science & Statistics, Room F37, O'Reilly Institute, Trinity College, Dublin 2.

Appendix 2 – Information Sheet for Participants

TRINITY COLLEGE DUBLIN

School of Computer Science and Statistics

INFORMATION SHEET FOR PARTICIPANTS

Research Title:

The Internet of Things - A Study of User Security and Privacy

Lead Researcher:

Cathal Enright - Trinity College Dublin, School of Computer Science & Statistics

Supervisors:

Patrick Joseph Wall - Trinity College Dublin, School of Computer Science & Statistics

Lead Researcher Contact Details*:*

Name: Cathal Enright

Phone: +353 (0) 86 3662413

Email: caenrigh@tcd.ie

Expected Duration of the Research:

The expected duration of this research is between May and August 2016.

This study is conducted in partial fulfillment of Cathal Enright's MSc in Management of Information Systems, to be awarded by the School of Computer Science and Statistics, Trinity College Dublin, Ireland.

Background to the research:

The Internet of Things (IoT) is the next big revolutionary technological change and many researchers make the claim that it is about to change the way we live our lives. Broadband Internet is become more widely available, the cost of connecting is decreasing, more devices are being created with Wi-Fi capabilities and sensors built into them, technology costs are going down, and the smartphone industry is bigger than ever and rising. All of these things are creating a huge interest in IoT.

IoT is the concept of connecting any device to the Internet (and/or to each other). Examples include health wearables, the Apple watch, smart TVs, smart fridges and self-driving vehicles etc. This will bring with it a very complex set of security and privacy issues, for the companies who build the products and the users of the IoT devices.

This research proposes to examine users perceptions of security and privacy issues while using IoT smart devices. The research also aims to find if consumers are concerned about their private data being stored and shared on IoT devices. The aim is to provide an overview of users perceptions and concerns. The research may also suggest ways in which users can mitigate their security and privacy concerns.

The procedures relevant to the participant within this particular study:

The lead researcher invites you to participate in this project based on the fact that you are currently, or have been previously, using IoT devices. Your participation will involve a semi-structured interview which will last between 30-60 minutes. The topics covered in the interview will include, but are not limited to, your understanding of IoT, a description of your IoT devices, a description of how you interact with these devices, what information you share on your IoT devices, what concerns you have while using such devices (including any security or privacy concerns while using technology in general), and your overall opinions about IoT. In some cases, I may ask that you participate in a short follow up interview. This will only occur where there is a need to confirm prior findings and/or identify any changes that may have taken place since the initial interview. For any participants who are to be re-interviewed, the same interview guide and Participant Information Sheet will be used.

Interviews will be electronically recorded. The recordings will be taken on a voice recorder application on the researcher's android smartphone. The recordings will be taken as .mp3 files. The recordings will be transferred to the researcher's laptop for transcribing purposes and deleted from researcher's smartphone immediately after transfer. The recordings will be kept on the researcher's laptop encrypted until September 30th 2016. Participants will be informed of this prior to the commencement of the interview and will be given the opportunity to withdraw from the interview process if they would prefer not to be recorded. Participants will also have an opportunity to review all recordings after the completion of the interview process and make any changes and/or corrections they deem necessary. All interview recordings will be encrypted and only the lead researcher and the research supervisor will have access to these recordings. Any recording made will not be replayed in any public forum or presentation of the research. You may stop electronic recording at any time, and you may at any time, even subsequent to your participation in this research, have such audio and/or video recordings destroyed. At no time will any electronic recording be identifiable unless you give prior written permission.

If you wish to participate in this research, you must agree to the following,

Declaration of conflicts of interest:

The lead researcher declares that he has no conflicts of interest of any sort in connection with this research. The lead researcher is not aware of any conflicts of interest between any of the research team and this research.

How Participants have been selected to participate in this research:

You have been selected for participation in this research because you use an IoT device and you are accessible to the lead researcher for follow up queries. You have not been selected at random.

The voluntary nature of the participation:

Your participation in this research is voluntary, and without prejudice to your legal and ethical rights. You have the right to withdraw at any time without penalty. You have the right to omit any responses to individual questions without penalty. If you are being

observed, you will be asked for your consent to be observed, and this consent can be withdrawn by you at any time.

Anticipated risks/benefits of participation:

There are no anticipated risks to your participation in this research. However, please be aware that if you make illicit activities known, these will be reported to appropriate authorities.

The provisions for debriefing after participation:

If requested, you will be fully debriefed at the end of your participation in this research. If you so wish, you will also be given a brief explanation of the study.

Dissemination of the Research, and Publications arising from the Research:

Results, data and findings from this research will be published as Cathal Enright's final MSc thesis. Additionally, results, data and findings from this research may be published in one or more peer-reviewed journals, conference proceedings, and a variety of other research publications and conferences. The results of this research will also be disseminated through a number of national and international networks. Primarily, Trinity College Dublin will be responsible for sharing research findings through their government and academic partnerships both in Ireland and abroad.

Research outcomes will be shared directly with Trinity College. The findings from this study may be used to better design IoT systems, including making improvements to security and privacy functionalities.

By participating in this research, you agree that this data may be used for such scientific purposes, and that you have no objection that the data is published in research and scientific publications in a way that does not reveal your specific identity.

At all times your data will be treated with full confidentiality. There will be preservation of participant and third-party anonymity in analysis, publication and presentation of resulting data and findings. Any results, data and findings will be fully anonymous and no personal details about you will be revealed or identified as yours. If you name any third parties, these will be anonymized.

There will be provision for verifying direct quotations and their contextual appropriateness. If any direct quote from you is to be used, you will be contacted in advance and asked to give permission for the use of the quote. You will also be asked if the use of the quote is contextually appropriate and otherwise accurate. If you decline to give permission, the quote will not be used.

The principle investigator must, at all times, act in accordance with all information provided in this and other documents.

Ethical Approval:

The lead researcher has obtained ethical approval for this research from the School of Computer Science and Statistics, Trinity College Dublin.

Appendix 3 – Participant Consent Form

TRINITY COLLEGE DUBLIN

School of Computer Science and Statistics

INFORMED CONSENT FORM

Research Title:

The Internet of Things - A Study of User Security and Privacy

Lead Researcher:

Cathal Enright - Trinity College Dublin, School of Computer Science and Statistics

Supervisors:

Patrick Joseph Wall - Trinity College Dublin, School of Computer Science and Statistics

Lead Researcher Contact Details*:*

Name: Cathal Enright

Phone: +353 (0) 86 3662413

Email: caenrigh@tcd.ie

Expected Duration:

The expected duration of this research is from May to August 2016.

This study is conducted in partial fulfillment of Cathal Enright's MSc, to be awarded by the School of Computer Science and Statistics, Trinity College Dublin, Ireland.

Background to the Research:

The Internet of Things (IoT) is the next big revolutionary technological change and many researchers make the claim that it is about to change the way we live our lives. Broadband Internet is become more widely available, the cost of connecting is decreasing, more devices are being created with Wi-Fi capabilities and sensors built into them, technology costs are going down, and the smartphone industry is bigger than ever and rising. All of these things are creating a huge interest in IoT.

IoT is the concept of connecting any device to the Internet (and/or to each other). Examples include health wearables, the Apple watch, smart TVs, smart fridges and self-driving vehicles etc. This will bring with it a very complex set of security and privacy issues, for the companies who build the products and the users of the IoT devices.

This research proposes to examine user's perceptions of security and privacy issues while using IoT smart devices. The research also aims to find if consumers are concerned about their private data being stored and shared on IoT devices. The aim is to provide an overview of users perceptions and concerns. The research may also suggest ways in which users can mitigate their security and privacy concerns.

Procedures to this Research:

As outlined in the previous section, this research will attempt to reveal security and privacy concerns that explain how the users feel towards IoT devices.

These research objectives will be achieved using a variety of research methods including semi-structured interview of a variety of participants. As a researcher and an avid user of IoT technologies I would like to invite you to participate in this study. Should you agree to participate, your involvement would consist of a 30-60 minute interview with the lead researcher. The topics covered in the interview will include, but are not limited to, your understanding of IoT, a description of your IoT devices, a description of how you interact with these devices, what information you share on your IoT devices, what concerns you have while using such devices, do you have any security or privacy concerns while

using technology in general, any security or privacy problems you encountered while using an IoT device and your overall opinions about IoT.

In some cases, I may ask that you participate in a short follow up interview. This will only occur where there is a need to confirm prior findings and/or identify any changes that may have taken place since the initial interview. If I ask that you be re-interviewed, the same interview guide and Participant Information Sheet will apply.

All interviews will be recorded electronically.

Interviews will be electronically recorded. Participants will be informed of this prior to the commencement of the interview and will be given the opportunity to withdraw from the interview process if they would prefer not to be recorded. Participants will also have an opportunity to review all recordings after the completion of the interview process and make any changes and/or corrections they deem necessary. All interview recordings will be encrypted and only the lead researcher and the research supervisor will have access to these recordings. Any recording made will not be replayed in any public forum or presentation of the research. You may stop electronic recording at any time, and you may at any time, even subsequent to your participation in this research, have such audio and/or video recordings destroyed. At no time will any electronic recording be identifiable unless you give prior written permission. The recordings will be taken on a voice recorder application on the researcher's android smartphone. The recordings will be taken as .mp3 files. The recordings will be transferred to the researcher’s laptop for transcribing purposes and deleted from researcher’s smartphone immediately after transfer. The recordings will be kept on the researcher's laptop encrypted until September 30th 2016.

There are no anticipated risks to your participation in this research. However, please be aware that if you make illicit activities known, these will be reported to appropriate authorities.

Publications from this Research:

Results, data and findings from this research will be published as Cathal Enright’s final MSc thesis. Additionally, results, data and findings from this research may be

published in one or more peer-reviewed journals, conference proceedings, and a variety of other research publications and conferences. The results of this research will also be disseminated through a number of national and international networks. Primarily, Trinity College Dublin will be responsible for sharing research findings through their government and academic partnerships both in Ireland and abroad.

Research outcomes will be shared directly with Trinity College. The findings from this study may be used to better design IoT systems, including making improvements to security and privacy functionalities.

By participating in this research, you agree that this data may be used for such scientific purposes, and that you have no objection that the data is published in research and scientific publications in a way that does not reveal your specific identity.

Declaration:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunities to ask questions and all of my questions have been answered to my satisfaction and I understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in research and scientific publications in a way that does not reveal my specific identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation, have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the lead researcher, supervisors, and research team.
- I freely and voluntarily agree to be part of this research study, through without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any questions and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
  I have received a copy of this agreement.

PARTICIPANTS NAME:

_____

PARTICIPANT'S SIGNATURE:

_____

Date: _____/_____/_____

Statement of Lead Researcher's Responsibility:

I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

Lead Researcher Contact Details*:*

Cathal Enright
Phone: +353 (0) 86 3662413
Email: caenrigh@tcd.ie

LEAD RESEARCHER'S SIGNATURE:

_____

DATE: _____/_____/_____

Appendix 4 – Interview Questions

1. Have you heard about, and do you understand what the Internet of Things (IoT) is?
2. Do you use any IoT/smart devices (i.e smartphones, smartwatch, self-automating cars, health wearable etc.)?
3. Does privacy or security matter to you, in relation to your personal information?
4. Does privacy or security matter to you, when using devices that connect to the internet?
5. What personal information do you think is stored on your smart devices?
6. Are you concerned about where your personal data is being held and stored?
6a. Do you have any concerns in relation to security and privacy on your smart devices?
7. What IoT devices do you plan to use/buy in future?
8. How much control do you believe you have over your personal information stored on your smart devices?
9. Which devices are you most concerned about being connected to the Internet?
10. Do you have any apprehensions about your IoT devices connecting to each other automatically, without your interaction?
11. Who has access to your IoT devices?
12. Do you encrypt any of your devices?
13. Do you use a different password on each of your IoT devices?
14. What devices do you own that connect to the internet? Do you ever leave your devices on charge and walk away?
15. Do you install manufacturers security updates on your IoT devices?
16. Are you aware that some happy of your IoT devices to have full administration rights over your social media pages and messages?
17. Do you think that companies are using your data from these connected devices securely?
18. Do you have different concerns for different types of personal data?
19. Does your IoT device(s) have a privacy policy displayed when first turned on that you must agree to?
20. Do you think about where IoT companies stores their data on you?
21. How do you think companies use your data?

22. Do you think companies should be more transparent with how they use your data? Why?
23. Has this interview changed or made you think more about privacy and security and IoT?

Bibliography

.

Abie, H. and I. Balasingham (2012). Risk-based adaptive security for smart IoT in eHealth. Proceedings of the 7th International Conference on Body Area Networks, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Abowd, G. D., et al. (1999). Towards a better understanding of context and context-awareness. Handheld and ubiquitous computing, Springer.

Adams, A. (1999). Users' perception of privacy in multimedia communication. CHI'99 Extended Abstracts on Human Factors in Computing Systems, ACM.

Airehrour, D., et al. (2016). "Secure routing for internet of things: A survey." Journal of Network and Computer Applications.

Akyildiz, I. F., et al. (2002). "Wireless sensor networks: a survey." Computer networks **38**(4): 393-422.

Akyildiz, I. F. and M. C. Vuran (2010). Wireless sensor networks, John Wiley & Sons.

Al Zefeiti, S. M. B. and N. A. Mohamad (2015). "Methodological Considerations in Studying Transformational Leadership and its Outcomes." International Journal of Engineering Business Management **7**.

Allan, A. (2004). "Passwords are near the breaking point." Gartner Research Note **12**.

Altman, I. (1975). "The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding."

Anderson, C. L. and R. Agarwal (2010). "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions." MIS Quarterly **34**(3): 613-643.

Arcury, T. A. and S. A. Quandt (1998). "Qualitative methods in arthritis research: sampling and data analysis." Arthritis & Rheumatism **11**(1): 66-74.

Armin, J., et al. (2015). 2020 Cybercrime Economic Costs: No measure No solution. Availability, Reliability and Security (ARES), 2015 10th International Conference on, IEEE.

Ashton, K. (2009). "That 'internet of things' thing." RFiD Journal **22**(7): 97-114.

Atzori, L., et al. (2010). "The internet of things: A survey." Computer networks **54**(15): 2787-2805.

Awad, N. F. and M. S. Krishnan (2006). "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization." MIS Quarterly: 13-28.

Baetens, J. (2010). "Delete: The Virtue of Forgetting in the Digital Age by Viktor Mayer-Schönberger. Princeton University Press, Princeton, NJ, USA, 2009. 256 pp. Trade, e-book. ISBN: 978-1-4008-3128-9." Leonardo **43**(5): 509-510.

Bandura, A. (1977). "Self-efficacy: toward a unifying theory of behavioral change." Psychological review **84**(2): 191.

Bandyopadhyay, D. and J. Sen (2011). "Internet of things: Applications and challenges in technology and standardization." Wireless Personal Communications **58**(1): 49-69.

Barcena, M. (2015). "Insecurity of the Internet of Things." from https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf.

Barcena, M. B., et al. (2014). "How safe is your quantified self." Symantech: Mountain View, CA, USA.

Barnickel, J., et al. (2010). Security and privacy for mobile electronic health monitoring and recording systems. World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium on a, IEEE.

Bassi, A. and G. Horn (2008). "Internet of Things in 2020: A Roadmap for the Future." European Commission: Information Society and Media.

Bélanger, F. and R. E. Crossler (2011). "Privacy in the digital age: a review of information privacy research in information systems." MIS Quarterly **35**(4): 1017-1042.

Black, I. (2006). "The presentation of interpretivist research." Qualitative Market Research: An International Journal **9**(4): 319-324.

Blaikie, N. (2009). "Designing social research."

Boer, H. and E. R. Seydel (1996). "Protection motivation theory."

Borgohain, T., et al. (2015). "Survey of Security and Privacy Issues of Internet of Things." arXiv preprint arXiv:1501.02211.

Brannen, J. (1992). "Combining qualitative and quantitative approaches: an overview." Mixing methods: Qualitative and quantitative research: 3-37.

Britz, J. (2010). Technology as a threat to privacy: ethical challenges to the information profession.

Brock, D. L. (2001). "The electronic product code (epc)." Auto-ID Center White Paper MIT-AUTOID-WH-002.

Brophy, C. (2016). "The IOActive IoT Security Survey." Retrieved June, 2016, from http://www.ioactive.com/news-events/iot-products-have-inadequate-security-according-to-practitioner-survey.html#_ednref1.

Brown, R. B. (2006). Doing your dissertation in business and management: the reality of researching and writing, Sage.

Bryman, A. (1992). "Quantitative and qualitative research: further reflections on their integration." Mixing methods: Qualitative and quantitative research: 57-78.

Bryman, A. (2003). Quantity and quality in social research, Routledge.

Bryman, A. (2012). Social Reasearch Mehtods, NewYork: Oxford University Press.

C.Tofel, K. (2016) "Got an IP webcam?" GigaOm Research. 2016.

Canada, O. o. t. P. C. o. (2014). "Wearable Computing - Challenges and opportunities for privacy protection."

Canada, O. o. t. P. C. o. (2016). "An introduction to privacy issues with a focus on the retail and home environments."

CASPIAN "Boycott Benetton: No RFID tracking chips in clothing!".

Chattha, N. A. (2014). NFC—Vulnerabilities and defense. Information Assurance and Cyber Security (CIACS), 2014 Conference on, IEEE.

Chen, S., et al. (2014). "A vision of IoT: Applications, challenges, and opportunities with china perspective." Internet of Things Journal, IEEE **1**(4): 349-359.

Child, J. T., et al. (2009). "Blogging, communication, and privacy management: Development of the blogging privacy management measure." Journal of the American Society for Information Science and Technology **60**(10): 2079-2094.

Child, J. T. and S. Petronio (2011). "Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the internet." Computer-mediated communication in personal relationships: 21-40.

Clapper, J. R. (2016). "Worldwide Threat Assessment."

Coetzee, L. and J. Eksteen (2011). The Internet of Things-promise for the future? An introduction. IST-Africa Conference Proceedings, 2011, IEEE.

Copie, A., et al. (2013). From cloud governance to iot governance. Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, IEEE.

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. System Sciences (HICSS), 2010 43rd Hawaii International Conference on, IEEE.

Cuzzocrea, A., et al. (2011). Analytics over large-scale multidimensional data: the big data revolution! Proceedings of the ACM 14th international workshop on Data Warehousing and OLAP, ACM.

Da Xu, L., et al. (2014). "Internet of things in industries: A survey." IEEE Transactions on Industrial Informatics **10**(4): 2233-2243.

Darianian, M. and M. P. Michael (2008). Smart home mobile RFID-based Internet-of-Things systems and services. Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on, IEEE.

Das, M. L. (2015). Privacy and Security Challenges in Internet of Things. Distributed Computing and Internet Technology, Springer**:** 33-48.

De Wolf, R., et al. (2014). "Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook." Computers in Human Behavior **35**: 444-454.

Desai, K. N. (2016). "Internet of Things: Privacy & Security Issues." International Journal for Innovative Research in Science and Technology **3**(2): 227-230.

Dijkman, R., et al. (2015). "Business models for the Internet of Things." International Journal of Information Management **35**(6): 672-678.

Dinev, T. and P. Hart (2004). "Internet privacy concerns and their antecedents-measurement validity and a regression model." Behaviour & Information Technology **23**(6): 413-422.

Dinev, T. and P. Hart (2006). "An extended privacy calculus model for e-commerce transactions." Information systems research **17**(1): 61-80.

Dohr, A., et al. (2010). The internet of things for ambient assisted living. 2010 Seventh International Conference on Information Technology, Ieee.

Easterby-Smith, M., et al. (2012). Management research, Sage.

El Kaliouby, R. (2015). "The mood-aware Internet of things." Blog Entries.

Electronics, G. H. I. (2003). "Bluetooth module."

Evans, D. (2011). "The internet of things." How the Next Evolution of the Internet is Changing Everything, Whitepaper, Cisco Internet Business Solutions Group (IBSG) **1**: 1-12.

Evans, D. (2011). "The internet of things: How the next evolution of the internet is changing everything." CISCO white paper **1**: 1-11.

Finkenzeller, K. (2003). "RFID handbook 2nd Edition."

Fisher, R. and G. Hancke (2014). DTLS for Lightweight Secure Data Streaming in the Internet of Things. P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on, IEEE.

Folk, C. (2015). The security implications of the Internet of Things. AFCEA, AFCEA.

FTC (2015). "Internet of Things: Privacy & Security in a Connected World." FTC Staff Report.

Furnell, S., et al. (2007). "Assessing the security perceptions of personal Internet users." Computers & Security **26**(5): 410-417.

Garrido, P. C., et al. (2010). A model for the development of NFC context-awareness applications on internet of things. Near Field Communication (NFC), 2010 Second International Workshop on, IEEE.

Gathegi, J. and M. Workman (2005). Observance and Contravention of Information Security Measures. Security and Management.

Gefen, D., et al. (2003). "Trust and TAM in online shopping: an integrated model." MIS Quarterly **27**(1): 51-90.

Gerla, M., et al. (2014). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. Internet of Things (WF-IoT), 2014 IEEE World Forum on, IEEE.

Google "Google self-driving car project."

Gordon, L. A. and M. P. Loeb (2002). "The economics of information security investment." ACM Transactions on Information and System Security (TISSEC) **5**(4): 438-457.

Gray, D. E. (2013). Doing research in the real world, Sage.

Gubbi, J., et al. (2013). "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems **29**(7): 1645-1660.

Gudivada, V. N., et al. (2015). "Big Data: Promises and Problems." IEEE Computer **48**(3): 20-23.

Guion, L. A., et al. (2001). "Conducting an In-depth Interview1."

Hager, C. T. and S. F. MidKiff (2003). An analysis of Bluetooth security vulnerabilities. Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE, IEEE.

Hair, J. F., et al. (2011). Essentials of Business Research Methods, M.E. Sharpe, Incorporated.

Harrell, M. C. and M. A. Bradley (2009). Data collection methods. Semi-structured interviews and focus groups, DTIC Document.

Harrington, S. J. (1996). "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions." MIS Quarterly: 257-278.

Hern, A. (2016). Car hacking is the future – and sooner or later you'll be hit. The Guardian, The Guardian.

Hong, J.-y., et al. (2009). "Context-aware systems: A literature review and classification." Expert Systems with Applications **36**(4): 8509-8522.

HP (2015). "Internet of Things research study." 2016, from www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

Hughes, C. (2014). "AN INTRODUCTION TO QUALITATIVE RESEARCH."

Hwang, Y. H. (2015). Iot security & privacy: threats and challenges. Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security, ACM.

Industry, R. Privacy and Data Protection Impact Assessment Framework for RFID Applications, January 2011.

Issarny, V., et al. (2011). "Service-oriented middleware for the future internet: state of the art and research directions." Journal of Internet Services and Applications **2**(1): 23-45.

ITU (2005). "ITU Internet report 2005: the internet of things." International Telecommunication Union.

ITU (2016). "ITU-T in brief."

ITU-T "Study group 20 at a glance."

ITU-T (2015). "Focus group on smart sustainable cities."

Jakobsson, M. and S. Wetzel (2001). Security weaknesses in Bluetooth. Cryptographers' Track at the RSA Conference, Springer.

Janesick, V. J. (2000). "The choreography of qualitative research design." Handbook of Qualitative Research.: 379-399.

Jankowski, S., et al. (2014). "The Internet of Things: Making sense of the next mega-trend." Goldman Sachs.

Jia, X., et al. (2012). RFID technology and its applications in Internet of Things (IoT). Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, IEEE.

Jia, X., et al. (2010). "An efficient anti-collision protocol for RFID tag identification." Communications Letters, IEEE **14**(11): 1014-1016.

Johnson, D. R. and D. Post (1996). "Law and borders: The rise of law in cyberspace." Stanford Law Review: 1367-1402.

Johnston, A. C. and M. Warkentin (2010). "Fear appeals and information security behaviors: an empirical study." MIS Quarterly: 549-566.

Jonassen, D. H. (1991). "Objectivism versus constructivism: Do we need a new philosophical paradigm?" Educational technology research and development **39**(3): 5-14.

Juels, A. (2006). "RFID security and privacy: A research survey." Selected Areas in Communications, IEEE Journal on **24**(2): 381-394.

Kaplan, B. and J. A. Maxwell (2005). Qualitative research methods for evaluating computer information systems. Evaluating the organizational impact of healthcare information systems, Springer**:** 30-55.

Karabacak, B. and I. Sogukpinar (2005). "ISRAM: information security risk analysis method." Computers & Security **24**(2): 147-159.

Kavitha, T. and D. Sridharan (2010). "Security vulnerabilities in wireless sensor networks: A survey." Journal of information Assurance and Security **5**(1): 31-44.

Kef, B. (2015). "NFC chips."

Khan, R., et al. (2012). Future internet: the internet of things architecture, possible applications and key challenges. Frontiers of Information Technology (FIT), 2012 10th International Conference on, IEEE.

Klenke, K. (2008). "Qualitative research in the study of leadership."

Korhonen, I., et al. (2003). "Health monitoring in the home of the future." Engineering in Medicine and Biology Magazine, IEEE **22**(3): 66-73.

Kuo, F.-Y. and M.-H. Hsu (2001). "Development and validation of ethical computer self-efficacy measure: The case of softlifting." Journal of Business Ethics **32**(4): 299-315.

Laplante, P. A. and N. Laplante (2016). "The Internet of Things in Healthcare: Potential Applications and Challenges." IT Professional **18**(3): 2-4.

Lee, D. (2016). Google car crash 'not a surprise' - US transport secretary. BBC Technology, BBC News.

Lee, D., et al. (2008). "Keeping our network safe: a model of online protection behaviour." Behaviour & Information Technology **27**(5): 445-454.

Lee, D.-W. (2016). "A Study on Actual Cases & Meanings for Internet of Things."

Lee, Y. and K. R. Larsen (2009). "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software." European journal of information systems **18**(2): 177-187.

Legard, R., et al. (2003). "In-depth interviews." Qualitative research practice: A guide for social science students and researchers: 138-169.

Leo, M., et al. (2014). A federated architecture approach for Internet of Things security. Euro Med Telco Conference (EMTC), 2014, IEEE.

Lerner, V. S. (2007). "Systems science, information systems theory, and informational macrodynamics: review." Kybernetes **36**(2): 192-224.

Levin, D. M. (1988). "The opening of vision: Nihilism and the postmodern situation."

Li, C., et al. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on, IEEE.

Li, Y. (2012). "Theories in online information privacy research: A critical review and an integrated framework." Decision Support Systems **54**(1): 471-481.

Lin, C.-P. and C. G. Ding (2003). "Modeling information ethics: The joint moderating role of locus of control and job insecurity." Journal of Business Ethics **48**(4): 335-346.

Lin, H. and N. W. Bergmann (2016). "IoT Privacy and Security Challenges for Smart Home Environments." Information **7**(3): 44.

Lioudakis, G. V., et al. (2007). A proxy for privacy: the discreet box. EUROCON, 2007. The International Conference on &# 34; Computer as a Tool&# 34;, IEEE.

Lowry, P. (2015). "Protection motivation theory - IS theory."

MacGillivray, C. T., Vernon (2015). "Worldwide Internet of Things Forecast 2015–2020." from http://www.idc.com/getdoc.jsp?containerId=256397.

Maddux, J. E. and R. W. Rogers (1983). "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change." Journal of experimental social psychology **19**(5): 469-479.

Malhotra, N. K., et al. (2004). "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." Information systems research **15**(4): 336-355.

Margulis, S. T. (2011). Three theories of privacy: An overview. Privacy Online, Springer**:** 9-17.

Marias, G. F., et al. (2012). "Security and privacy issues for the network of the future." Security and Communication Networks **5**(9): 987-1005.

Mayer, C. P. (2009). "Security and privacy challenges in the internet of things." Electronic Communications of the EASST **17**.

McCann, J. and D. Bryson (2009). Smart clothes and wearable technology, Elsevier.

Miessler, D. S., Craig (2014). "Internet of Things Top Ten." OWASP.

Minerva, R. (2015). "Towards a defintion of Internet of Things (IoT)." IEEE Internet Initiative.

Mohamed, N. and I. H. Ahmad (2012). "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia." Computers in Human Behavior **28**(6): 2366-2375.

Morgan, D. L. (2007). "Paradigms lost and pragmatism regained methodological implications of combining qualitative and quantitative methods." Journal of mixed methods research **1**(1): 48-76.

Mulani, T. T. and S. V. Pingle (2016). "Internet of Things." International Research Journal of Multidisciplinary Studies **2**(3).

Ncta (2014). "Infographic: The growth of the Internet of things."

Ng, B.-Y., et al. (2009). "Studying users' computer security behavior: A health belief perspective." Decision Support Systems **46**(4): 815-825.

Ogden, J. (2014). "How RFID chips have sped up production and lowered costs."

Opdenakker, R. (2006). Advantages and disadvantages of four interview techniques in qualitative research. Forum Qualitative Sozialforschung/Forum: Qualitative Social Research.

Orlikowski, W. J. and D. C. Gash (1994). "Technological frames: making sense of information technology in organizations." ACM Transactions on Information Systems (TOIS) **12**(2): 174-207.

OWASP, O. W. A. S. P. (2016). "Internet of Things Top Ten." 2016, from https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

Pahnila, S., et al. (2007). Employees' behavior towards IS security policy compliance. System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on, IEEE.

Pantelopoulos, A. and N. G. Bourbakis (2010). "A survey on wearable sensor-based systems for health monitoring and prognosis." Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on **40**(1): 1-12.

Patton, M. Q. (2005). Qualitative research, Wiley Online Library.

Perera, C., et al. (2014). "Context aware computing for the internet of things: A survey." Communications Surveys & Tutorials, IEEE **16**(1): 414-454.

Peterson, R. (2004). "Crafting information technology governance." Information Systems Management **21**(4): 7-22.

Petronio, S. (1991). "Communication boundary management: A theoretical model of managing disclosure of private information between marital couples." Communication Theory **1**(4): 311-335.

Petronio, S. (2008). Communication privacy management theory, Wiley Online Library.

Petronio, S. (2013). "Brief status report on communication privacy management theory." Journal of Family Communication **13**(1): 6-14.

Petronio, S. and I. Altman (2002). "Boundaries of privacy."

Petronio, S., et al. (2008). Engaging theories in interpersonal communication: Multiple perspectives, Sage Thousand Oaks, CA.

Phelps, J., et al. (2000). "Privacy concerns and consumer willingness to provide personal information." Journal of Public Policy & Marketing **19**(1): 27-41.

Ponemon, L. (2015). "Cost of data breach study: Global Analysis." Poneomon Institute sponsored by IBM.

Power, D. J. (2016). "“Big Brother” can watch us." Journal of Decision Systems **25**(sup1): 578-588.

Quinlan, C., et al. (2011). Business research methods, South-Western Cengage Learning Andover.

Rahman, M., et al. (2016) "Secure Management of Low Power Fitness Trackers."

Rajkumar, R. R., et al. (2010). Cyber-physical systems: the next computing revolution. Proceedings of the 47th Design Automation Conference, ACM.

Remenyi, D. and B. Williams (1995). "Some aspects of methodology for research in information systems." Journal of Information Technology **10**(3): 191-201.

Remenyi, D. and B. Williams (1998). Doing research in business and management: an introduction to process and method, Sage.

Revell, S. (2013) Internet of Things (IoT) and machine to machine communications (M2M) challenges and oppurtunities. **Final Paper**,

Ritchie, J., et al. (2013). Qualitative research practice: A guide for social science students and researchers, Sage.

Rogers, R. W. (1975). "A protection motivation theory of fear appeals and attitude change1." The journal of psychology **91**(1): 93-114.

Rogers, R. W. and S. Prentice-Dunn (1997). "Protection motivation theory."

Roman, R., et al. (2011). "Securing the internet of things." Computer **44**(9): 51-58.

Roman, R., et al. (2013). "On the features and challenges of security and privacy in distributed internet of things." Computer networks **57**(10): 2266-2279.

Rose, K., et al. (2015). "The Internet of Things (IoT): An Overview–Understanding the Issues and Challenges of a More Connected World." Internet Society.

Ryan, P. and A.-M. Glynn (2014). The Internet of Things -Article 29 Working Party Issues Opinion.

Sandra, L. (2012). "Anonymous cyber-attacks cost."

Sattarova Feruza, Y. and T.-h. Kim "IT security review: Privacy, protection, access control, assurance and system security."

Saunders, M., et al. (2009). Research Methods for Business Students, Financial Times Prentice Hall.

Saunders, M. N. (2011). Research methods for business students, 5/e, Pearson Education India.

Schaffers, H., et al. (2011). "Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation." Future internet assembly **6656**(31): 431-446.

Schatz, D. and R. Bashroush (2016). "The impact of repeated data breach events on organisations' market value." Information and Computer Security **24**(1): 73-92.

Shi, E. and A. Perrig (2004). "Designing secure sensor networks." IEEE Wireless Communications **11**(6): 38-43.

Sicari, S., et al. (2015). "Security, privacy and trust in Internet of Things: The road ahead." Computer networks **76**: 146-164.

Singh, D., et al. (2014). A survey of internet-of-things: future vision, architecture, challenges and services. Internet of Things (WF-IoT), 2014 IEEE World Forum on, IEEE.

Siponen, M. (2001). "Five dimensions of information security awareness." Computers and Society **31**(2): 24-29.

Skarmeta, A. and M. V. Moreno (2013). "Internet of things." Secure Data Management: 48-53.

Smith, H. J., et al. (1996). "Information privacy: measuring individuals' concerns about organizational practices." MIS Quarterly: 167-196.

Soh, P. J., et al. (2015). "Wearable Wireless Health Monitoring: Current Developments, Challenges, and Future Trends." Microwave Magazine, IEEE **16**(4): 55-70.

Spanos, G. and L. Angelis (2016). "The impact of information security events to the stock market: A systematic literature review." Computers & Security **58**: 216-229.

Srinivasan, V., et al. (2008). Protecting your daily in-home activity information from a wireless snooping attack. Proceedings of the 10th international conference on Ubiquitous computing, ACM.

Sundmaeker, H., et al. (2010). "Vision and Challenges for Realising the Internet of Things, CERP-IoT cluster." Information Society and Media, Directoriate General, European Commission, Brussels.

Swan, M. (2012). "Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0." Journal of Sensor and Actuator Networks **1**(3): 217-253.

Tan, L. and N. Wang (2010). Future internet: The internet of things. Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, IEEE.

Tangient, L. L. C. "Wi-Fi Chips."

Team, V. (2016). "2016 Data Breach Investigations Report."

Thielman, S. (2016). Fatal crash prompts federal investigation of Tesla self-driving cars. The Guardian, The Guardian.

Thierer, A. D. (2015). "The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation." Adam Thierer, The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation **21**.

Uckelmann, D., et al. (2011). An architectural approach towards the future internet of things. Architecting the internet of things, Springer**:** 1-24.

Union, E. (2010). Charter of Fundamental Rights of the European Union. Brussels, European Union.

van der Meulen, R. (2015). "Gartner Press Release." from http://www.gartner.com/newsroom/id/3165317.

Van der Meulen, R. (2016). "Gartner Identifies Top 10 IoT Technologies for 2017 and 2018." Gartner. from http://www.gartner.com/newsroom/id/3221818.

Vance, A., et al. (2012). "Motivating IS security compliance: insights from habit and protection motivation theory." Information & Management **49**(3): 190-198.

Walliman, N. (2011). Your research project: Designing and planning your work, Sage Publications.

Walsham, G. (1993). Interpreting information systems in organizations, John Wiley & Sons, Inc.

Walsham, G. (2006). "Doing interpretive research." European journal of information systems **15**(3): 320-330.

Wang, Y., et al. (2006). "A survey of security issues in wireless sensor networks."

Want, R., et al. (2015). "Enabling the Internet of Things." IEEE Computer **48**(1): 28-35.

Weber, R. (2004). "Editor's comments: the rhetoric of positivism versus interpretivism: a personal view." MIS Quarterly: iii-xii.

Weber, R. H. (2009). "Internet of things–Need for a new legal environment?" Computer Law & Security Review **25**(6): 522-527.

Weber, R. H. (2010). "Internet of Things–New security and privacy challenges." Computer Law & Security Review **26**(1): 23-30.

Weber, R. H. (2010). Shaping internet governance: Regulatory challenges, Springer Science & Business Media.

Weber, R. H. (2011). "Accountability in the Internet of Things." Computer Law & Security Review **27**(2): 133-138.

Weber, R. H. (2015). "Internet of things: Privacy issues revisited." Computer Law & Security Review **31**(5): 618-627.

Weber, R. H. (2016). "Governance of the Internet of Things—From Infancy to First Attempts of Implementation?" Laws **5**(3): 28.

Weber, R. H. (2010). Internet of Things, Springer.

Weiser, M. (1991). "The computer for the 21st century." Scientific american **265**(3): 94-104.

Wengraf, T. (2001). Qualitative research interviewing: Biographic narrative and semi-structured methods, Sage.

West, R. and L. H. Turner (2010). Understanding interpersonal communication: Making choices in changing times, Cengage Learning.

Westhues, J. (2005). "Hacking the prox card." RFID: Applications, Security, and Privacy: 291-300.

Westin, A. F. (1968). "Privacy and freedom." Washington and Lee Law Review **25**(1): 166.

Whitmore, A., et al. (2015). "The Internet of Things—A survey of topics and trends." Information Systems Frontiers **17**(2): 261-274.

Wilson, J. (2014). Essentials of business research: A guide to doing your research project, Sage.

Wong, F.-L. and F. Stajano (2005). Location privacy in bluetooth. European Workshop on Security in Ad-hoc and Sensor Networks, Springer.

Woods, V. (2016). "Gartner Press Release." from http://www.gartner.com/newsroom/id/3185623.

Woon, I., et al. (2005). "A protection motivation theory approach to home wireless security." ICIS 2005 proceedings: 31.

WP29 (2014). ARTICLE 29 DATA PROTECTION WORKING PARTY opinion 8/2014 on the on recent developments on the Internet of things.

Wu, Y., et al. (2005). "Protection motivation theory and adolescent drug trafficking: relationship between health motivation and longitudinal risk involvement." Journal of pediatric psychology **30**(2): 127-137.

Xia, F., et al. (2012). "Internet of things." International Journal of Communication Systems **25**(9): 1101.

Xu, H., et al. (2011). "Information privacy concerns: Linking individual perceptions with institutional privacy assurances." Journal of the Association for Information Systems **12**(12): 798.

Xu, T., et al. (2014). Security of IoT systems: Design challenges and opportunities. Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, IEEE Press.

Yan, L., et al. (2008). "The Internet of things: from RFID to the next-generation pervasive networked systems."

Yeong, A. (2011). "Introduction To Business Research Methods."

Youn, S. (2005). "Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach." Journal of Broadcasting & Electronic Media **49**(1): 86-110.

Zhao, K. and L. Ge (2013). A survey on the internet of things security. Computational Intelligence and Security (CIS), 2013 9th International Conference on, IEEE.

Zheng, L., et al. (2011). "Technologies, applications, and governance in the internet of things." Internet of things-Global technological and societal trends. From smart environments and spaces to green ICT.