University of Wollongong
Research Online

Faculty of Informatics - Honours Theses (Archive)

University of Wollongong Thesis Collections

2005

RFID Privacy and Security: A Content Analysis

K. Johnston
University of Wollongong

Publication Details

This thesis was originally submitted as Johnston, K, RFID Privacy and Security: A Content Analysis, Bachelor of Information and Communication Technology (Honours), University of Wollongong, 2005,101p.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

RFID Privacy and Security: A Content Analysis

Abstract
Radio Frequency Identification (RFID) is a technology that is becoming readily available. It is currently used to identify cats and dogs, as well as tracking inanimate objects throughout the world by using the Electronic Product Code (EPC) standard. Trials are currently underway that involve the implantation of RFID transponders in humans in various parts of the world. This paper discusses the possible concerns with wide spread use of RFID, on both inanimate and living things. It will identify and discuss several socio-technical aspects of RFID, including privacy and security.

Publication Details
This thesis was originally submitted as Johnston, K, RFID Privacy and Security: A Content Analysis, Bachelor of Information and Communication Technology (Honours), University of Wollongong, 2005,101p.

This thesis is available at Research Online: http://ro.uow.edu.au/thesesinfo/6

Kirsty Johnston

2437843

IACT450

Honours Thesis

Topic: RFID Privacy and Security:

A Content Analysis

Supervisor: Katina Michael

Table of Contents

Table of Contents ii
List of Figures iv
List of Tables iv
Acknowledgements v

1. Introduction 1
   1.1. Introduction 1
   1.2. Background 1
      1.2.1 Definitions 1
      1.2.2 Recent Developments in RFID 2
      1.2.3 RFID System 3
      1.2.4 Implementations of RFID 5
   1.3. Research Objectives 6
   1.4. Methodology 7
      1.4.1 Content Analysis 7
      1.4.2 Online Surveys 8
   1.5. Justification 9
   1.6. Limitations 9
2. Literature Review 11
   2.1 Introduction 11
   2.2 Privacy 11
      2.2.1 Education 11
      2.2.2 Informing Consumers of the Presence of RFID Tags 13
      2.2.3 Preventative Reading Methods 14
   2.3 Security 18
      2.3.1 Surveillance 18
      2.3.2 Theft Prevention 19
      2.3.3 Supply Chain Management 20
   2.4 Gap 21
   2.5 Conclusion 23
3. Methodology 24
   3.1 Introduction 24
   3.2 Content Analysis 25
      3.2.1 Introduction 25
      3.2.2 Advantages and Disadvantages of Computer-Aided Content Analysis 26
      3.2.3 Leximancer 27
   3.3 Online Survey 29
      3.3.1 Introduction 29
      3.3.2 Advantages and Disadvantages of Online Surveys 30
      3.3.3 Content 30
   3.4 Unit of Analysis/Time Horizon 32
   3.5 Conclusion 32
4. Exploration of the Themes and Concepts of RFID Privacy and Security 34

4.1 Introduction 34
4.2 Leximancer Map Analysis 35
4.2.1 Privacy 35
4.2.2 Reader 38
4.2.3 Technology 39
4.2.4 Information 41
4.2.5 Authentication 43
4.3 Frequency and Relationship Matrices 45
4.4 Narrative Analysis 48
4.5 Development of Survey Questions 50
4.6 Conclusion 51
5. Analysis of Society's Opinion 53
5.1 Introduction 53
5.2 General Background of Participants 53
5.3 Analysis of Results 54
5.3.1 Implementation of RFID in Humans 54
5.3.2 Possible uses of RFID Transponders 55
5.3.3 The Level of Concern over the uses of RFID 56
5.3.4 The Level of Concern over the Wide Scale Implementation 57
5.3.5 Approval of RFID Tag Data 58
5.4 Discussion 60
5.5 Conclusion 62
6. Conclusion 63
6.1 Introduction 63
6.2 Principal Conclusions and Implications 63
6.3 Future Research 65
6.4 Conclusion 66
7. Reference List 67
8. Appendices 70
8.1 Appendix 1 – Content Analysis Article List 70
8.2 Appendix 2 – Ranked Concept List 76
8.3 Appendix 3 – Highlighted Relationship Matrix 80
8.4 Appendix 4 – Survey Questions 81
8.5 Appendix 5 – Ethics Approval Form 101

List of Figures

Figure 1 Research Diagram 25
Figure 2 Phases of Processing in Leximancer from Leximancer v 2.16 (The Program).....28
Figure 3 An example map of "The U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq" from Leximancer.com 28
Figure 4 - Leximancer Map - Major Themes.....35
Figure 5 - Leximancer Maps - Privacy 36
Figure 6 - Leximancer Map - Reader.....38
Figure 7 - Leximancer Map - Technology.....40
Figure 8 - Leximancer Maps - Information 42
Figure 9 - Leximancer Maps - Authentication.....44
Figure 10 - Age Distribution Graph.....54
Figure 11 - Results for Auto-Identification of a Human.....55
Figure 12 - Response for Level of Concern over Tracking Crime Suspects 56
Figure 13 - Response over Government Body Collecting Personal Information 57
Figure 14 - Government and Commercial Comparison (Pre-Test Data).....58
Figure 15 - Data that has been accepted to be stored on a RFID tag.....59
Figure 16 - Data that has not been accepted to be stored on a RFID tag.....60

List of Tables

Table 1 - Concepts Linked to Privacy.....37
Table 2 - Concepts Linked to Reader 39
Table 3 - Concepts Linked to Technology.....41
Table 4 - Concepts Linked to Information.....43
Table 5 - Concepts Linked to Authentication.....45
Table 6 - Frequency Matrix 46
Table 7 - Relationship Matrix.....47
Table 8 - Coloured Highlighted Matrix 80

Acknowledgements

There are many people whom I must thank, because without them this thesis would not be possible. Firstly, I must thank my family for putting up with my mood swings and late night writing sessions. I would particularly like to thank my mum, Christine Johnston, who helped by continuously proof reading several of my drafts. I would also like to thank my friends who helped by completing my survey and asking others to do it too, without them Chapter 5 would be lacking much content.

I need to thank my boyfriend, Joel Roland, who has supported me through this time. He continually reminds me that life is bigger than just this thesis, and without him I do not think I would have any hair left on my head!

Last, but far from least, my supervisor and someone whom I now call a friend, Dr Katina Michael. She has spent countless hours helping me through this process. I have never left her office having not learnt something, or spending the next hour just absorbing the wisdom that she has passed on to me. To her I owe my greatest thanks and gratitude.

1. Introduction

1.1. Introduction

Radio Frequency Identification (RFID) is a technology that is becoming readily available. It is currently used to identify cats and dogs, as well as tracking inanimate objects throughout the world by using the Electronic Product Code (EPC) standard. Trials are currently underway that involve the implantation of RFID transponders in humans in various parts of the world. This paper discusses the possible concerns with wide spread use of RFID, on both inanimate and living things. It will identify and discuss several socio-technical aspects of RFID, including privacy and security.

1.2. Background

1.2.1 Definitions

Throughout the literature there are many definitions of RFID tags. Most of these are very similar. A definition is given by Juels, Rivest & Szydlo (2003).

> *"An RFID (Radio-Frequency IDentification) tag consists of a small integrated circuit attached to a small antennae, capable of transmitting a unique serial number a distance of several meters to a reading device in response to a query"* (Juels, Rivest & Szydlo 2003, p. 103).

Another attribute of RFID tags is that they has the ability to be "automatically identified at a distance without a direct line-of-sight using an electromagnetic challenge/response exchange" (Want 2004, p. 41). Ni et al. (2004, p. 702) give a slightly more technical definition which includes the "means of storing and retrieving data through electromagnetic transmission to an RF compatible circuit". For the ease of this paper, and its readers, this paper will use the first definition given, as it presents a close representation to the majority of definitions written (Juels, Rivest & Szydlo 2003; Michael 2003; Molnar & Wagner 2004).

1.2.2 Recent Developments in RFID

Sanjay Sarma co-founded the Auto-ID Centre at MIT in the late 1990's, to promote and develop RFID transponders. In the article "Integrating RFID", Sarma (2004) discusses the Auto-ID Centre focusing on two main concepts in order to make RFID more readily available on a wider scale. The first was to reduce the chip size needed, which was done by the removal of complexity in the chip, including eliminating "encryption from the simplest transponders because there was no memory to protect" (Sarma 2004, p. 1). The second part of the research was to develop a strategy which will

> *"…[p]ut much of the data and intelligence associated with tagged items, which had hitherto resided on the RFID transponders themselves, on the network instead."* (Sarma 2004, p. 2)

The Auto-ID Center achieved this by a new numbering scheme called the EPC (Electronic Product Code).

1.2.3 RFID System

Many authors have described how the RFID system can be broken down into different sections.

> *"An RFID system is composed of readers and tags. Readers generate signals that are dual purpose: they provide power for a tag, and they create an interrogation signal. A tag captures the energy it receives from a reader to supply its own power and then executes commands sent by the reader"* (Want 2004, p. 42).

The literature predominately describes two different elements of the RFID system, the reader and the tag (Juels, Rivest & Szydlo 2003; Molnar & Wagner 2004; Ni et al. 2004; Sarma 2004). Michael (2004, p. 474) discusses other parts of the RFID system which include the antennae and a computer, of which the role is to interpret all the information collected. Even though these two parts are not RFID specific technologies, it is important to note their existence in the system.

The role of the reader is to collect the relevant information that needs to be processed. The article "The Magic of RFID" by Want (2004) discusses the technical aspect of the reader. This detail is too in-depth for the purposes of this paper, and therefore it will not be discussed further. There are factors with the use of RFID that could cause problems for RFID readers. One of problems is that

> *"A RFID reader is really only able to communicate with one tag at a time. If more than one tag responds to a query by the reader … the reader detects a 'collision'. In this case, it doesn't read accurately any of the information transmitted by the tags"* (Juels, Rivest & Szydlo 2003, p. 106).

Sarma (2004, p. 3) mentions "location tolerance", a system that allows items that are not in line of sight to be read. However, this is a problem in itself, as readers are unable to determine "whether a tag is in fact in the reader's prescribed zone, or whether the read tag is simply passing by" (Sarma 2004, p. 3).

There are several physical aspects of RFID tags to be noted. It has been described as a device which is "smaller than a grain of rice" (Michael & Masters 2004, p. 505). There are two different types of tags that exist, passive and active. Passive tags are more common than active tags, as they do not require a battery as the tag receives the power that it needs from the signal itself (Juels, Rivest & Szydlo 2003; Want 2004). Active tags can power themselves from a button-cell battery included in the tag, along with the radio transceiver (Ni et al. 2004, p. 702).

There is current discussion about what information will be held on the tag. Some recommend that actual data (name, age, height etc) is stored. Others suggest that it will just hold a serial number, known as its Electronic Product Code (EPC), and managed by EPCGlobal (Juels, Rivest & Szydlo 2003, p. 103).

> *"The ID number, as envisioned by the AutoID Center is unique to a given tag. It contains not only the traditional information contained in a printed barcode (indicating manufacture and product type), but also a unique serial number for that tag"* (Juels, Rivest & Szydlo 2003, p. 103).

Sanjay Sarma (as mentioned in section 1.2.2) co-founded the AutoID Center that Juels et al (2003) has mentioned. Juels et al (2003) describes the EPC (Electronic Product Code) to be used similar to the way a license plate is used to identify a car. In order to effectively implement EPCGlobal other infrastructure components will be needed, which include the EPCIS (EPC Information Service). EPCGlobal is now trying to promote and implement the EPC system in the commercial sector (Sarma 2004, p. 7).

1.2.4 Implementations of RFID

RFID started many years ago in the 1940s when the United States of America used the technology to help identify friendly aircraft.

> *"It was not until the late 1980s however, when the Dutch government voiced their requirement for a livestock tracking system that the commercial direction of RF/ID changed"* (Michael 2003, p. 143).

The realisation that this technology could be used for a commercial application is what started the chain reaction that leads to the use of RFID today and not because it is a new technology. There are several services that RFID can offer including assisting in an emergency.

> *" An individual could be identified by the RFID implant, giving emergency services access to the implantee's medical data and history that could be potentially life-saving"* (Michael 2004, p. 471).

Other services that could be offered with the use of RFID in mobile commerce when integrated with e-security, e-banking and e-health, include a lifetime identifier, banking, biosensors, law enforcement, crime prevention, the monitoring of employees, and as an alternative to military dog tags (Michael & Masters 2004, p. 505). Modern courier companies use this technology to monitor where packages are at any give time through a location-based service. A more recent and real life example was indicated

> *"…[l]ast October when the U.S. government announced its military branches would demand their suppliers use active and passive RFID tags in all equipment shipped to the military by January 2005."* (McGinity 2004, p. 16)

There are almost endless scenarios for the use of RFID, and while this technology continues to be developed and implemented, society and industry will continue to come up with new ideas for RFID.

1.3. Research Objectives

The following objectives were produced from the gap that has become evident from the literature review. More information can be found about this in the literature review (Chapter 2), and in particular Section 2.4, which identifies the gap.

1. To identify existing work regarding RFID transponders throughout the literature in order to create a succinct list of previously identified concerns, and to evaluate the extent to which these known issues arise in the literature.

2. To critically analyse these results through frequency and relationship matrices as well as conducting a narrative analysis.

3. To determine the level of awareness and asses the level of concern over the results, in order to gauge the level of education of RFID transponders in society.

1.4. Methodology

The research methodology used in this research paper will be twofold. Firstly, content analysis will be conducted, in order to extract and highlight the issues that are currently being raised through the literature in relation to RFID transponders. Secondly, an online survey will be created to obtain an indication of society's reaction to the issues obtained from the content analysis.

1.4.1 Content Analysis

In this research paper, content analysis will be used to extract and highlight the issues that are currently being raised in relation to RFID transponders. Content analysis is

> *"…A detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns, themes or biases"* (Leedy & Ormrod 2005, p. 108).

The tool used for the research will be Leximancer. The articles entered into Leximancer will be online works, predominately journals and conference papers, however this will extend to magazine articles and newspapers. The content analysis procedure will satisfy Objective 1 from Section 1.3. The articles entered into Leximancer will be pre-read and determined as articles relating to the topic in order to give a narrower set of results. The results will be critically analysed by creating matrices and conducting a narrative analysis as describe by Saunders, Lewis & Thornhill (2003, p. 401), which will meet the requirements of Objective 2.

1.4.2 Online Surveys

In order to complete Objective 3 from Section 1.3, an online survey will be created. The survey will ask general questions about the level of knowledge of RFID, and specific questions molded by the issues discussed from the content analysis. The survey will follow a pre-test/post-test format, where the respondent will be presented with questions, then information about the topic will then be presented, and finally the same set of questions will be represented. The intended results for the survey is to see what effect a raised awareness on the topic will have on the answers to the questions, and therefore satisfy Objective 3.

1.5. Justification

RFID privacy and security is a topic that is causing a current debate throughout the academic world. This is indicated by a recent issue of the *Communications of the ACM* (Volume 48, Issue 9, September 2005), which dedicated a large proportion of the journal to RFID privacy and security. This research paper is written with the purpose of raising awareness of the possible concerns with the use of RFID transponders. The content analysis will bring out the topics that need to be investigated further. The survey will indicate society's ideas about RFID transponders. This will then help highlight the reasons for educating society about technologies before implementation, and not after the technology has been implemented.

1.6. Limitations

There are several limitations to the research that can be carried out. The limitations include

1. The articles subjected to content analysis will be written from the year 2000 to the present, because RFID has only become relevant to consumers and businesses in the last 5 years, and therefore most of the relevant literature has been written during this period.
2. The articles subjected to content analysis will be of an online nature, due to the requirements of the content analysis tool that is being used.

3. Budgetary and time constraints will cause the scope of the survey to be limited and therefore an adequate global sample will not be achieved.
4. The inability to obtain actual RFID transponders and to interview people who have already been chipped.
5. No case studies can be performed because no government or society has made RFID implementation compulsory.
6. The survey will only be available online and therefore those who do not have access to the Internet will not be able to complete the survey.

2. Literature Review

2.1 Introduction

The purpose of this literature review is to discuss all the research that has been completed to date. This chapter will summarise and then critically analyse the research found. From these findings, the paper will propose a gap in the research that is evident from the literature.

The literature will be broken down into two defined sections. The privacy section will discuss the literature on education of the technology, advising consumers of the presence of RFID tags, and preventative reading measures. The security section will discuss the literature on surveillance, theft prevention, and the use RFID to improve the security of the supply change.

2.2 Privacy

2.2.1 Education

Many authors suggest that the key for public acceptance of RFID is to educate users about the technology. Millar (2004) has written many articles referring to RFID and privacy. Throughout most of her writings she repeatedly states that "…[e]ducation is needed to ensure consumers understand and accept the technology" (Millar 2004, p.

64), and that "…[c]onsumer education also will be useful in dispelling misperceptions about its use" (Millar 2005, p. 2).

The article by Smith (2005) discusses a case study, in which a school underwent a trial of RFID badges in order to take the roll every morning. The school did this by issuing every student with a badge, and placing readers around the school. However, the program went further than expected and not only installed the readers in the classroom, but also in the toilets so that the student's movements could be tracked.

> *"Some students and parents were understandably upset and, after receiving much negative attention, the program was scrapped…"* (Smith 2005, p. 37).

Parents and students not initially being informed correctly about the use of RFID in the school caused the scrapping of this program. This highlights the need for more education about the technology before it is implemented.

The article "RFID is Really Getting Under People's Skin" (Messmer 2004), is an article about John Halamka, who was voluntarily implanted with an RFID chip. The article quotes Halamka as saying, "The security issue 'must be understood as one of the risks of having an implanted identifier'" (Messmer 2004, p. 3). By implanting himself he believes he is emphasising the need for education of the technology before it is implemented on a wide scale.

There is discussion as to who will be responsible for the education of consumers about RFID technology. Gatty states in his article that

> *"…[t]he Federal Trade Commission (FTC)… will leave it up to industry and retailers who use RFID to educate consumers and provide adequate protections form privacy abuse"* (Gatty 2005, p. 2).

This statement is supported by some retail analysts who

> *"…[h]ave urged retailers to embark on public relations exercises and education campaigns in an attempt to reassure consumers that the introduction of RFID technology will not infringe civil liberties or be used to spy covertly on customers"* (Jones et al. 2004a, p. 169).

Throughout the literature on the education of the public of RFID tags, it is consistent that all the authors agree on this topic. VeriChip is an organisation that implants humans with RFID tags in order for certain functions, mainly medical records, to be recorded on the tag. VeriChip states on their web page (www.verichipcorp.com), that education about the technology is given to every client before implantation. Every article highlights the fact that before this technology is implemented, there needs to be education about the technology to the general public, regardless of whom the responsibility falls on.

2.2.2 Informing Consumers of the Presence of RFID Tags

One of the more prevalent privacy issues throughout the literature is the ability to indicate to the consumer which items are tagged and which ones are not. The article

"Radio Frequency Identification in Retailing and Privacy and Public Policy Issues" (Jones et al. 2004b) discusses how

> *"…[t]here are concerns that customers may not be aware, or be given notice, that RFID tags have been attached to products within retail outlets"* (Jones et al. 2004b, p. 50).

The article then discusses how this could leave the consumers unaware that they were being monitored and therefore invading their privacy. It is also important that the notice should be obvious to consumers. It should be

> *"…[c]lear, conspicuous and accurate. The notice should advise consumer if an RFID tag or reader is present and if the technology is being used to collect personally identifiable information about consumers"* (Gatty 2005, p. 2).

The concern that people should know when there is an RFID tag present is one that is agreed on by many authors. There were no articles found that contradicted this statement.

2.2.3 Preventative Reading Methods

Some consumers believe that RFID poses a threat to their privacy. Literature on this issue focuses on the use of blocker and kill tags. The concept behind these tags is that "[r]etailers could use a form of RFID tag that could be deactivated after the point of sale" (Jones et al. 2004a, p. 170) in order to reduce some of the concerns about this technology. The article "The Blocker Tag: Selective Blocking of RFID Tags for

Consumer Privacy" by Juels, Rivest & Szydlo (2003, p. 104) discusses extensively the concepts behind blocker and kill tags. The article explains the purpose of kill tags and why they are inadequate for the use of consumers.

> *"The most straight forward approach for the protection of consumer privacy is to "kill" RFID tags before they are placed in the hands of consumers. A killed tag is truly dead and can never be re-activated."* (Juels, Rivest & Szydlo 2003, p. 104)

Tags can be killed by sending the tag a special "kill" command, which will "…disable the tracking mechanism … (and) may also be programmed to erase the information held on the tags" (Anonymous 2003, p. 2). The authors (Juels, Rivest and Szydlo, 2003) then provide several examples of how the use of kill tags does not necessarily provide benefit to consumers. For example, if the tag contained information regarding the cooking instructions, or the use by date of a product, then this information would be lost through the use of a kill tag before it could be useful.

The article discusses other possible ways of protecting the consumer from the possible threats to their privacy that RFID could cause. The Faraday Cage uses a metal mesh or foil to protect the tag from being read. The active jamming approach uses RF signals to disrupt other signals. However, this approach could disrupt all nearby RFID readers, causing problems on a wider scale. The "Smart" RFID tag approach uses a cryptographic method (encryption and decryption of transmitted data), that increases the functionality and privacy of the tag, which would cause an increase the cost of making the tag.

Throughout the article, Juels, Rivest & Szydlo (2003) predominately focus on the use of blocker tags in protecting consumer's privacy from the threat of RFID tags.

> *"A blocker tag simulates the full spectrum of possible serial numbers for tags, thereby obscuring the serial numbers of other tags. The blocker tag effectively overwhelms this process by forcing it to sweep the full space of all possible tags identifiers which is extremely large"* (Juels, Rivest & Szydlo 2003, p. 107).

The article then acknowledges the technical workings of the tag, which will not be discussed in this research paper. The concept behind the use of the blocker tag is that if a consumer carries a blocker tag, then all other tags in the immediate area can therefore not be read. This process will set up a "privacy zone", which consists of a particular set of numbers that are to be protected by the blocker tag.

> *"With the use of privacy zones and some dynamic alteration of tag serial numbers, it is possible to implement a natural range of privacy polices that may simultaneously satisfy the needs of consumer and businesses"* (Juels, Rivest & Szydlo 2003, p. 108).

The negative side of blocker tags is that they can be used maliciously. The functionality of a blocker tag overloads the reader with information about false tags. "Thus the malicious blocker tag effectively mounts a denial-of-service attacks against the RFID reader protocol" (Juels, Rivest & Szydlo 2003, p. 110). This article

comprehensively covers the importance of kill tags and blocker tags, and shows the in depth working of these technologies. However, this article mentions only kill tags and blocker tags, and does not consider any other aspects of privacy that could be related to RFID tags.

The solution to the problems discussed above could be found in soft blocker tags. The article by Juels and Brainard (2004), titled "Soft Blocking: Flexible Blocker Tags on the Cheap" state that "…[s]oft blockers simply express the privacy preferences of their owners to RFID readers" (Juels & Brainard 2004, p. 2). A soft blocker is created by adding a piece of firmware or software to the tag, which is known as the tag privacy agent (TaPA). The tags are required to have classifications so that the readers know what privacy policy should be implemented. For example,

> *" An "enviroblocker" tag causes a TaPA to block all data fields on "private" tags except the field containing the recycling number on plastic containers"* (Juels & Brainard 2004, p. 3).

The article then technically describes the technology that allows this process to occur. This is definitely a solution to some of the issues created by RFID transponders, however limitations of this technology would arise, as it would be impossible to manage this technology for every possible scenario.

2.3 Security

2.3.1 Surveillance

A concept throughout the literature that has been continually discussed is that of surveillance. The nature of RFID technology allows the tag to be tracked, and therefore allows the surveillance of the tag's owner.

> *"…[t]he concerns revolve around consumer privacy and fears that RFID technology could be used to allow retailers … to track their movement without their knowledge"* (Jones et al. 2004a, pp. 168-169).

Jones et al. (2004a) state that current technology is only able to read a short distance at the present time, and that in order to have mass surveillance, sensors would have to be deployed at frequent intervals. This is a massive undertaking that would ultimately cost a vast amount of money, as the necessary infrastructure is not currently in place.

The concerns of consumers are justified as written by Jones et al. (2004b). The authors state that

> *"If the RFID tags are not removed or deactivated when the customer leaves a store with his/her purchases that customer can be monitored via the radio signals their purchases continue to emit"* (Jones et al. 2004b, p. 50).

The article quotes the National Consumer Council's (2004) concerns that the responsibility of the deactivation of the tags may fall upon the customers, or that retailers might offer incentives to not deactivate the tags. This aspect of surveillance specifically talks about the privacy issues of surveillance. However, surveillance offers many positive uses for security. Surveillance can be used for the tracking of children, to ensure their safety.

> *"In England, eleven-year-old Danielle Duval is about to have an active chip (that is, containing a rechargeable battery) implanted in her. Her mother says it is not different from tracking a stolen car, simply that it is being used for a more important application"* (Michael & Michael 2005, p. 30).

This application of RFID could one day save this child's life. If the child were to get kidnapped, then her location could be tracked for a quick recovery. This article mentions that even though tracking the child is possible, it can not stop an offender from committing a crime against the victim, nor does it allow emergency personnel to appear instantaneously (Michael & Michael 2005, p. 22).

2.3.2 Theft Prevention

The "RFID Report" by Smith (2005) mentions several uses of RFID that increase the theft prevention of many goods.

> *"Key rings with buttons that release car locks are another example of RFID, and some newer cars use the technology to prevent the car from starting unless the*

key gob is hanging from or at least near the steering column" (Smith 2005, p. 37).

This shows a way in which RFID can be used to protect personal goods. It can be used to protect companies in the loss of commercial goods.

> *"RFID technology not only can detect if items are being removed from the store without being paid for, but also can alert security guards if a large volume of particular products have suddenly been removed from a store's shelves in a large-scale shop-lifting incident"* (Jones et al. 2004a, p. 168).

This could provide an increase in security and eventually lower the current rate of theft. The use of RFID in society could make most items less vulnerable to theft by only allowing the owners of goods to activate them. However, as long as goods can be physically moved, this will not stop someone stealing items, but rather only lets the owner know that the items are gone.

2.3.3 Supply Chain Management

RFID can significantly improve the security of supply chain management, as it is seen as the technology to replace barcodes.

> *"…[t]he technology would seem to have potential to revolutionise the efficiency, accuracy and security of the supply chain"* (Jones et al. 2004b p. 46, 2004a, p. 167).

An example of this technology already being implemented is the Defence Department of the United States of America who now require that "all products it purchases be outfitted with RFID to improve logistics and supply chain management" (Harris 2005, p. 1). RFID tags would be able to track every movement the product made through the supply chain from the manufacturer to the consumer. This would enable retailers to examine their supply chain, and figure out where things are more likely to go wrong. RFID would also improve the function of the warehouse, as products could be stored according to their shape, instead of by their category, which would allow more efficient packing and stacking of goods. It would also enable the warehouse manager to track the location of goods and therefore improve the security of the goods (Jones et al. 2004b, p. 48).

2.4 Gap

There is much literature on the topic of RFID tags. The technology behind the devices, the encryption methods, the work done by the AutoID centre and the endless uses of the technology are all very well documented. However, there is substantially less literature on the privacy and security aspects of RFID. Sections 2.2 and 2.3 have given a detailed outline of the prominent concerns for RFID tags in relation to privacy and security. Some of these articles are very in-depth and give a very good explanation of the issue, but most are only concerned about one aspect. The articles that do refer to more than one issue only do so very briefly.

Want (2004) gives a very good overview of RFID as a whole. He discusses the RFID technology and the RFID system in detail. However, in this article he dedicates less than half a page to privacy and security. While these sections discuss the relevant issues, it is very brief, and therefore a not a good summary.

The article "Privacy in the Global E-Village" (Pottie 2004) acknowledges several of the key issues that have been discussed. These include surveillance, the knowledge of the presence of a tag, and education about RFID in general. However, this article is only three pages in length, and the relevant issues are discussed in less than a paragraph each.

Jones et al. (2004a) focus their paper on the importance of RFID in relation to its use in retail. This article discusses several of the issues including education about the tag, informing consumers of the presence of a tag and improvements in supply chain management. However, the other issues are left unnoticed.

Throughout the readings, there is one consistent gap in the literature. Many authors have written about the topic, but they have either done this too briefly, or have only studied one part in-depth. The gap is that currently there is no comprehensive, succinct list of all the issues discussed throughout the literature. No author has yet taken the step of linking together all the issues raised by the articles in regards to RFID privacy and security. There are no papers, to date, that discuss a completed computer-aided content analysis on this topic, which when completed will satisfy Objective 1 from Section 1.3. No online surveys have been completed that are specific to RFID privacy and security, and therefore society's opinion about this topic

has yet to be indicated (Objective 3, Section 1.3). This research paper intends to fill this gap, and in order to do so it will follow the methodology described in Section 3.

2.5 Conclusion

The literature review has discussed the prominent issues in the literature. It should be noted that many authors do not emphasise the difference between privacy and security, and quite often these words are used interchangeably throughout the literature. The literature on the education of the general public about RFID technology, the advisement of consumers of the presence of RFID tags, and preventative reading measures such as blocker and kill tags were discussed in the privacy section, and throughout this section there was agreement on all the issues from the authors. The literature on surveillance, theft prevention, and the RFID to improve the security of supply change management was discussed in the security section. Even though there was consensus throughout the topics of theft prevention and supply change management, there were differing views of opinion regarding the implications of surveillance

Throughout the literature the gap was evident. The papers that talk about more than one issue are very brief and the papers that are in detail only talk about the one issue. There are no papers that give a detail analysis of all the issues, and that is the gap that this research paper intends to fill.

3. Methodology

3.1 Introduction

The methodology in this paper will be twofold. Firstly, after reviewing the literature, it has become obvious that the piece of missing research is that there are no papers that comprehensively list and discuss all the issues raised by RFID. This can be obtained by performing a content analysis of this topic. The content analysis will be computer-aided and performed with the help of a tool named "Leximancer". Secondly, in order to satisfy the objective 3 (of Section 1.3), which was to determine the level of awareness and asses the level of concern over the results, an online survey will be performed. It will follow a classic pre-test/post-test design, which asks questions, presents information, and then asks the same questions again, to see if providing the respondent with factual information about the topic changes their opinion.

Content Analysis is both qualitative and quantitative (Leedy & Ormrod 2005, p. 143). The reason for this is that content analysis will count each time particular words come up and provide some statistically analysis, therefore making it quantitative. It also shows the relationships between the themes, and therefore making it qualitative as well. The online survey will be quantitative. Figure 1 is a diagram of how the two research methods will be used in order to complete this research.

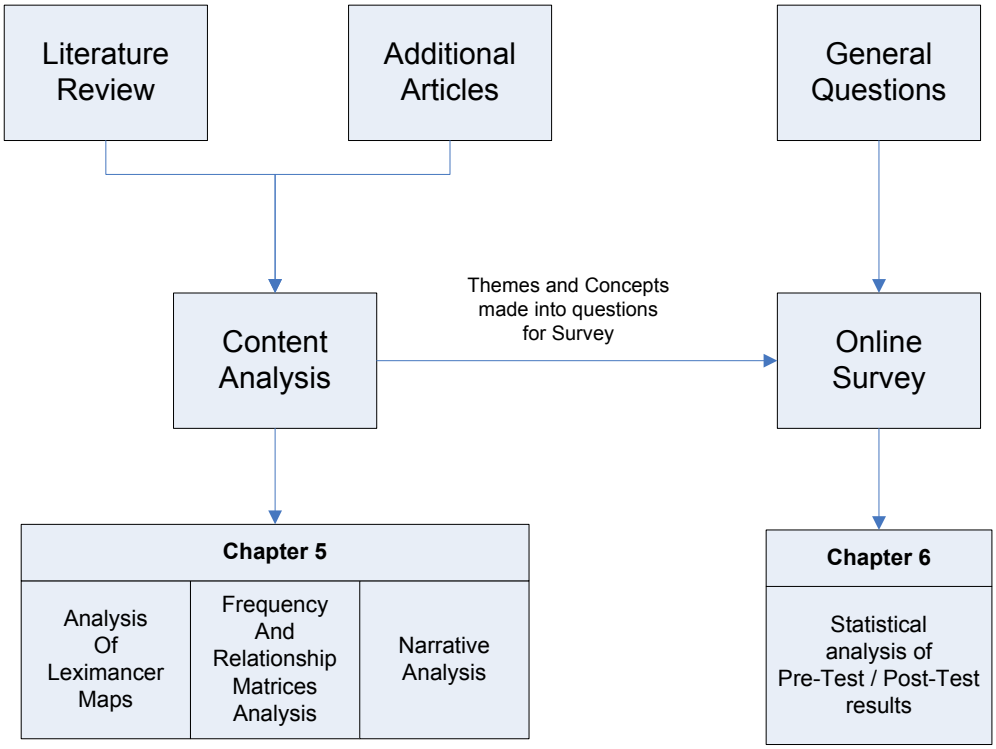

Figure 1 Research Diagram

3.2 Content Analysis

3.2.1 Introduction

In order to satisfy Objective 1 from Section 1.3, content analysis will be performed as the primary method used in this research paper. Content analysis is defined as

> *"… [a] detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns, themes or biases. Content analyses are typically performed on forms of human communication, including books, newspapers, films, television, art, music, videotapes of human interactions and transcripts of conversations."* (Leedy & Ormrod 2005, p. 143)

In this paper, the content analysis material will be restricted to a variety of online articles, including journal publications, conference papers, magazine articles and newspaper articles. The material that will be subjected to the analysis will be carefully selected, to make sure that it is relevant to the research topic. Defining markers that will determine whether an article is to be analysed will include relevant keywords such as “RFID”, “privacy” and “security”. The article will be pre-read to ensure the content is relevant. The choice of articles will also be restricted to those written from the year 2000 onwards, because RFID has only become relevant to consumers and businesses in the last 5 years, and therefore most of the detailed, in depth and relevant literature has been written during this period.

3.2.2 Advantages and Disadvantages of Computer-Aided Content Analysis

The content analysis used in this research paper will be aided by the use of a computer program named Leximancer (Section 3.2.3). There are several advantages and disadvantages of using computer-aided content analysis. The advantages include that the rules for coding are clearly identified and that the computer provides the perfect coder. One disadvantage is that there is often too much text to analyse, and therefore data reduction would need to be performed (Weber 1985, p. 41). The data reduction for this research will limit the number of articles used in content analysis to fifty and the articles will be pre-read to ensure relevance. Weber describes several ways of manipulating text including

> *"...[w]ord frequency counts, key-word-in-context (KWIC) listing, concordances, classification of words into content categories, content category counts, and retrievals based on content categories and co-occurrences"* (Weber 1985, p. 41).

Leximancer uses several of these techniques to manipulate text to obtain results.

3.2.3 Leximancer

The content analysis will be assisted through the use of a tool named "Leximancer."

> *"Leximancer is a data-mining tool that can be used to analyse the content of collections of textual documents and to visually display the extracted information. The information is displayed by a means of a conceptual map that provides a bird's eye view of the material representing the main concepts contained within the text and how they are related"* (Leximancer 2004, p. 4).

Leximancer has several phases in which it performs the content analysis. They are Text Preprocessing, Automatic Seed (Concept) Extraction, Concept Editing, Concept Thesaurus Learning, Classification and Mapping (Figure 2). It is expected that fifty articles will be parsed through Leximancer.

Please see print copy for Figure 2

Figure 2 Phases of Processing in Leximancer from Leximancer v 2.16 (The Program)

Leximancer will be used to bring out the major concepts that have been prominent throughout the material. Leximancer does this by showing a map with all the themes entered on the graph. The graph has 2 axes, and the closer to the centre of an axis the more prominence the theme has. Figure 3 is an example map from Leximancer.com that shows the U.S. Intelligence Community's Pre-war Intelligence Assessments on Iraq.

Please see print copy for Figure 3

Figure 3 An example map of "The U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq" from Leximancer.com

These concepts will then be critically analysed by the use of frequency and relationship matrices while focusing on privacy and security and then modelled into a narrative analysis (Objective 2, Section 1.3). Saunders, Lewis and Thornhill discuss the use of narrative analysis and state that "… [n]arrative analysis may be used as a means to explore linkages, relationships and socially constructed explanations…" (2003, p. 402).

3.3 Online Survey

3.3.1 Introduction

The themes that have been highlighted through the results of the content analysis will then be presented to the public in the form of an online survey (Objective 3, Section 1.3).

> *"Survey research involves acquiring information about one or more groups of people – perhaps about their characteristics, opinions, attitudes or previous experiences – by asking them questions and tabulating their answers"* (Leedy & Ormrod 2005, p. 183).

The survey that is conducted will be online, and data will be collected and stored into a database. The advantage of the survey being online is that it provides a larger

opportunity for more people to access it, and therefore will give a greater, more diversified, sample of society.

3.3.2 Advantages and Disadvantages of Online Surveys

The advantages for using online (Internet) surveys are "…the low cost and the speed of data collection" (Czaja & Blair 2005, p. 40). It is significantly cheaper than any other forms of surveys as it removes all postage, telephone and paper costs of the survey. It also allows quick data collection as data is being entered straight into a database. The disadvantages associated with online surveys include that not everybody has Internet connection, low response rates, and the possibility for bias (Czaja & Blair 2005, pp. 42-43).

3.3.3 Content

The design of the survey will be of a classic pre-test/post-test design. The survey will be presented in four sections. The first section will ask generic information such as the participant's age bracket, the country of birth, the country in which most of the participant's life has been spent, the participant's religious background, education level and the industry in which they are currently employed. The purpose of this information is to help identify trends in the answers of the rest of the survey. There can be many social, cultural, religious and ethical issues that can affect someone's response to RFID implementation (Michael & Michael 2004). For example, many religions clearly state that any sort of changes to the body, whether it is tattooing, piercing or the implanting of RFID tags, is against the will of their god. Education is

also a factor that needs to be examined. It is unknown if a university graduate would know more about RFID tags than someone who only completed the minimum mandatory schooling requirement. Age is also an important factor. People who have grown up with computers, for example current university students, are expected to have different results than an eighty year old grandmother. Someone who works in the IT field is also expected to know more about the technology than someone who works in a different industry. No surveys will be excluded from the results because of these factors, but rather these factors will be used to critically analyse certain trends in the results.

The second section will be a page of questions relating to the person's prior knowledge of the topic. The survey will also ask questions about the key elements that have been raised from the content analysis process. These questions will not be able to be written until the first method is almost complete. After this section has been completed, the next section will be implemented, where the respondent will be presented with factual information about RFID.

After this information is read, the respondent will be able to move onto the last section (Section 4). This will be presented to the respondent and the same questions that appeared on section 2 will be asked again. The purpose of this section is to obtain the same information after the respondent has been informed of facts about RFID. A comparison of the data sets will then be performed, to see if the information that was provided has changed a person's opinion about the topic. This will justify Objective 3 (Section 1.3), which was to determine the level of awareness of RFID tagging. This data will show whether informing the participant will have an impact on their opinion

in regards to RFID transponders and their uses. A copy of the full survey can be viewed in Appendix 4.

3.4 Unit of Analysis/Time Horizon

The unit of analysis for this paper is the Meaning Unit. Anderson & Kanuka (2003) state that

> *"Henri (1991) rejected the process of a priori and authoritatively fixing the size of the unit based on criteria that are not directly related to the construct under study. Instead, she proposes a thematic or meaning unit"* (Anderson & Kanuka 2003, p.180).

This is interpreted as meaning that the unit of analysis is not a fixed size. Therefore the unit of analysis will be referring to keywords such as "RFID", "privacy" and "security", and according to the content analysis results may expand to included "education of the technology" and "surveillance" as well as other issues. This research is a cross-sectional study. It will only be gathered once over period of weeks. If resources allowed, it may be turned into a longitudinal study at a later date.

3.5 Conclusion

The methodology that will be used to complete the research for this paper will meet the objectives that have been defined in Section 1.3. Objectives 1 and 2 will be

completed through the use of content analysis. This process will highlight the main themes and indicate their prominence throughout the literature. These themes will then be converted into questions for the online survey in order to complete Objective 3, which was to determine the level of awareness and asses the level of concern over the results. These two methodologies will not only complete the objectives, but also fill the gap in the literature.

4. Exploration of the Themes and Concepts of RFID Privacy and Security

4.1 Introduction

This chapter explores the themes and concepts surrounding RFID as a result of the content analysis. A list of the body of text that was analysed can be found in Appendix 1. The selection of text was processed through the computer-aided content analysis tool named Leximancer. As a result of this, several Leximancer maps were produced (as seen in Figures 4 - 9), and a ranked concepts list was created (Appendix 2).

There are two classifications of terms in Leximancer, themes and concepts. Large coloured circles on the map represent themes and each theme has many concepts, which are represented by dots. Figure 4 shows a map of just the major themes. Each concept was compared to a relative frequency, which indicates the frequency as a percentage of that concept when it appeared near the theme. There were several words that were removed from the analysis. For example, the words RFID and tags had to be in the article for it to be included, and therefore nothing could be learnt from their inclusion. Other words that were omitted include people, require and including, as these are generic words that would be found in any selection of texts, and are not specific to the topic.

Please see print copy for Figure 4

Figure 4 - Leximancer Map - Major Themes

The Leximancer results also enable frequency and relationship matrices to be constructed, and more results can be drawn from this as discussed in Section 4.3. The conclusions will then be displayed in a Narrative Analysis, as described by Saunders, Lewis and Thornhill (2003, pp. 401-402). The last section indicates how the results were used to form the questions from the survey, the results of which will be discussed in Chapter 5.

4.2 Leximancer Map Analysis

4.2.1 Privacy

Privacy is a strong theme that overlaps many other themes on the map (Figure 5). Concepts inside the theme include public, identity and personal. The concept of public refers to the many articles mentioning the response that has come from society over

different trials of RFID, particularly those that use RFID in retail for the item level tracking of goods. There is a large debate as to whether the RFID system has the ability to link customer's identities to the tags that they are carrying. Some state that

> *"…[t]he impact of consumer privacy concerns on retailers' RFID adoption doesn't exist as long as there is no association of a customer's identity with an RFID tag. If the store just sees RFID tags and doesn't identify you, you really have nothing to worry about"* (Berthiaume 2005, p. 2).

The concept personal refers to the personal information that could be gathered through the RFID system.

Please see print copy for Figure 5

Figure 5 - Leximancer Maps - Privacy

The main concepts linked with this theme are as follows.

Concept	Relative Frequency
Technology	30.6%
Consumer	24.5%
System	22.9%
Reader	21.6%
Security	20.5%
Information	20.2%
Tracking	20%

Table 1 - Concepts Linked to Privacy

There are many important concepts that are linked with the theme of privacy. The concepts of technology, reader and information will be discussed below in their own themes. The concept consumer is linked because ultimately it is the consumer's privacy that could be compromised. The concept of tracking is considered the largest concern.

> *"The ability of RFID-tagged products to track merchandise from inception to the point of sale and beyond has some privacy experts sounding an alarm. These privacy advocates worry about the prevalence of RFID tags eventually being used to track people unwittingly"* (Germain 2003, p. 2).

The RFID system also needs to be secure in order to protect privacy. Not only do the transmissions from the tag to reader have to be protected from unauthorised reading, but also the information that is sent from the reader to the network to access the database needs to be secure.

4.2.2 Reader

The theme of Reader (Figure 6) in relation to RFID refers to the device that can read RFID transponders. The concepts that are inside the theme are passive, power, serial, number, database, unique, range and cost. The concepts of passive and power refer to the type of tag known as passive, which receives its power from the reader's signal. The signal that is communicated from the tag to the reader is a unique serial number, which is then used to access the information from the database. The cost of the RFID system, both for the tag and the reader is listed as one of the main items that is preventing the wide scale implementation of RFID, as readers typically cost greater than $US1000 each (Cavoukian 2004, p. 10). The range (distance) that a reader can read is constantly changing and this is a privacy and security concern as "[A]ll RFID operates through radio, which by its nature, anyone within range can receive" (Good et al. 2004, p. 1).

Please see print copy for Figure 6

Figure 6 - Leximancer Map - Reader

The main concepts linked with this theme are as follows.

Concept	Relative Frequency
Information	23%
System	22.7%
Privacy	21.7%
Data	18.4%
Number	17.6%
Security	14.9%

Table 2 - Concepts Linked to Reader

Most of these concepts are evidently linked to the theme. For example, the reader is part of the RFID system that collects information and data that can be identified through a unique number stored on the tag. Privacy is a theme, which is discussed above in section 4.2.1. The concept of security refers to ensuring that the system is protected against unauthorised access, which includes both data transactions from the tag to the reader and the reader to the database.

4.2.3 Technology

Technology (Figure 7) in regards to RFID refers not only to the individual pieces of the system, but also using the technology as a whole system. There are many of concepts inside the theme of technology that are not specific to technology, and many that are more related to privacy than technology (as discussed in section 4.2.1). Those that are related to technology include goods, inventory, retail, tracking, industry and development. The relationships behind these terms are fairly obvious. The technology is used in retail and industry to help them develop better supply chain management (SCM) by enabling fast tracking of their inventory.

> *"Such tracking can be accomplished by monitoring objects with attached transponders ("tags") to them, whether it be in a store, a warehouse, or beyond these premises"* (Plitcha 2004, p. 1).

The concept development also refers to the development of the RFID technology, which in turn will aid a faster implementation into society.

Please see print copy for Figure 7

Figure 7 - Leximancer Map - Technology

The main concepts linked with this theme are as follows.

Concept	Relative Frequency
Privacy	35%
Tracking	28.9%
System	27.5%
Information	26.2%
Security	19.7%
Data	19.7%

Table 3 - Concepts Linked to Technology

The concept that has the strongest link with technology is privacy. As seen in Figure 4 these themes overlap each other. Many articles suggest that RFID technology will be a threat to privacy, and this is discussed above (Section 4.2.1). The RFID system is made up of different pieces of technology, and together the RFID system's purpose is to use pieces of information and data in order to track and identify goods. The concept of security in regards to RFID technology can be split into two categories. Firstly it is being used to improve the security of goods, through the ability to track goods moving through the supply chain. Secondly, many consider the technology as a security risk due to the lack of authentication standards, and there is no way to tell when a tag is being read, nor does it keep a history of who or when it was read. (Garfinkel, Juels & Pappu 2005, p. 4)

4.2.4 Information

Information (Figure 8) generally refers to a collection of facts from which a conclusion can be drawn, however in regards to RFID it refers to the data being stored on the tag, or the data that can be accessed through gaining a serial number from the tag. The concepts that are inside the theme of information are data, provide, access, devices, system, standard, control, identification and application. These concepts can

be split into 3 different categories. The first category refers to the information itself and includes the concepts of data and provide, where provide refers to which information is provided on a tag, and who provided it.

> *"The data transmitted by a tag may provide identification or location information, or specifics about the product tagged, such as price, colour, or place and date of purchase…"* (Cavoukian 2004, p. 11).

The second category refers to the RFID system's ability access and store the information and includes the concepts of access, devices, system, standard and control. The third category refers to the purpose of the information and includes the concepts of identification and application, where application implies the use of the technology in a system.

Please see print copy for Figure 8

Figure 8 - Leximancer Maps - Information

The main concepts linked with this theme are as follows.

Concept	Relative Frequency
System	30.7%
Data	29.3%
Technology	28.3%
Reader	28.3%
Privacy	25%
Product	20.5%
Security	19.9%

Table 4 - Concepts Linked to Information

There are several very obvious links listed above. Firstly, it is the system that will store the information. Data is the information before it has been processed, and the information stored will usually be about the product or person to which the tag is attached. Technology simply refers to the devices (like the reader) that are involved in the RFID system. The privacy concept is one that has been discussed in-depth in section 4.2.1, and it is the security of the information that will protect the information against tampering and unauthorised access.

4.2.5 Authentication

Authentication (Figure 9) in a general context refers validating the authenticity of something or someone. The concepts that are inside the theme of authentication are blocker, protocol, approach, problem and level. All of these concepts are related because they all describe different methods or aspects in regards to improving authentication in the RFID system. The issue that is surrounding authentication involves the lack of ability to protect RFID tags from unauthorised readings. It also involves accurately identifying the validity of that tag's identity.

"Authentication is an important RFID security measure for preventing counterfeit manufacture or substitution" (Ranasinghe, Engels & Cole 2004, p. 3).

There are many articles that were analysed that contained very specific technical content about authentication schemes and protocols, which is not discussed in this paper.

Please see print copy for Figure 9

Figure 9 - Leximancer Maps - Authentication

The main concepts linked this theme are as follows.

Concept	Relative Frequency
Reader	40.5%
System	32.8%
Security	30%
Number	29.3%
Information	27.2%
Data	23.7%

Table 5 - Concepts Linked to Authentication

Authentication is strongly linked to the concept of reader, as it is the reader that must complete the authentication, both to validate that the reader is authorised to read that tag and the tag that is being read is valid. The RFID system should include authentication as a security feature. The concept of numbers in relation to authentication refers to a unique series of digits that could be use to validate the information and data that is obtained through the RFID system.

4.3 Frequency and Relationship Matrices

The matrix (Table 6) identifies the frequency between all the themes and their linked concepts as mentioned in Section 4.2. The grey highlighted area shows the total count of each theme or concept throughout the body of literature. The rest of the matrix shows how many times the themes or concepts appear near each other (usually within 3 sentences), so that links can be identified.

Entity	RFID	tags	privacy	reader	technology	information	system	data	security	tracking	product	number	consumer
RFID	2333	2076	623	625	553	510	536	403	408	329	336	300	291
tags	2076	2097	560	626	488	470	502	384	354	310	332	293	273
privacy	623	560	632	137	194	128	145	110	132	127	77	45	155
reader	625	626	137	629	78	145	143	116	94	57	76	111	60
technology	553	488	194	78	553	145	151	109	109	160	95	41	94
information	510	470	128	145	145	511	157	150	102	94	105	79	68
system	536	502	145	143	151	157	537	105	133	85	73	71	59
data	403	384	110	116	109	150	105	403	79	63	62	63	51
security	408	354	132	94	109	102	133	79	416	49	48	59	27
tracking	329	310	127	57	160	94	85	63	49	329	83	44	70
product	336	332	77	76	95	105	73	62	48	83	337	64	80
number	300	293	45	111	41	79	71	63	59	44	64	304	22
consumer	291	273	155	60	94	68	59	51	27	70	80	22	291

Table 6 - Frequency Matrix

For simplicity, the numbers in the frequency matrix (Table 6) were converted into a scale between 1 (low) and 10 (high), as seen in the relationship matrix (Table 7). The scale was calculated by finding number of times two concepts appeared together compared against the total number of times one of the concepts appears throughout the text. The concepts that appear above the diagonal grey line are compared to the horizontal axis, and the concepts that appear below the diagonal grey line are compared to the vertical axis.

Entity	RFID	tags	privacy	reader	technology	information	system	data	security	tracking	product	number	consumer
RFID	2333	9	3	3	3	3	3	2	2	2	2	2	2
tags	10	2097	3	3	3	3	3	2	2	2	2	2	2
privacy	10	9	632	3	4	3	3	2	3	3	2	1	3
reader	10	10	3	629	2	3	3	2	2	1	2	2	1
technology	10	9	4	2	553	3	3	2	2	2	2	1	2
information	10	10	3	3	3	511	4	3	2	2	3	2	2
system	10	10	3	3	3	3	537	2	3	2	2	2	2
data	10	10	3	3	3	4	3	403	2	2	2	2	2
security	10	9	4	3	3	3	4	2	416	2	2	2	1
tracking	10	10	4	2	5	3	3	2	2	329	3	2	3
product	10	10	3	3	3	4	3	2	2	3	337	2	3
number	10	10	2	4	2	3	3	3	2	2	3	304	1
consumer	10	10	6	3	4	3	3	2	1	3	3	1	291

Table 7 - Relationship Matrix

There are several interesting conclusions that can be drawn from the information in this matrix. Firstly, it is important to note that it is an expected result that the first columns are filled with high numbers, as it was a requirement for the text to be included in the content analysis sample that it's subject was RFID tags. Secondly, the high result for consumer and privacy indicates that the main affect RFID will have on consumers is the invasion of their privacy. Another noticeable result was that the main concern in regards to tracking is that it will be easier to accomplish as the technology develops and therefore becomes more readily available.

There were three sets of results that drew the same conclusion regardless of which concept they were referred to. The first of these is the link between privacy and technology. This indicates that it is the technology that would enable the possible

breaches of privacy. The second of these is the link between security and system, which shows that the security of the system is integral to the implementation of an RFID system. The last of these is the missing link between consumer and security. Unlike the very first conclusion drawn, which showed that it was consumer's privacy that could be invaded, it shows that there is no link between consumer and security, and this implies that security needs to be applied to system more than it does the consumer itself. A coloured matrix highlighting these conclusions can be found in Appendix 3.

4.4 Narrative Analysis

The content analysis was performed using a computer-aided content analysis tool named Leximancer. There were fifty articles placed through the tool. Each article was screened for relevance, and as part of the inclusion criteria, the words RFID and privacy or security not only had to be present in the article, but also had to be the main focus of the article. Several major online databases were searched for journal articles, which included ACM, IEEE and Proquest.

The content analysis resulted in two different types of analysis. The first type was that of the Leximancer maps. These showed five major themes, which included privacy, reader, technology, information and authentication. RFID and tags were purposefully left out of these results as every article had these words included, and therefore nothing could be learnt from their inclusion. Security was not a theme by itself, however it was linked to all five themes. Also linked to these themes were several concepts including data, tracking, product, number and consumer.

Each of these themes and concepts, along with the concepts of RFID and tags, were displayed in a set of matrices, which is the second type of analysis from the content analysis. The first matrix (table 6) showed the total frequency of each of the concepts. The second matrix (table 7) showed relationship between the concepts through a scale of 1 to 10. The outlying results were then identified and discussed.

The results from the Leximancer maps showed several key results. Tracking was noted as the main way in which RFID technology would breach a person's privacy. Information was categorised into three categories, which included the information provider, the ability to access and store information, and the purpose of the information. Authentication was a theme that could also be broken down into two segments. Firstly the ability to authenticate goods using the technology, and secondly the need to improve the authentication that is needed to access the information on a RFID tag.

The matrix revealed various results. Technology was linked to both privacy and tracking. This shows that it is the ability for this technology to do the tracking that causes a person to lose their privacy. It also highlighted the link between security and system, and drew attention to the lack of link between consumer and security. This implies that there is no security risk to the person when they are carrying an RFID tag, but rather only to the system in regards to unauthorised access.

The two different types of analysis show several results of significance. Initially it shows the link of privacy to the consumer, and interestingly not to industry. This

would imply that the need to protect the privacy of industry, including supply chain management information, has not been researched extensively yet. The major privacy breach is the ability to track tags. This is an aspect of the technology that could be altered with development. Technology is also linked to authentication, because it is through development of the technology that an efficient and effective authentication system can be implemented to prevent unauthorised reading of RFID tags.

The outcomes of this show that privacy and security are very separate concepts. For example, privacy is specific to people and consumers, where as security is underlying to all themes and concepts, and has a specific connection to the system. RFID tags are not at present considered a security threat to the person. This two analysis together complete the outcomes of Objective 1 and 2 as listed in Section 1.3.

4.5 Development of Survey Questions

The RFID specific questions in the survey were developed from a number of sources. Some of the questions were general questions to find out the participants opinion about RFID. A majority of the RFID specific questions in the survey were developed from concepts that were learnt through the content analysis survey. An outline of the questions can be found in Appendix 4.

Many of the different sections in Question 14 (and 24) were developed from tracking. This included the questions asking about monitoring package location, children's location and staff work habits, as well as tracking crime suspects, money spending

and shopping habits which all ask about the ability for the technology to track the tags.

There were numerous questions that arose from the theme of information. Questions 15a and 15b asked about different organisational institutions storing information over a long time period. Question 16 asked about the ability to update information, and Question 17 referred to who had access to the information. The entire of question 19 asked about what type of information should be stored on the RFID tag.

4.6 Conclusion

The content analysis has resulted in several notable conclusions. Firstly, the five major themes in regards to RFID were identified, and they were privacy, reader, technology, information and authentication. It was discussed how security, although not a theme on it's own, was an underlying concept to all five themes. Both analyses supported the conclusion that privacy was specifically related to the consumer, and security was specifically related to the system. A missing link between consumer and security identified that RFID tags were not, at present, considered a security threat to humans.

Tracking was noted as a concept that caused a high concern over the breaching of privacy. Consumer privacy was mentioned on a regular basis, however conclusions were drawn that indicated a lack of research in regards to protecting commercial privacy. Ultimately, the development of technology is considered the biggest concern in relation to privacy because as the technology develops it will become harder to

regulate its implementation. This research lists the major concerns that were identified through the content analysis as listed in Objective 1 (Section 1.3) and has critically analysed the results through the use of matrices and a narrative analysis (Objective 2, Section 1.3).

5. Analysis of Society's Opinion

5.1 Introduction

The online survey was conducted over a three week period. In this time emails were sent to many people to request that they would complete the survey. The total number of responses recorded was 106, however only 101 of these are usable. This is because some of the participants did not approve the ethics statement, while other results were incorrectly recorded by the system. Every question had the option to not answer the question, and so if while discussing the results the percentages do not add up to 100% this is because one or more of the respondents have opted out of answering this particular question.

The survey was conducted in a pretest/posttest design. Participants were initially presented with a set of questions, information was then provided, and then the same questions were asked again. The purpose of this is to gauge whether education about the topic changes the participant's opinion, in order to satisfy Objective 3 from Section 1.3. A full set of questions and the ethics approval form can be found in appendices 4 and 5 respectively.

5.2 General Background of Participants

This section will talk about the background of the participants in the survey, with particular notice to any irregularity to a random sample of society. The gender of the participants was fairly equal, however the age distribution was skewed in certain groups, as seen in Figure 10.

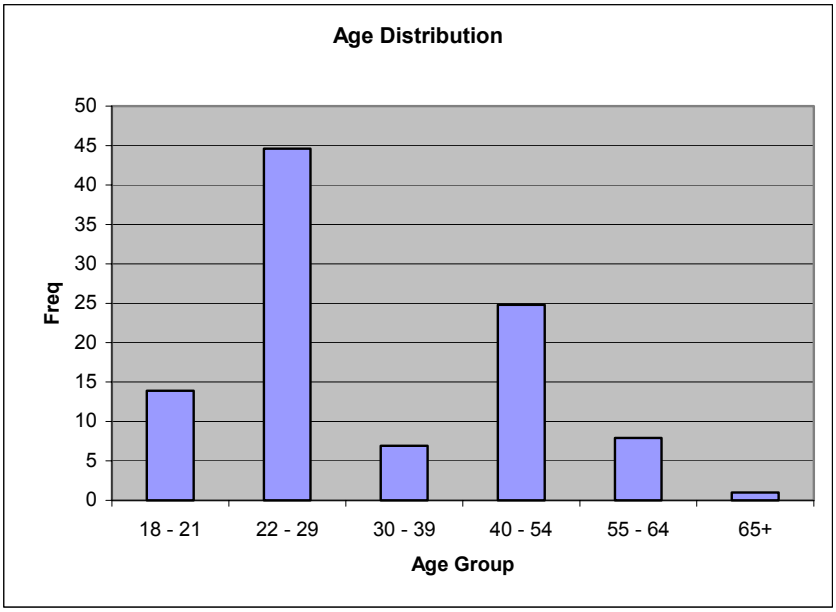

Figure 10 - Age Distribution Graph

An aspect that would also affect the results is that 50.5% of respondents have completed a university degree, and 22.8 % have completed tertiary education. This is slightly abnormal for a random sample, but it was an expected result, as a majority of the research was conducted in a university setting. Some background considerations that could affect the results in specific relation to the topic include that 34.7% of respondents were working or studying in an IT related field. It should also be noted that 30.7% said that they knew what RFID was before starting the survey, and that 49.5% were unsure of the technology.

5.3 Analysis of Results

5.3.1 Implementation of RFID in Humans

Before the information was presented to the respondents, only 22.8% knew that RFID was currently being implanted into humans. This changed to 72.3% in the post-test

results. The next question asked whether the respondent would be willing to be implanted with a RFID tag, and the results were nearly identical before and after the information. In the post-test results 11.9% would get implanted, 72.3% would not get implanted, and 15.8% were unsure.

5.3.2 Possible uses of RFID Transponders

The next series of questions that were presented asked the participants about the possible uses of RFID. In the pre-test results, many of the questions had a large response in the "Not Sure" category, however after the information was presented most of these results showed a shift to the correct answer. An example of this is in Figure 11, which shows the results to the question of whether a RFID tag could automatically identify a human. The exception to this was in response to whether an RFID tag could automatically unlock cars, and this showed a swing towards the incorrect answer of "No".

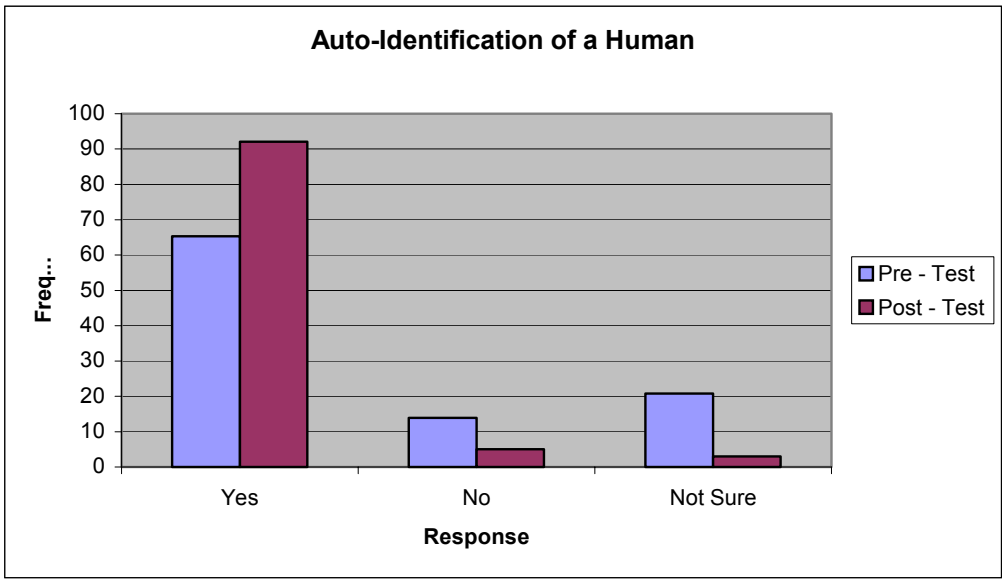

Figure 11 - Results for Auto-Identification of a Human

5.3.3 The Level of Concern over the uses of RFID

The results in this section were varied depending on the question that was asked. These questions asked the participants about their level of concern over certain uses of the technology. Some questions had little noticeable change. For example, the level of concern over the automatic checkout at the supermarket and the monitoring of package location remained consistently low, where as the concern level over tracking money spending remained consistently high. Initially, many respondents had lower level of concerns over patient identification, however after the information was presented, there was a split between those who were extremely concerned compared to those who had a low level of concern. There were some results that had a slight swing towards a higher level of concern, and they included monitoring children's location, tracking shopping habits and monitoring staff habits. An interesting result was that of the ability to track crime suspects (Figure 12). Initially there was a skew towards no concern, but after the information was presented, the responses evened out to be almost the same for all responses.

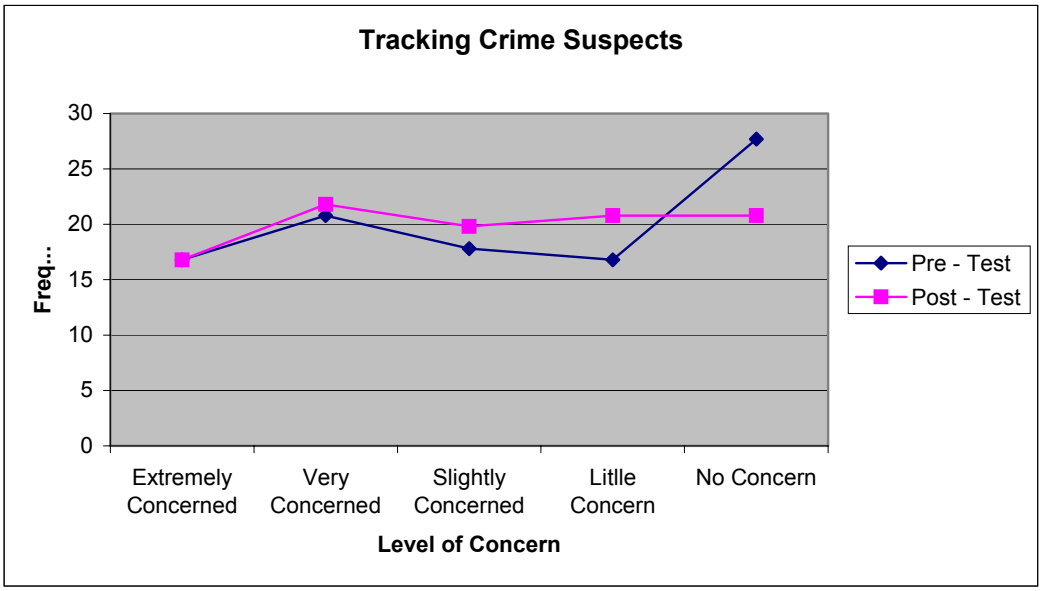

Figure 12 - Response for Level of Concern over Tracking Crime Suspects

5.3.4 The Level of Concern over the Wide Scale Implementation

The next questions asked the participants about their opinion on government and commercial bodies collecting personal information over a period of time. The results for a government body changed after the information had been presented. As can be seen from the graph (Figure 13), even though the number of people who were extremely concerned dropped, the overall level of concern has risen.

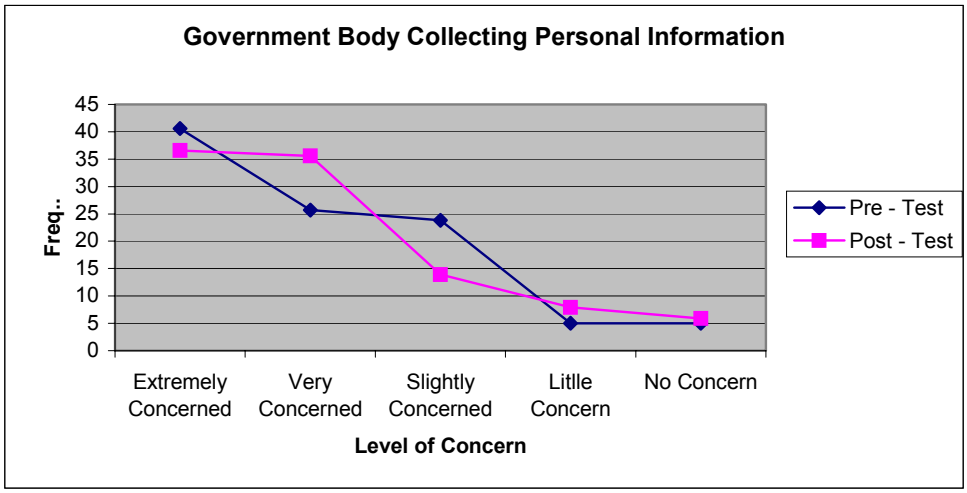

Figure 13 - Response over Government Body Collecting Personal Information

An interesting result was that of the commercial body collecting data showed no changed from pre-test to post-test. As expected people were more concerned over the commercial body collecting information, rather than the government body, as shown in Figure 14.

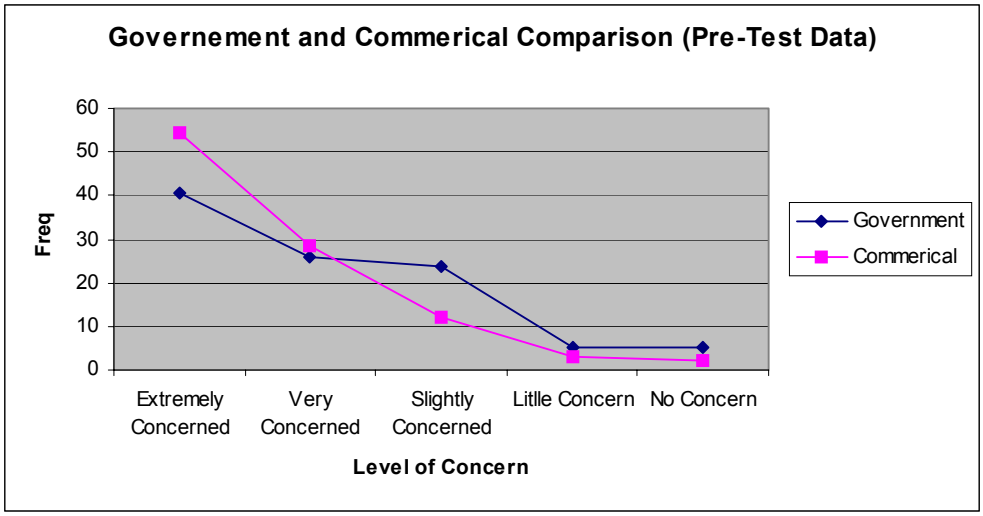

Figure 14 - Government and Commercial Comparison (Pre-Test Data)

Questions were asked about the level of concern over somebody else having the responsibility to update the respondent's personal information. Initially the level of concern was high, but after the information was presented the level lowered slightly. Participants were also asked about their level of concern over the implementation of a nation-wide ID scheme. There was almost no change in the data, however it should be noted that 53.5% of people were extremely concerned, and 26.7% were very concerned. This is a high statistic, and by itself is an argument against such a scheme. A similar result was found for the question that regarded only authorised personnel accessing the system, and statistics were once again indicating a high level of concern.

5.3.5 Approval of RFID Tag Data

This section asked participants which pieces of data they would approve to be stored on a RFID tag. There were two different scenarios for which all the questions fell into. Firstly, the questions of whether personal information and medical information

should be stored both had a slight swing to the approval of data onto the tag, however there were still some who did not approve the addition of data onto the tag. These results can be seen in Figure 15.

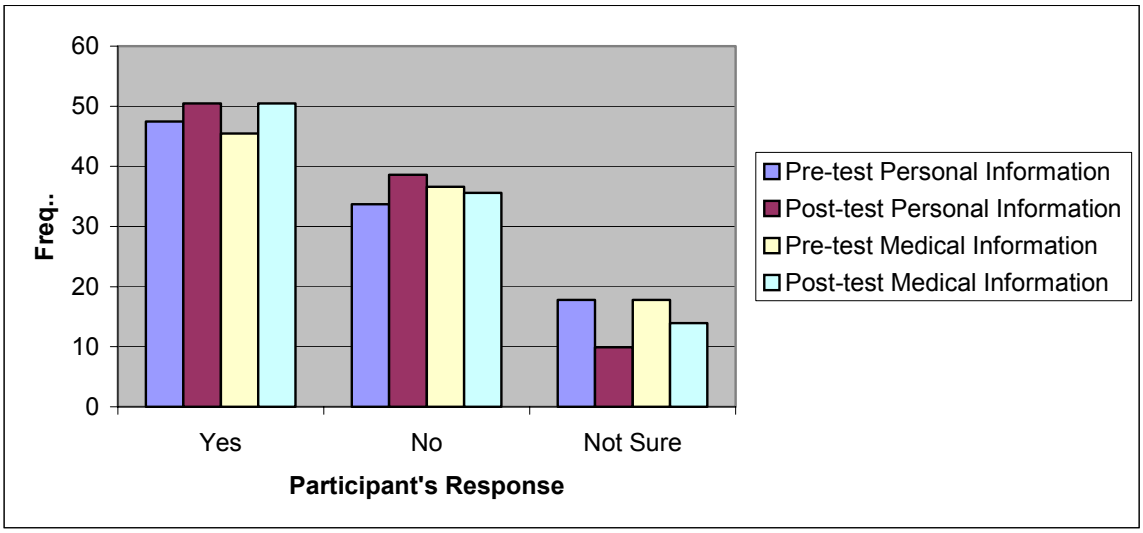

Figure 15 - Data that has been accepted to be stored on a RFID tag

The other scenario is that of the responses that indicate that the participants are clearly against this data being added onto the tag. These include Family Details, Favourite Things, Cultural Background, Employment History, Tax File Number (TFN) and Banking Details. A graph of the post-test responses can be found in Figure 16.

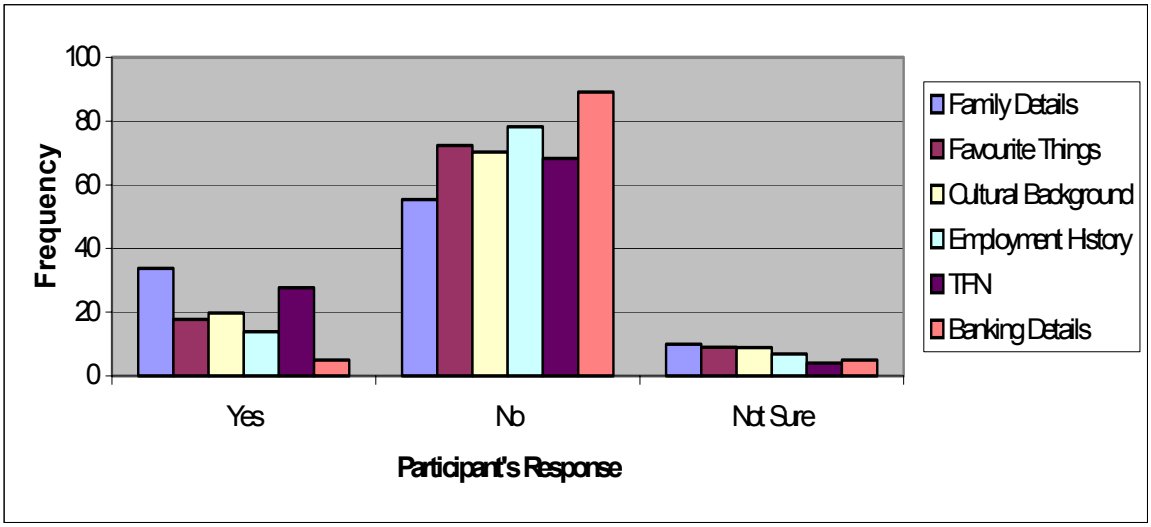

Figure 16 - Data that has not been accepted to be stored on a RFID tag

5.4 Discussion

The purpose of the survey was to gain an indication of society's opinion in regards to RFID tags. Firstly, a high majority (72.3%) of people were not willing to be implanted with an RFID tag. There was also a high level of concern over the implementation of a nation-wide identification scheme, which shows that society is not ready for such a scheme, which may or may not involve RFID transponders.

Several uses of the technology also showed a high level of concern over some of the uses of RFID tags. These included the tracking of money spending and shopping habits, as well as the monitoring of staff work habits and children's locations. There are some uses of the technology that showed a low level of concern including the monitoring of package location and the use of an automatic check at the supermarket. The uses with a high level of concern require the monitoring or tracking of an

individual, where as the uses with a low level of concern can aid consumers, but do not track or monitor actual people.

An underlying purpose of completing a pre-test / post-test designed survey was to see what effect education on the topic would have to the answers of the questions. This is because education about RFID tags is readily discussed throughout the literature (Section 2.2.1). The education of the topic brought about a varied change throughout the questions. Some responses did not change at all. For example the questions regarding the willingness of the participant to get implanted with an RFID tag and a commercial body collecting information over a time period showed very little, if no change in the results.

Other responses had a large change in results and these were typically, but not exclusively, questions that asked about the possible uses of RFID. For example the question that asked whether an RFID tag could be used to automatically identify a human had a change from 65.3% to 92.3%. The question regarding the responsibility of updating information showed a decline in the level of concern after the information was presented, which shows that education about the topic could allow greater adoption from the public. This indicates that although society has some fundamental ideas about what information they would or would not like collected about them, the actual knowledge about the potential uses and possibly even consequences needs to be improved before wide scale use of RFID can begin.

5.5 Conclusion

There were several notable results that arose from the survey's data. Firstly, the highest levels of concern were over the uses that were specifically related to the tracking or monitoring of individuals. Other results include that participants showed less concern over a government body collecting personal information than a commercial body. It was also found that it was important that only authorised personnel could access the information. Overall, the difference in results from the pre-test to the post-test results showed that education about the topic will change people's opinion, and therefore education about the topic is crucial for greater acceptance (Objective 3, Section 1.3).

6. Conclusion

6.1 Introduction

There are several aims of this paper. Firstly, there is a need to fill the gap in the literature, that being of the lack of in depth and conclusive papers that mention RFID privacy and security. In order to do this a content analysis was performed to create a succinct list of the most relevant concepts (Objective 1, Section 1.3). This was put forward in a narrative analysis where major conclusions were drawn (Objective 2, Section 1.3), and these results can be found in chapter 4. Secondly, an online survey was conducted in order to determine the level of awareness of the concepts surrounding RFID privacy and security (Objective 3, Section 1.3), and these results were presented and discussed in chapter 5.

6.2 Principal Conclusions and Implications

There were several key results from the content analysis. The first of these is that the five major themes are privacy, reader, technology, information and authentication. Security was not listed as a major theme, however it was an underlying concept to all five themes.

The frequency and relationship matrices revealed many key links as well as some that were noticeably missing. The first of two main missing links was that of privacy and industry, which implies that the protection of privacy in industry has not yet been

researched in depth. The second is the missing link of security and consumer, which indicates that RFID transponders are not considered a security threat to people.

Links that were identified include the link from security to system. This explains the need to make sure that unauthorised people are not able to access the system, and that all transmissions through the system are secure. There was also a direct link from privacy to consumers, which coincides with the previous noted missing link of privacy to industry. This indicates that privacy is a problem specifically for individuals and not for corporations.

The last two links match up with the findings from the survey. Privacy is linked to technology, and technology is linked to tracking. The survey indicates that there is high concern over uses of RFID technologies that involve the tracking and monitoring of individuals. The level of concern over uses of the technology that do not involve the tracking of individuals is much lower. This shows that tracking is a major aspect of privacy, and that this is an aspect of the technology that will need to be addressed if the privacy concerns are to be repressed.

Other results from the survey indicate that many respondents were not willing to be implanted with RFID tags. There is also a high level of concern over a national identification scheme. This shows that the public would not be willing at the moment to accept such as scheme using RFID transponders, and that maybe education about the topic will lead to greater acceptance.

These findings are relevant to many people throughout all parts of the world. Firstly, it is relevant to the many researchers that are currently studying this topic. More importantly, as this technology is developing and becoming readily available, this research could become relevant to everyone. If RFID was implanted on a wide scale basis, then this paper could answer many questions about the technology.

6.3 Future Research

There are multiple recommendations for future research that can arise from this paper. The research that has been done in this paper could be completed on a wider scale. For example, more articles could be added to the content analysis selection, and the survey could be completed on a worldwide basis over a period of time.

As previously mentioned there were two missing links in the research. The first of these is the link from security to consumer, and the second of these is from privacy to industry. These aspects need to be researched in depth, as the research about these topics is limited. If the links are missing because there are no links, then this itself could be researched to find out why there are not links.

Other aspects that could be researched further in depth include any of the links that were mentioned in the narrative analysis in Section 4.4. In particular the link between privacy and tracking could be examined to a greater extent, as well as the different security aspects that need to be addressed in implementing an RFID system.

6.4 Conclusion

The completion of the two methodologies, the content analysis and the survey, have satisfied all the objectives mentioned in Section 1.3. The content analysis indicated that security was specifically linked to the technology, and that the technology allowed the possible breach of privacy through the ability of the technology to track individuals. The survey results indicated that the level of knowledge of RFID transponders is limited, and therefore the respondents were not willing to accept the technology. Ultimately, further education of the public will need to be conducted in order for the wide scale implementation of RFID tags to be introduced into society successfully.

7. Reference List

Anderson, T & Kanuka, H 2003, *e-Research Methods, Strategies and Issues*, Pearson Education Inc., USA.

Anonymous 2003, 'Security friend and foe', *Industrial Engineer, Norcross*, vol. 35, no. 11, p. 39.

Berthiaume, D 2005, 'A PRIVATE MATTER', *Chain Store Age*, p. 48A.

Cavoukian, A 2004, *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*, Information and Privacy Commissioner / Ontario.

Czaja, R & Blair, J 2005, *Designing Surveys. A Guide to Decisions and Procedures*, 2 edn, Sage Publications, Inc., Thousand Oaks, California.

Garfinkel, SL, Juels, A & Pappu, R 2005, 'RFID privacy: an overview of problems and proposed solutions', *Security & Privacy Magazine, IEEE*, vol. 3, no. 3, pp. 34-43.

Gatty, B 2005, 'Off To A Good Start With The Feds', *Food Logistics*, no. 76, p. 12.

Germain, JM 2003, 'RFID Tags and the Question of Personal Privacy', *www.TechNewsWorld.com*, 11/18/03.

Good, N, Molnar, D, Urban, JM, Mulligan, D, Miles, E, Quilter, L & Wagner, D 2004, 'Radio frequency Id and privacy with information goods', in *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, ACM Press, Washington DC, USA, pp. 41-2.

Harris, S 2005, 'It's a Tag, Tag, Tag, Tag World', *Government Executive*, vol. 37, no. 4, pp. 17-8.

Jones, P, Clarke-Hill, C, Shears, P, Comfort, D & Hillier, D 2004a, 'Radio Frequency Identification in the UK: Opportunities and Challenges', *International Journal of Retail & Distribution Management*, vol. 32, no. 3, pp. 163-71.

---- 2004b, 'Radio Frequency Identification in Retailing and Privacy and Public Policy Issues', *Management Research News*, vol. 32, no. 8, pp. 46-56.

Juels, A & Brainard, J 2004, 'Soft Blocking: Flexible Blocker Tags on the Cheap', paper presented to 2004 ACM Workshop on Privacy in the Electronic Society, Washington DC, USA.

Juels, A, Rivest, RL & Szydlo, M 2003, 'The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy', paper presented to 10th ACM Conference on Computer and Communications Security, Washington D.C, USA.

Leedy, PD & Ormrod, JE 2005, *Practical Research: Planning and Design*, 8th edn, Pearson Merrill Prentice Hall, Upper Saddle River, New Jersey.

Leximancer 2004, *Leximancer Manual*.

McGinity, M 2004, 'RFID: Is This Game of Tag Fair Play?' *Communications of the ACM*, vol. 47, no. 1, pp. 15 - 22.

Messmer, E 2004, 'RFID is Really Getting Under People's Skin', *Network World*, vol. 22, no. 13, pp. 1 - 2.

Michael, K 2003, 'Trends in the selection of automatic identification technology in electronic commerce applications", in N. Cerpa & P. Bro (eds.), *Building society through e-commerce: e-Government, e-Business and e-Learning*, Chile: University of Talca, pp. 132 - 152.

---- 2004, "Location-based services: a vehicle for IT&T convergence" in K. Cheng et al. (eds), *Advances in e-Engineering and Digital Enterprise Technology*, Professional Engineering Publishing, London, pp. 467-477.

Michael, K. & Masters, A. (2004). "Applications of human transponder implants in mobile commerce", *The 8th World Multiconference on Systemics, Cybernetics and Informatics* (18-21st July: Orlando, Florida), vol. V, pp. 505-512.

Michael, K & Michael, M.G. 2004, "The social, cultural, religious and ethical implications of automatic identification", *Proceedings of the Seventh International Conference in Electronic Commerce Research* (10-13th June: Dallas, Texas), pp. 433-450

---- 2005, 'Microchipping People The Rise of the Electrophorus', *Quadrant*, vol. 59, no. 3, pp. 22-33.

Millar, SA 2004, 'RFID & EPC Systems', *Paper, Film and Foil Converter*, vol. 78, no. 11, p. 16.

---- 2005, 'RFID: Emerging Policy Issues', *Paper, Film and Foil Converter*, vol. 79, no. 4, p. 32.

Molnar, D & Wagner, D 2004, 'Privacy and Security in Library RFID: Issues, Practices and Architectures', paper presented to Computer and Communications Security, Washington DC, USA.

Ni, L, Liu, Y, Lau, Y & Patil, A 2004, 'LANDMARC: Indoor Location Sensing Using Active RFID', *Wireless Networks*, vol. 10.

Plitcha, G 2004, *Accommodating RFID Technology and Expectations of Privacy: An Examination and Proposed Guidelines*, Electronic Privacy Information Centre.

Pottie, GJ 2004, 'Privacy in the Global E-Village', *Communications of the ACM*, vol. 47, no. 2, pp. 21-3.

Ranasinghe, DC, Engels, DW & Cole, PH 2004, 'Security and privacy solutions for low-cost RFID systems', paper presented to Intelligent Sensors, Sensor Networks and Information Processing Conference, 14-17 Dec. 2004.

Saunders, M, Lewis, P & Thornhill, A 2003, *Research Methods for Business Students*, Pearson Education Limited, Harlow, England.

Sarma, S 2004, 'Integrating RFID', *Queue*, vol. 2, no. 7, pp. 50 - 7.

Smith, L 2005, 'RFID Report', *The Humanist*, vol. 65, no. 3, p. 37.

VeriChip Company - Privacy Policy, viewed 23/10/2005 <http://www.verichipcorp.com/content/company/privacy>.

Want, R 2004, 'The Magic of RFID', *Queue*, vol. 2, no. 7.

Weber, RP 1985, *Basic Content Analysis*, Quantitative Applications in the Social Sciences, Sage Publications, Inc., Beverly Hills, California.

8. Appendices

8.1 Appendix 1 – Content Analysis Article List

Albrecht, K 2002, 'Supermarket Cards: The Tip of the Retail Surveillance Iceberg', *Denver University Law Review*, vol. 79, no. 4, pp. 534-9 and 58-68.

Alfonsi, BJ 2004, 'Privacy debate centers on radio frequency identification', *Security & Privacy Magazine, IEEE*, vol. 2, no. 2, p. 12.

Alippi, C & Vanini, G 2004, 'A genetic-based application oriented approach to optimize RFID-like passive sensor devices for homeland security', paper presented to Proceedings of the 2004 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, 2004.

Anonymous 2005, 'New Covert Taggant Formulation Prevents Counterfeit RFID Tags', *Paint & Coatings Industry*, vol. 21, no. 7, p. 14.

'Another link in the chain', 2004, *Card Technology Today*, vol. 16, no. 4, pp. 11-2.

Bansal, R 2004, 'Now you see it and now you don't [RFID technology]', *Microwave Magazine, IEEE*, vol. 5, no. 4, pp. 32-4.

Berthiaume, D 2005, 'A PRIVATE MATTER', *Chain Store Age*, p. 48A.

Blackman, A 2005, 'Personal Business: Wave Goodbye To Magnetic Strips On Cards', *Wall Street Journal*, Jul 31, 2005, p. 4.

Cavoukian, A 2004, *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*, Information and Privacy Commissioner / Ontario.

Claburn, T & Hulme, GV 2004, 'RFID's Security Challenge', *Security pipeline*, November 15, 2004.

'Drug Safety; Security implemented to combat counterfeit drugs', 2005, *Medical Devices & Surgical Technology Week*, p. 193.

EPCglobal 2004, *Overview of Design, Benefits, & Security*, EPC Global Inc., New Jersey.

Gao, X, Xiang, Z, Wang, H, Shen, J, Huang, J & Song, S 2004, 'An approach to security and privacy of RFID system for supply chain', paper presented to E-Commerce Technology for Dynamic E-Business, 2004. IEEE International Conference.

Garfinkel, SL, Juels, A & Pappu, R 2005, 'RFID privacy: an overview of problems and proposed solutions', *Security & Privacy Magazine, IEEE*, vol. 3, no. 3, pp. 34-43.

Germain, JM 2003, 'RFID Tags and the Question of Personal Privacy', *www.TechNewsWorld.com*, 11/18/03.

Gittlen, S 2005, 'The life and times of an RFID chip', *Network World*, vol. 22, no. 30, p. 41.

Glover, T 2005, 'The end of privacy is nigh as use of radio chips spread', *Sunday Business*, May 29, 2005, p. 1.

Good, N, Molnar, D, Urban, JM, Mulligan, D, Miles, E, Quilter, L & Wagner, D 2004, 'Radio frequency Id and privacy with information goods', in *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, ACM Press, Washington DC, USA, pp. 41-2.

'Integrated Engineering: Integrated Engineering introduces anti- eavesdropping device; Securing privacy for e-Passports', 2005, *M2 Presswire*, p. 1.

Juels, A & Brainard, J 2004, 'Soft blocking: flexible blocker tags on the cheap', paper presented to Proceedings of the 2004 ACM workshop on Privacy in the electronic society, Washington DC, USA.

Juels, A, Rivest, RL & Szydlo, M 2003, 'The blocker tag: selective blocking of RFID tags for consumer privacy', in *Proceedings of the 10th ACM conference on Computer and communications security*, ACM Press, Washington D.C., USA, pp. 103-11.

Knospe, H & Pohl, H 2004, 'RFID security', *Information Security Technical Report*, vol. 9, no. 4, pp. 39-50.

Kumagai, J & Cherry, S 2004, 'Sensors and Sensibility', *Spectrum, IEEE*, vol. 41, no. 7, pp. 22-6, 8.

Lager, M 2005, 'RFID: Beyond Concept', *Customer Relationship Management*, vol. 9, no. 8, p. 14.

Lyman, J 2005, 'Researchers Chip Away at RFID security', *www.TechNewsWorld.com*, 31/01/05.

Mathieson, S 2004, 'Vive la difference, while you can', *Infosecurity Today*, vol. 1, no. 6, pp. 20-2.

McGinity, M 2004, 'RFID: is this game of tag fair play?' *Commun. ACM*, vol. 47, no. 1, pp. 15-8.

Messmer, E 2005, 'Black Hat event highlights RFID and VoIP security threats', *Network World*, vol. 22, no. 30, p. 14.

Molnar, D & Wagner, D 2004, 'Privacy and security in library RFID: issues, practices, and architectures', in *Proceedings of the 11th ACM conference on Computer and communications security*, ACM Press, Washington DC, USA, pp. 210-9.

Mueller, M 2005, 'New applications for contactless technology', *Card Technology Today*, vol. 17, no. 4, pp. 10-1.

Offman, C 2005, 'Inside information About 1,000 people - including doctors, a police chief and nightclubbers - have now had a microchip the size of a rice grain injected into their arms. However, sceptics are alarmed by the device that is turning people into walking databanks', *Financial Times*, Jul 9, 2005, p. 22.

Park, J-S, Kim, Y-l & Lee, Y-J 2005, 'Security considerations for RFID technology adoption', paper presented to The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005.

Perakslis, C & Wolk, R 2005, 'Social acceptance of RFID as a biometric security method', paper presented to 2005 International Symposim on Technology and Society, 2005. Weapons and Wires: Prevention and Safety in a Time of Fear. ISTAS 2005.

Plitcha, G 2004, *Accommodating RFID Technology and Expectations of Privacy: An Examination and Proposed Guidelines*, Electronic Privacy Information Centre.

Potter, B 2005, 'RFID: misunderstood or untrustworthy?' *Network Security*, vol. 2005, no. 4, pp. 17-8.

Pottie, GJ 2004, 'Privacy in the global e-village', *Commun. ACM*, vol. 47, no. 2, pp. 21-3.

Ranasinghe, DC, Engels, DW & Cole, PH 2004, 'Security and privacy solutions for low-cost RFID systems', paper presented to Intelligent Sensors, Sensor Networks and Information Processing Conference, 14-17 Dec. 2004.

Saito, J & Sakurai, K 2005, 'Grouping Proof for RFID Tags', paper presented to 19th International Conference on Advanced Information Networking and Applications, 2005., 25-30 March, 2005.

Schindler, E 2003 'Location, location, location ', *netWorker* vol. 7 no. 2 pp. 11-4

Shimizu, N, Yagio, R & Saito, M 2005, 'A Study of Information Services Based on Personal Belongings', paper presented to 19th International Conference on Advanced Information Networking and Applications, 2005., 25-30 March, 2005.

Staake, T, Thiesse, F & Fleisch, E 2005, 'Extending the EPC network: the potential of RFID in anti-counterfeiting', in *Proceedings of the 2005 ACM symposium on Applied computing*, ACM Press, Santa Fe, New Mexico, pp. 1607-12.

Takaragi, K, Usami, M, Imura, R, Itsuki, R & Satoh, T 2001, 'An ultra small individual recognition security chip', *Micro, IEEE*, vol. 21, no. 6, pp. 43-9.

Want, R 2004 'The magic of RFID ', *Queue* vol. 2 no. 7 pp. 40-8

Weinstein, R 2005, 'RFID: A Technical Overview and Its Application to the Enterprise', *IT Professional*, vol. 7, no. 3, pp. 27 - 33.

Weis, SA 2004, 'RFID Privacy Workshop', *Security & Privacy Magazine, IEEE*, vol. 2, no. 2, pp. 48-50.

---- 2005, 'Security Parallels between People and Pervasive Devices', paper presented to TheThird IEEE International Conference on Pervasive Computing and Communications Workshops, 2005. (PerCom 2005 Workshops).

Weiss, A 2003, 'Me and my shadow', *netWorker*, vol. 7, no. 3, pp. 24-30.

Writer, DRSLA 2005, 'Commentary: Radio Frequency ID: Revisiting a privacy alert', *The Daily Record*, Jun 6, 2005, p. 1.

Yasuura, J 2003, 'Towards the Digitally Named World - challenges for new social infrastructures based on information technologies', paper presented to Proceedings of the Euromicro Symposium on Digital System Design, 2003.

Zalud, B 2005, 'California RFID Day Dreaming', *Security*, vol. 42, no. 8, p. 74.

8.2 Appendix 2 – Ranked Concept List

Entities:

Concept	Absolute Count	Relative Count
Rfid	2333	100%
tags	2097	89.8%
privacy	632	27%
reader	629	26.9%
technology	553	23.7%
system	537	23%
information	511	21.9%
security	416	17.8%
data	403	17.2%
product	337	14.4%
tracking	329	14.1%
number	304	13%
consumer	291	12.4%
devices	221	9.4%
items	220	9.4%
read	218	9.3%
applications	218	9.3%
chip	214	9.1%
time	205	8.7%
individual	204	8.7%
require	202	8.6%
cards	174	7.4%
standards	173	7.4%
supply	169	7.2%
identification	169	7.2%
issues	166	7.1%
company	165	7%
code	160	6.8%
access	160	6.8%
including	155	6.6%
unique	152	6.5%
radio	149	6.3%
year	149	6.3%
retail	147	6.3%
Epc	146	6.2%
range	146	6.2%
concerns	145	6.2%
blocker	144	6.1%
provide	143	6.1%
authentication	143	6.1%
protocol	142	6%
should	136	5.8%
key	136	5.8%
database	136	5.8%

public	132	5.6%
personal	131	5.6%
problem	131	5.6%
cost	130	5.5%
store	129	5.5%
services	120	5.1%
based	117	5%
people	117	5%
control	115	4.9%
developed	114	4.8%
available	114	4.8%
approach	114	4.8%
world	109	4.6%
serial	106	4.5%
reading	104	4.4%
smart	103	4.4%
private	103	4.4%
passive	102	4.3%
frequency	101	4.3%
industry	101	4.3%
management	100	4.2%
implementation	100	4.2%
designed	97	4.1%
scheme	97	4.1%
small	96	4.1%
protection	96	4.1%
power	96	4.1%
work	94	4%
bar	94	4%
goods	94	4%
identity	92	3.9%
objects	91	3.9%
person	88	3.7%
communication	88	3.7%
paper	86	3.6%
library	86	3.6%
level	86	3.6%
inventory	84	3.6%
process	83	3.5%
active	82	3.5%
large	81	3.4%
memory	81	3.4%
identify	80	3.4%
stores	80	3.4%
potential	80	3.4%
means	79	3.3%
secure	79	3.3%
important	76	3.2%
government	76	3.2%
business	75	3.2%

place	73	3.1%
network	73	3.1%
attached	73	3.1%
commercial	73	3.1%
computer	73	3.1%
embedded	73	3.1%
electronic	72	3%
customer	72	3%
stored	72	3%
specific	72	3%
current	71	3%
future	69	2.9%
encryption	68	2.9%
set	68	2.9%
today	67	2.8%
case	67	2.8%
user	67	2.8%
protect	66	2.8%
antenna	65	2.7%
policy	63	2.7%
similar	63	2.7%
order	63	2.7%
size	62	2.6%
distance	61	2.6%
physical	61	2.6%
Wal-mart	60	2.5%
low	60	2.5%
ability	60	2.5%
bits	60	2.5%
few	59	2.5%
present	59	2.5%
back	59	2.5%
pic	58	2.4%
address	57	2.4%
methods	56	2.4%
Epcglobal	56	2.4%
solutions	56	2.4%
research	56	2.4%
addition	55	2.3%
support	55	2.3%
manufacturers	55	2.3%
Us	54	2.3%
market	54	2.3%
help	54	2.3%
software	53	2.2%
easily	53	2.2%
end	52	2.2%
digital	51	2.1%
called	51	2.1%
real	50	2.1%

law	50	2.1%
related	50	2.1%
national	49	2.1%
global	49	2.1%
human	48	2%
technical	48	2%
credit	47	2%
deployment	47	2%
contactless	45	1.9%
wireless	45	1.9%
theft	41	1.7%
Auto-id_Center	41	1.7%
computing	38	1.6%
note	37	1.5%
Ieee	37	1.5%
Electronic_Product_Code	36	1.5%
records	36	1.5%
article	35	1.5%
report	34	1.4%
Massachusetts_Institute_Of_Technology	32	1.3%
project	27	1.1%

8.3 Appendix 3 – Highlighted Relationship Matrix

Entity	RFID	tags	privacy	reader	technology	information	system	data	security	tracking	product	number	consumer
RFID	2333	9	3	3	3	3	3	2	2	2	2	2	2
tags	10	2097	3	3	3	3	3	2	2	2	2	2	2
privacy	10	9	632	3	4	3	3	2	3	3	2	1	3
reader	10	10	3	629	2	3	3	2	2	1	2	2	1
technology	10	9	4	2	553	3	3	2	2	2	2	1	2
information	10	10	3	3	3	511	4	3	2	2	3	2	2
system	10	10	3	3	3	3	537	2	3	2	2	2	2
data	10	10	3	3	3	4	3	403	2	2	2	2	2
security	10	9	4	3	3	3	4	2	416	2	2	2	1
tracking	10	10	4	2	5	3	3	2	2	329	3	2	3
product	10	10	3	3	3	4	3	2	2	3	337	2	3
number	10	10	2	4	2	3	3	3	2	2	3	304	1
consumer	10	10	6	3	4	3	3	2	1	3	3	1	291

Table 8 - Coloured Highlighted Matrix

8.4 Appendix 4 – Survey Questions

Subject: Research Honours

Subject Code: IACT441

Instruction: Please read all instructions carefully. Please note that this survey is for the research of , and not for
.

Hello, and thankyou for responding to my request for help in completing my Honours Thesis. You will find the survey below, but there are some pieces of information that are important to understand before starting the survey.

This survey is about Radio Frequency Identification (RFID) tags. If you have no prior knowledge of this topic, then this is perfectly fine, as it is part of the survey's aim to gather knowledge about society's understanding of the topic. If you do not know the answer to the question, please answer it as best as you can, and move on to the next question. Please note that at anytime you are free to cease completing the survey, and that for any individual question you have the option of not answering that question. Taking either of these options will not affect the outcome of the research. This survey is completely anonymous.

The Survey consists of 4 parts. Their names and purpose are listed below.

• Section 1 – General Information Questions
This section asks general background questions, which includes your age and gender etc.

• Section 2 – RFID Specific Questions
This section asks questions specific to RFID and it's uses to gauge what is already known about the topic.

• Section 3 – Information about RFID
This section provides factual information about RFID. There are no questions, you will just be asked to have read the information carefully.

• Section 4 – RFID Specific Questions
This section asks the same questions in section 2, to see if education about the topic changes your opinion about the topic.

I also ask you to pass on the email, and the link to the survey to all

of your friends, families and co-workers so that they can also complete the survey if they would like to. Obviously, the more responses to the survey the better the research will be. The only condition is that all participants must be at least 18 years of age.

Below is the Ethics Statement, and by clicking the "I Agree" option, you agree to all of the guidelines listed below. If you do not agree with the Ethics Statement, then unfortunately you can not complete the survey, and I would ask you now to close down this window, and continue with your day.

Thankyou once again for your time,
Kirsty Johnston

Ethics Statement

I have been asked to complete the survey written to assist Kirsty Johnston to finish her Honours Thesis on the topic of Radio Frequency Identification (RFID) tags as part of a Bachelor of Information & Communication Technology degree, supervised by Dr Katina Michael, in the Faculty of Informatics at the University of Wollongong.

I acknowledge that, if I consent to participate in this research, I will be asked to undertake a online survey lasting approximately 15 minutes. The survey has different sections, which I have been made aware of. I also understand that I have the option at any time not to answer a particular question/s, and that this will not affect the outcome of the survey. I acknowledge that I must be at least 18 years of age to complete this survey.

I am aware that the data collected from my participation will be used for a thesis and possibly journal publications, and I consent for it to be used in that manner.

I understand that my participation in this research is voluntary, I am free to refuse to participate, and I am free to withdraw from the research at any time. My refusal to participate or withdrawal of consent will not affect my treatment or relationship with the University of Wollongong.

If I have any enquiries about the research, I can contact
Jor her supervisor, , on
.

- ☐ I Agree
- ☐ I Disagree

Section 1 – General Information Questions

Q1. What is your Gender?

- ☐ Male
- ☐ Female
- ☐ I choose not to answer this question

Q2. What is your Age?

- ☐ 18-21
- ☐ 22-29
- ☐ 30-39
- ☐ 40-54
- ☐ 55-64
- ☐ 65+
- ☐ I choose not to answer this question

Q3. Which of the following options best describes your level of education?

- ☐ Did not Complete School
- ☐ Completed Secondary Schooling
- ☐ Apprenticeship Completed
- ☐ Tertiary Education Completed
- ☐ University Degree Completed
- ☐ None of the above Apply to my situation
- ☐ I choose not to answer this question

Q4. Which of the following options best describes your current employment status?

- ☐ Unemployed
- ☐ Studying
- ☐ Casual
- ☐ Part time
- ☐ Full time
- ☐ Retired
- ☐ I choose not to answer this question

Q5. Which of the following best describes your average household income this year?

- ☐ $0 - $20000
- ☐ $20000 - $40000
- ☐ $40000 - $60000
- ☐ $60000 - $80000
- ☐ $80000 - $100000
- ☐ $100000+
- ☐ I choose not to answer this question

Q6. Are you working or studying in an IT related field?

- ☐ Yes
- ☐ No
- ☐ I choose not to answer this question

Q7. What is your Religion?
Please type NA if you choose not to answer this question.

Q8. In which country did you spend most of your childhood?

Please type NA if you choose not to answer this question.

Q9. What is your cultural upbringing?
Please type NA if you choose not to answer this question.

Section 2 - RFID Specific Questions

Q10. Before being asked to complete this survey, did you know what an RFID tag was?

- Yes
- Had Some Idea
- No
- I choose not to answer this question

Q11. Do you think that RFID tags are being implanted in humans today?

- Yes
- No
- Not Sure
- I choose not to answer this question

Q12. Would you be willing to be implanted with a RFID transponder in your body?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

Q13. For each of the following, Do you think that the task can be completed by a RFID tag?

a. Automatic Identification of a Package?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

b. Automatic Identification of a Human?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

c. Measuring the temperature of the object (Human/Animal or inanimate) of which it is implanted in?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

d. Testing the blood of a Human or Animal to find out the iron levels?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

e. Automatic unlocking of cars?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

f. Purchasing items without having to go through a check out?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

Q14. How concerned are you with the following uses of RFID tags?

a. Monitoring package location?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

b. Monitoring children's location?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

c. Automatic checkout at the supermarket?

- ☐ Extremely Concerned

- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

d. Monitoring staff work habits?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

e. Tracking Crime Suspects?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

f. Tracking shopping habits?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

g. Tracking Money Spending?

- ☐ Extremely Concerned
- ☐ Very Concerned

- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

h. Automatic Patient Identification?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q15a. How concerned would you be with a government body collecting personal information over a long time period?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q15b. How concerned would you be with a commercial body collecting personal information over a long time period?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q16. How concerned would you be if someone else had the control and the responsibility of updating your information?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q17. How concerned would you be that only authorised personnel have access to the RFID system?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q18. How concerned would you be if the government chose to implement a nation wide identification scheme using RFID tags?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q19. Which of the following data do you accept being collected by the RFID system?

a. Personal Details (Name, Birth Date, Address, Phone Number etc)

- ☐ Yes
- ☐ No

- ☐ Not Sure
- ☐ I choose not to answer this question

b. Family Details (Mother's and Father's Details etc.)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

c. Medical Information (Medical Healthcare Number, Health Insurance Provider, Allergies, Current Health Conditions - Illnesses etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

d. Cultural Background (Nationality, Religion etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

e. Tax File Number / Social Security Number

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

f. Employment Details (Education Level, Work History etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure

- ☐ I choose not to answer this question

g. Banking Details (Credit Card Number, Bank Account Numbers, Bank Balances etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

h. Favourite Things (Foods, Colour, Clothes etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

Section 3 - RFID Specific Questions

Please read the following information regarding RFID technology carefully.

Radio Frequency Identification (RFID) is a technology that is becoming readily available. It is currently used to identify cats and dogs, as well as tracking inanimate objects throughout the world by using the Electronic Product Code (EPC) standard. Trials are currently underway in various parts of the world that involve the implantation of RFID transponders in humans.

RFID tags can be defined as a device that contains a small integrated circuit and an antenna, which when queried can send out a unique serial number so that it, and the article which carries it, can be identified. The major difference between a RFID tag and a barcode is that barcodes require line of sight in order to read the information, whereas RFID tags do not.

There are several services that RFID tags can offer, including assisting in an emergency where a patient could be identified by the implant, and then give access to the patient's medical records to the relevant medical personnel. Other services that could be offered with the use of RFID in mobile commerce when integrated with e-

security, e-banking and e-health include a lifetime identifier, banking, biosensors, law enforcement, crime prevention, the monitoring of employees, and as an alternative to military dog tags. Modern courier companies use this technology to monitor where packages are at any give time through location-based services.

Q20. I have read the information presented in the above reading.

- ☐ Yes
- ☐ No
- ☐ I choose not to answer this question

Section 4 - RFID Specific Questions

The same questions in Section 2 will now be presented again for you to re-answer.

Q21. Do you think that RFID tags are being implanted in humans today?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

Q22. Would you be willing to be implanted with a RFID transponder in your body?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

Q23. For each of the following, Do you think that the task can be completed by a RFID tag?

a. Automatic Identification of a Package?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

b. Automatic Identification of a Human?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

d. Testing the blood of a Human or Animal to find out the iron levels?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

e. Automatic unlocking of cars?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

f. Purchasing items without having to go through a check out?

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

Q24. How concerned are you with the following uses of RFID tags?

a. Monitoring package location?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

b. Monitoring children's location?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

c. Automatic checkout at the supermarket?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

d. Monitoring staff work habits?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

e. Tracking Crime Suspects?

- ☐ Extremely Concerned

- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

f. Tracking shopping habits?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

g. Tracking Money Spending?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

h. Automatic Patient Identification?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q25a. How concerned would you be with a government body collecting personal information over a long time period?

- ☐ Extremely Concerned

- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q25b. How concerned would you be with a commercial body collecting personal information over a long time period?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q26. How concerned would you be if someone else had the control and the responsibility of updating your information?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q27. How concerned would you be that only authorised personnel have access to the RFID system?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q28. How concerned would you be if the government chose to implement a nation wide identification scheme using RFID tags?

- ☐ Extremely Concerned
- ☐ Very Concerned
- ☐ Slightly Concerned
- ☐ Little Concern
- ☐ No Concern
- ☐ I choose not to answer this question

Q29. Which of the following data do you accept being collected by the RFID system?

a. Personal Details (Name, Birth Date, Address, Phone Number etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

b. Family Details (Mother's and Father's Details etc.)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

c. Medical Information (Medical Healthcare Number, Health Insurance Provider, Allergies, Current Health Conditions - Illnesses etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

d. Cultural Background (Nationality, Religion etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

e. Tax File Number / Social Security Number

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

f. Employment Details (Education Level, Work History etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

g. Banking Details (Credit Card Number, Bank Account Numbers, Bank Balances etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

h. Favourite Things (Foods, Colour, Clothes etc)

- ☐ Yes
- ☐ No
- ☐ Not Sure
- ☐ I choose not to answer this question

Thankyou for taking the time to complete my survey.

Please click the submit button to submit your results.

Please note that the survey will not allow you to submit unless all questions are answered. Please make sure that you have done this. If you have chosen not to answer a question, please make sure that you have selected the I choose not to answer this question option, or that NA has been typed into the appropriate box.

I have read all the instructions given, and have answered this survey as truthfully as possible and to the best of my ability.

- ☐ Yes
- ☐ No
- ☐ I choose not to answer this question

8.5 Appendix 5 – Ethics Approval Form

Please see print copy for Appendix 5