

https://dspace.org/

Ethics, autonomy, privacy and RFID technology

Bisschoff, Runette

2022
https://hdl.handle.net/10539/34088

Downloaded from a DSpace repository. https://dspace.org/

ETHICS, AUTONOMY, PRIVACY AND RFID TECHNOLOGY

by

Runette Bisschoff 1302419



A Research Report submitted to the Faculty of Humanities, University of the Witwatersrand, Johannesburg, in partial fulfilment of the requirements for the degree of

Master of Arts

Applied Ethics for Professionals UNIVERSITY OF THE WITWATERSRAND

Johannesburg, April 2021

ABSTRACT

This paper examines the risk that subcutaneous micro-chips pose to privacy. I argue that although human RFID-SM's may pose a risk to informational privacy in their current state, they are being improved and made more secure. They should not be banned for uses where they contribute to the safety & security, autonomy, dignity and quality of life of people as per their specific needs or wants- especially where they can prevent more significant harm.

Acknowledgements

This research report would not have been possible without the help of the following people:

My supervisor Dr. Brian Penrose (now deceased)

I am thankful for his patience, guidance and support throughout the writing of this research report. His thorough, detailed comments was definitely one of his strong points for which he will be remembered for. It was a privilege to work with him.

My locum supervisor Dr Ashley Coates

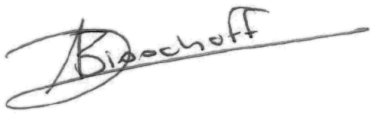
Thank you for stepping in and being willing to assist me in the completion of this research report.

To my family and friends

Thank you for your encouragement, constructive comments and discussions. The process of writing this research report has been a long and daunting challenge but in the end it was a very interesting and fulfilling journey. You were always there for me when I needed you.

DECLARATION

I declare that this research report is my own unaided work. It is submitted for the degree of Master of Arts, Applied Ethics for Professionals, in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any other degree or examination in any other university.



Runette Bisschoff

1302419

20 December 2021

TABLE OF CONTENTS

ABSTRACT 2

DECLARATION 3

1 Introduction: 1

2 RFID Technology and Its Uses: 6

2.1 Explanation of RFID Technology: 6

2.2 General Uses of RFID Technology: 10

3 Virtues of the Use of Human RFID-SM's: 13

3.1 Convenience: 14

3.1.1 Automation of Processes: 14

3.1.2 Uploading Small Documents to Your RFID-SM: 15

3.1.3 Replacing Luggables and Wearables with Implants: 16

3.2 Control (Tracking and Tracing): 19

3.2.1 Workplace: 19

3.2.2 Identification and Location Purposes after a Disaster or Death: 21

3.2.3 Long Term Care Facilities: 23

3.2.4 Inside a Hospital Environment: 25

3.3 Safety and Care: 26

3.3.1 Personalized Firearms: 26

3.3.2 VeriMed Project: 27

3.3.3 Monitoring Function: 32

3.3.4 Digital Identity 34

4 Autonomy, Coercion and RFID-SM Implants: 37

4.1 Autonomy and Coercion: 37
4.2 Possible Coercion in Different Sectors: 38
4.2.1 Parents and Guardians: 39
4.2.1.1 Children: 39
4.2.1.2 The Cognitively Impaired: 40
4.2.2 Workplace: 41
4.2.3 Commerce: 42
4.2.4 Government: 44
5 Unlimited Surveillance and Informational Privacy: 47
5.1 Informational Privacy: 47
5.2 The Impact of the Use of RFID-SM's on Unlimited Surveillance in Comparison to Other Privacy Invasive ICT: 48
5.2.1 Public Spaces: 48
5.2.2 Semi-Public Spaces: 51
5.2.2.1 Retail Establishments: 51
5.2.2.2 Workspaces 54
5.2.3 Private Spaces: 55
5.3 Big Data: 59
6 Illicit access to personal information: (threat to privacy by abuse) 62
6.1 The role of the use of RFID-SM's in illicit access to personal information: 62
6.1.1 Hacking: 63
6.1.2 Cloning: 66
6.1.3 Viral spread: 68

7 Final Comments/Justification: 70

8 Bibliography: 74

1 Introduction:

Humans live in a digital world where information communication technology (ICT) forms an integral part of their daily lives. ICT makes possible a life of convenience and global connectedness that they have become accustomed to and prefer not to live without. The original intent of ICT developers is usually not to harm users or to invade their privacy but to make life easier and more effective for everybody.

According to Natasha Lomas, ICT is a morally neutral tool, and protection should be around ICT usage and not the technology per se.

> Technology is neither good nor bad, it is a tool. However hammers are tools too. They are wonderful for pounding in nails. That doesn't mean that someone can't pick up a hammer and use it to commit murder. We have laws to say that one shouldn't murder; we don't specialize the laws to call out hammers. Similarly, the laws surrounding privacy need to be laws about data and usage, not about the technology (Lomas, 2015).

The "ethical dilemma" humans are currently facing with ICT regarding the collection, storage, analysis, and use of personal information/data is that harm due to personal information abuse is a growing reality (Ferguson, Thornley & Gibb, 2016:544). There seems to be a global disrespect for other people's informational privacy (McCloskey, 1980:33). The use of privacy-invasive technology without the necessary security measures may make abuse and harm by those with malicious intent even easier.

Radio Frequency Identification (RFID) technology uses radio waves to communicate information from tags/micro-chips to compatible readers linked to computers. Readers interrogate tags in

their vicinity to answer the question: "Are you who or what you say you are?" So, the tag's primary purpose is accurate, automatic identification of the items they are attached to (Brown, 2016; van Hooijdonk, 2017).

RFID technology is commonly used with great success in many different sectors. In the past, the use of RFID technology was limited to objects, production processes, goods in transit and warehouses. Where consumers are under the impression that they do not come in contact with RFID technology regularly, they usually do not have privacy concerns about the use of the technology.

RFID tagging is not limited to production processes, transportation purposes, or warehouses within the supply chain anymore (Malone, 2006:1). Some retail outlets are now using RFID tags on item level within the retail outlet itself. Where this is the case, consumers can come in frequent contact with tagged objects. Consumers fear increased privacy invasion as commerce, government, employers and other interested parties may be able to accurately identify and track them, study their behaviour and habits, and build up profiles on them – especially where tags embedded in purchased items that are carried around or worn, remain activated or retain their ability to be re-activated after point of sale (Clarke & Flaherty, 2008, 516; Malone, 2006:3).

Implantable RFID subcutaneous micro-chips (hereafter “RFID-SM”) have been in existence for quite some time (Werber, Baggia & Znidarsic, 2018). For many years, household pets, wild animals, and farm animals have been and are still implanted for tracking and tracing purposes.

The biggest concern around loss of privacy is where the human body becomes the object of RFID use. In humans, first-generation RFID-SM devices act as identifiers and are used for access control, automation of processes, and safety & security within RFID enabled environments. RFID-

SM's are increasingly improved. Over and above being unique identifiers, they can now store, monitor, generate and communicate information automatically for specific predetermined purposes (Kaur, 2012:101). Latest generation RFID-SM devices can even serve as enablers for small computerized tasks.

The idea of implanting technology inside the human body, under the skin, makes most people shiver (Darrow, 2017). Fundamentalist Christian groups object passionately to RFID-SM as the “Mark of the Beast” (Church of the Great God, 2018). By portraying it as the “Mark of the Beast”, people fear that they will go straight to hell if they get an RFID-SM and use it as a device for payment and identification. People who consent to have RFID-SM's are receiving hate mail and videos containing hate speech from anti-RFID-SM activists (Heffernan, Vetere & Chang, 2016:56). Judaism and Islam disallow tattoos. They may have the same mindset towards human RFID-SM (Foster & Jaeger, 2008:47). Another concern around RFID-SM is the possibility of body enhancement. Some people feel that the augmentation or improvement of human bodies is immoral (Foster & Jaeger, 2007:28).

RFID technology is a controversial, privacy-invasive technology that can easily be abused without the necessary security measures in place. Some intellectual opponents and ethical critics of the technology are troubled with the concept of a human RFID-SM implant and want it to be banned. They are especially concerned about privacy invasive uses of the RFID-SM and the prospect of harvesting personal information from specific, identifiable individuals. They are also concerned about the possibility of abuse of the technology itself and abuse of the information harvested (Frith, 2020). This research report focuses on privacy, especially informational privacy issues around the use of human RFID-SM’s. Religious issues like the RFID-SM being the "Mark of the Beast" and the possibility of bodily enhancement may be mentioned but will not be discussed in detail as they fall outside this research report's scope.

Despite the controversies mentioned above, Bio-hackers (a group of people that experiment with technology to find ways through which the human body can be made more useful and life in itself can be made more convenient and better are continuing to implant themselves as well as other interested and consenting individuals with RFID-SM's as development progresses (Spector, 2014:4). While the more conservative person may experience the idea of implanting an RFID-SM under his/her skin to automate processes as sinister and frightening, Bio-hackers and self-experimenters thrive on the concept (Catherwood, Finlay & McLaughlin, 2015:1). Bio-hackers, grinders and self-experimenters find luggables (carry with you) as well as wearables (wear on your body or clothes) old-fashioned, irritating and uncomfortable. They prefer RFID-SM implants (Heffernan et al., 2016:55). The estimated number of people worldwide with RFID-SM's are between 50 000 and 100 000. There is a slowly growing but increasing community open to receiving and using RFID-SM's (Grauer, 2018).

At this stage, Sweden is at the forefront of human RFID-SM's, with more than 3 500 people that have them. Swedes feel comfortable with using RFID-SM's. They use them for gym membership identification and SJ, the Swedish rail company, allows commuters to register their RFID-SM's on SJ's RFID system and use it for commuting. As an almost cashless society, Swedes use the implants for payments (Billing, 2019; Gauttier, 2018:5). They have not had any criminal activities reported on RFID-SM use. That said, one must bear in mind that Swedes are financially well off, and most of them have a high level of computer literacy. Sweden has a meagre overall crime rate and a high level of trust towards the government and fellow citizens (Savage, 2018). The aforementioned is in line with Lomas' quote mentioned earlier (page 1). In the case of Sweden, Lomas is correct regarding the use of technology. This may however not be the case in other countries where the applicable infrastructure is not in place, where citizens may not have the correct mindset to make it work, where there is little trust between government, commerce and

citizens and even between citizens themselves, where crime is rife and where there is little to no respect for other people's privacy.

During their Tech Week in October 2019, the United Arab Emirates (UAE) announced their interest in RFID-SM's (Dass, 2019). There is still uncertainty over what uses they want to employ it for and whether they will use it. The UAE has the financial means to roll out sufficient standardized infrastructure to enable RFID-SM use throughout, e.g. a city like Dubai, backed by networked databases containing complete information on implantees. It will be interesting to see how this unfolds in the future, as Dubai's workforce includes many foreigners with different cultural and religious backgrounds from all over the globe.

In this report I will argue that although human RFID-SM's may pose a risk to informational privacy in their current state, they are being improved and made more secure. They should not be banned for uses where they contribute to the safety & security, autonomy, dignity and quality of life of people as per their specific needs or wants – especially where they can prevent more significant harm. Control and un-coerced informed consent (for implantation and removal) should always be in the hands of the innocent bearer, legal guardian or documented in a living will. We may find that some uses need more regulation than others, (e.g. government and workplace) to protect our moral right to privacy and informational privacy.

In Part 2 I will explain a bit more about how RFID works and the various uses to which it have been and can be put. Then, in Part 3 I will lay out some of what I see as the virtues of RFID technology. In Part 4 I will look more closely into autonomy and the possibility of coercion where people agree to be implanted with RFID-SM's. Part 5 is dedicated to Unlimited Surveillance and Informational Privacy. In part 6, I look at the possibility of abuse as well as security measures that can be put in place to curb abuse of RFID-SM's.

2 RFID Technology and Its Uses:

2.1 Explanation of RFID Technology:

As mentioned previously, RFID technology is a wireless technology that makes use of radio waves. Radio waves are the same waves that enable us to tune into and listen to radio and TV broadcasts. RFID radio waves travel silently and invisibly through shopping bags, walls, wood, backpacks, and wallets (Clarke et al., 2008: 518; McIntyre, Michael & Albrecht, 2015:13,15). As a safety precaution, there are backpacks and wallets available in the marketplace that can block out radio waves. Near Field Communication (NFC) is a subset of RFID. The major difference between RFID and NFC is that NFC has shorter read ranges than RFID. Most cell phones have NFC capability and can act as a reader for NFC tags. NFC tags can launch apps and share business cards with NFC enabled cell phones (Heffernan et al., 2016:54; Kaur, 2012:101).

The essential components for an RFID system are a tag, an antenna and a reader connected to a computer. Communication between a tag and a reader happens over a distance and does not require a line of sight (Lockton & Rosenberg, 2005:221). The reader's antenna contains a "demodulator that transforms the analogue radio data into digital data suitable for computer processing" (Lockton et al., 2005:222). At the bare minimum, a tag holds a unique 16-digit ID number assigned to that specific tag. This unique 16-digit ID number can be retrieved by a compatible, authorized reader and cross-referenced to a particular (linked) database that contains information on the tagged item (Foster et al., 2008:45). Tags and readers (scanners) are becoming smaller yet more powerful through Nanotechnology (Aubert, 2011:676). Tags can be read-only (data is fixed), or they can be read/write or re-writable (data can be re-written and modified 100 000 times) (Gadzheva, 2007:218; Gasson & Koops, 2013:252; Grauer, 2018).

"RFID's are typically found in three frequency families: low-frequency (125 and 134 kilohertz), high-frequency (13.56 megahertz), and ultra-high frequency (UHF) (800-915 megahertz)" (Grauer, 2018). The technology covers a broad range of interfaces, frequencies, protocols and devices, so each tag and reader is designed with unique capabilities and uses in mind. There are currently three different kinds of tags available on the market. They are active tags, semi-passive tags and passive tags. The read range depends on the type of tag, the task it needs to fulfil, the frequency used, the size of the antenna in the tag, and the antenna's size in the reader (McIntyre et al., 2015:15).

Active tags have batteries of their own to transmit their stored data constantly until the battery goes flat. The need for frequent replacement of batteries makes them more expensive than passive tags. Active tags have more memory (storage capacity) and faster processing time than passive tags (McIntyre et al., 2015:14). The read range of active tags can be anything between 100m and 3km. It is possible to do real-time tracking with active tags. It is also possible to track active tags via satellite.

Semi-passive tags, like active tags, have batteries of their own and a read range of 100m or more. The difference between active tags and semi-passive tags is that semi-passive tags remain inactive and only transmit data when they detect a signal from a compatible reader. Their batteries last longer, and their maintenance is cheaper than active tags (Gadzheva, 2007:218; McIntyre et al., 2015:14).

Passive tags are available in long read range and short read range (Zalud, 2016: 57). When used on objects, the long-range allows a read distance of around 10m to 30m. Passive tags have an almost limitless lifespan, and they are cheaper than active and semi-passive tags because they do not contain batteries of their own. They stay inactive until they come in close vicinity of a

reader's magnetic field that can tune in to the exact frequency (wavelength) of the tag (Rosenberg, 2008:340). They obtain energy from the compatible reader, and that energy enables them to transmit their stored data.

When passive RFID tags became available in the retail environment, the thought was that they would replace the conventional barcode, but that did not happen. The two technologies have different uses and functions. Barcodes need line of sight to be scanned while tags do not. Barcodes are also still cheaper than passive RFID tags. A barcode carries a Universal Product Code (UPC) that identifies a specific type of product. The same UPC number is used for a particular brand and tin size of baked beans – globally and consistently (Clarke et al., 2008:514).

Where passive RFID tags are used on item level within the Supply Chain, it is assumed that the unique 16-digit ID number of the RFID tag, called the Electronic Product Code (EPC), is assigned to the item it is attached to. As per the example used before, here it is assigned to a specific tin of baked beans. The RFID tag on or in the tin then enables that specific tin of baked beans to be tracked and/or located by a reader, over a distance and without the necessity of line of sight. Tracking and tracing are possible from conception to the point of sale and sometimes even after the sale (if the tag is not killed at the point of sale). The unique 16-digit ID number is usually linked to a back-end database where more detailed (unlimited) information on the tagged item (tin of baked beans) is stored (Malone, 2006:1; Rotter, Daskala, Compañó, Anrig & Fuhrer, 2012:30). A typical database may be tiny (with limited information on a limited number of tagged items), or it can be massive (containing unlimited information on multiple tagged items). The computers on which the databases are stored may be stand-alone or linked to local or even global computer networks.

Examples of information stored on the tag or database may be, but is not limited to the following - manufacturer, date & place of manufacturing, shipping date, received date, expiry date, condition of the tin, date and time it was sold and to whom (Cochran, Tatikonda, & Magid, 2007:218).

The same principles described above in terms of RFID tags attached to or embedded into objects apply to RFID and NFC human implantable subcutaneous micro-chips (RFID-SM's and NFC-SM's). The most crucial difference between non-implantables and RFID-SM's is that active and semi-passive tags are not suitable for implants. RFID-SM's have shorter read ranges than non-implantable tags (even shorter than passive non-implantable tags). The read range of a high-frequency NFC-SM in the hand is between 1cm and 2cm. The read range of a low-frequency RFID-SM, read by a standard handheld or mobile scanner, is around 10cm to 15cm. The read range of a low-frequency RFID-SM, read by a strong reader that is, e.g. fixed inside a doorframe, can be prolonged to around 50cm. The read range of RFID-SM's that makes use of Ultra High Frequency (UHF) is about 10m (Lockton et al., 2005:222). RFID-SM's are small and durable. RFID-SM's have less storage capacity on the microchip itself than what non-implantable tags have. They are cylindrically shaped, and the size is comparable to that of a grain of rice (11mm x 1mm). The RFID-SM is concealed in a bio-compatible glass container to avoid tissue reaction. The RFID-SM is implanted via a thick needle that injects and releases it under the skin (Lockton et al., 2005:224).

Conclusion:

There are several different RFID tags available in the marketplace. It is essential to differentiate between active, semi-passive, passive non-implantable and passive implantables because they all have different frequencies, capabilities and purpose of use. The focus of this research report is on passive implantables.

2.2 General Uses of RFID Technology:

During WWII, RFID technology was used to identify aeroplanes as "Friend or Foe" (Heffernan, Vetere, & Chang, 2017:59; Madrid, Korsvold, Rochat & Abarca, 2012:199; Rodriguez; 2019:1585). Today, RFID technology is commonly used with great success in many different sectors, e.g. transport, pharmaceutical, security, surveillance, and Supply Chain Management (SCM). Different types of tags have different functionalities and are used for diverse purposes. To understand the dissimilarities between active, semi-passive and passive tags better, some of their uses will be described briefly.

Active tags can be used to track the location of shipping containers, trucks, heavy machinery, trains, cash-in-transit vehicles and aeroplanes (Patel, 2017:547).

Semi-passive tags can be used for automated e-toll payment collection, monitoring of traffic congestion and scrutinizing speed violations on toll roads. They can also be used in vehicle immobilizers to deter theft. They can be embedded in helmets or clothing of mineworkers, fire-fighters and paramedics to locate them after a disaster, e.g. if they are buried under piles of rubble. Semi-passive tags are suitable for warehouses where they establish the location of shipping crates and pallets and reduce employee theft. The information harvested from the RFID tags helps to optimize stock quantities, just-in-time inventory control, and better decision-making to better fulfil customers' needs. Like active tags, they can be used for unobtrusive surveillance purposes over a relatively long distance to establish a location at a given time (McIntyre et al., 2015:14).

Due to their short read range of 10m to 30m (shorter than active and semi-passive), passive tags (non-implantables) are impractical to use on crates and pallets for in-transit tracking. Despite this, passive tags have established themselves as handy tools that are highly and increasingly used

in everyday situations. In the pharmaceutical sector, they are used on item level to combat counterfeiting. Libraries use them for self-check-out, and automatic book returns. In many workplaces, they are embedded in luggable (carry with you) or wearable (wear on your body or clothes) access cards. Here they are used for access control, to manage employee absenteeism, or even monitor employees' productivity. The banking industry embeds them in bank cards and uses them as identifiers for cashless payments. Retail environments use them for item-level tagging, especially in clothing and small, valuable items like lipstick and razor blades (Lockton et al., 2005:223).

In the animal kingdom, thousands of pets worldwide are implanted with passive RFID-SM's for identification purposes to reunite them with their owners if lost and found. Wild animals are implanted for tracking purposes to study their behaviour and migration patterns. Farm animals are implanted to prevent disease spreading like mad cow disease and rabies. Thoroughbred horses are micro-chipped for identification purposes (Foster et al., 2008:44; Lockton et al., 2005:222).

Consumers are often unaware that they are using, possess, or come in contact with RFID technology frequently. Still, from the aforementioned, it is clear that human beings progressively do come closer to and use RFID technology regularly or even daily.

Now that we have a clearer understanding of how RFID technology works and where it is used, the focus will move to the use of human RFID-SM's. In the paragraphs that follow, I will briefly explain how RFID-SM's came to existence.

In 1998, as an experiment, Kevin Warwick, Professor in cybernetics at the University of Reading in the UK was the first human to implant an RFID-SM into his upper arm to see if his computer

can track his movements throughout the university, operating doors, switching on lights and logging in to his computer without lifting a finger (Foster et al., 2008:45). The experiment was successful. So, the possibility of human RFID-SM's has been lurking in the background for many years already.

The idea to use RFID-SM's in humans on a greater scale came to life when the attack on the World Trade Centre in New York was broadcast on September 11, 2001. An employee of the Digital Angel Corporation in America saw fire-fighters and other rescue workers writing their badge numbers on their hands or bodies to be identified later on if needed (Gadzheva, 2007:217; Heffernan et al., 2017:59). IBM provided seed funding in the order of $30 million to develop the VeriChip, a human implantable RFID-SM, developed by Digital Angel Corporation (Lupton, 2015:308). The US Food and Drug Administration (FDA) that regulates medical devices in America approved the VeriChip RFID-SM in 2004 as a class 2 medical device and declared it suitable for subcutaneous human use. To date, the VeriChip is the only RFID-SM to receive approval by the FDA, to use for identification purposes within a medical context where informed consent is given (Smith, 2007:125).

Conclusion:

There is a wide-variety of uses to RFID technology and they rely on the different types of tags as distinguished in the previous sub-section.

3 Virtues of the Use of Human RFID-SM's:

As unique identifiers and devices that can generate, monitor, store and communicate private information, RFID-SM's have virtues made possible by proper use. In this section, I will attempt to build a solid presumptive case for the acceptability of some of the RFID-SM uses by weighing up benefits.

I will argue that there are uses where human RFID-SM's have huge potential to improve human life in ethically significant ways. I will organize the content according to convenience, control and safety & care. In this context, "convenience" is more substantial or more profound than what the term suggests typically. It refers to a form of convenience that can improve a person's quality of life as it allows seamless movement through different daily activities. Control can be interpreted positively, especially where it refers to the possibility of tracking, tracing and identifying persons in life/death situations, where locating the person is beneficial to him/her or their loved ones. Safety & care in this context refers to uses that have the potential to not only save a person's life but to contribute to a better quality of life, prevent more significant harm and possibly add quality to prolonged life.

The prerequisite for implantation must always be that free, un-coerced informed consent is obtained before implantation. The innocent citizen must have the freedom to remove the RFID-SM at any time s/he does not need or want it anymore (Gadzheva, 2007:222). Sufficient and adequate standardized infrastructure should be in place for optimal functionality (Smith 2007:134). The type and extent of the infrastructure (private home, care facility, workplace, national or global) is dependent on the use (access card, storage device for personal information, payments or monitoring device) as well as specifications (short read range of 1 cm, longer read

range of 50cm or long read range of 10m) of the secure RFID-SM and the development of secure purpose-driven readers and databases.

I will work from the assumption that implants are superior to luggables and wearables in the sense that implanted RFID-SM's are more hygienic, resistant to crushing, tearing and moisture and that they will not be forgotten somewhere, get misplaced or lost. A luggable or wearable can easily be tampered with, removed or even accidentally discarded (Lupton, 2015:310; Masters & Michael, 2005:3). RFID-SM's are invisible to the naked eye, and they have a shorter read range than luggables and wearables (Heffernan et al., 2016:55). We do not know how long the Covid-19 pandemic will be with us or how the "new normal" will look. A wearable outside the body can easily be contaminated with Covid-19 droplets and not sanitized because it is not on the hand area. Newer RFID-SM's are usually implanted in the web of the hand (Grauer, 2018). If your hand touches a contaminated surface, the part of your hand that contains the RFID-SM will be sanitized regularly as part of your daily routine.

The above taken into account, it may however be more ethical in terms of possible coercion and freedom of choice to offer people an option between a luggable, wearable and implantable as it is the same technology; it is just packaged differently (Mass, 2014).

3.1 Convenience:

3.1.1 Automation of Processes:

The primary purpose of technological advancement is to make tasks and life as easy, effective and comfortable as possible. A non-disabled person may find it merely frustrating to perform repetitive tasks manually. It can sometimes be challenging to open a door or switch on a light while carrying a stack of documents or bags of groceries. For the non-disabled person, automation of processes may be nice to have.

The physically challenged or wheelchair-bound may benefit even more from RFID-SM's and automated processes. RFID technology is an enabler of "smart" environments. With an RFID-SM the physically disabled person would be able to open and close objects (e.g., doors and windows) and switch devices and appliances on and off. The use of RFID-SM's may add quality, autonomy and dignity to their lives as it will enable them to perform tasks that are impossible for them to achieve without the technology.

Conclusion:

Automated processes may add quality to life or make independent living a possibility for disabled people (depending on the type and level).

3.1.2 Uploading Small Documents to Your RFID-SM:

First-generation RFID-SM's have minimal storage capacity on the microchip itself. It only carries a unique 16-digit ID number that serves as a link to a database that contains applicable personal information on the implantee (Rotter et al., 2012:30). No personal information is stored on the RFID-SM itself. Despite being low-level technology, older generation RFID-SM's will always be readable due to the "backward compatibility" of ICT (Grauer, 2018).

Newer generation RFID-SM's do have more storage capacity on the microchip itself. They also have built-in security features (encryption and password protection) and are available in the re-writable format. The latest generation RFID-SM's are so advanced that they can be seen as elementary computers (Gasson et al., 2013:253).

More storage capacity on new generation RFID-SM's itself makes it possible to upload keys (ID numbers) from different databases to the RFID-SM or upload a small amount of crucial personal information to the re-writable microchip itself. With a NFC-SM it is possible to upload your

business card and automatically share it to someone else's cell phone (with NFC capability) by pressing the NFC-SM against the cell phone. What you upload to the RFID-SM need not be permanent. Keys and crucial information can be removed and replaced as needed (Grauer, 2018).

A person that travels overseas can link valuable travel documents to the RFID-SM or store crucial personal information on the RFID-SM itself. Once links are established the traveller can have peace of mind that the information will not be stolen or lost, leaving him/her with a predicament in a foreign country.

Currently, the storage capacity on the RFID-SM is still limited because some of the available space on the RFID-SM goes into strong encryption and password protection. As the technology advances, more storage capacity will become available on the RFID-SM itself (Gadzheva, 2007:221; Gasson et al., 2013:252).

Conclusion:

More storage space on newer generations of RFID-SM's makes it possible to store crucial information, a small document and/or keys (links) to databases on the RFID-SM itself. This information can be encrypted and password protected.

3.1.3 Replacing Luggables and Wearables with Implants:

It may be possible to upload the functionality of luggables in your wallet to a purpose-specific RFID-SM. Latest generation RFID-SM's are capable of encryption. They are password protected and NFC-SM's have a very short read range of 1cm to 2cm (Grauer, 2018).

With a purpose-specific RFID-SM, a person can go jogging without taking his/her keys or wallet and still re-enter his/her property. If s/he decides on the spur of the moment to purchase something on the way home, s/he has all his/her important documents with him/her to perform the transaction.

The attention of people with small children and older adults with walking aids is sometimes distracted. They easily fall prey to kidnappers or pick-pocketers that observe them from a distance and notice their vulnerability. If they do not have to worry about the things they have to carry with them, like keys, purses or handbags, they will be better equipped to focus on their surroundings and the possibility of suffering harm (Catherwood et al., 2015:4). Having a purpose-specific RFID-SM implant with a short read range and built-in security features may be beneficial. It may lower the risk of opportunistic petty crimes and may even prevent kidnapping as it allows the implantee to be more alert of his/her surroundings instead of having to focus and protect valuable luggables.

Wallets, keys and handbags are bulky, visible and easy to grab in a split second. RFID-SM's are invisible to other people and cannot be grabbed from a person (Heffernan et al., 2017:59). A person with malicious intent will have to know that you have an RFID-SM, what kind of information you store on the RFID-SM (at that moment) and what tasks/applications you are using the RFID-SM for. S/he will have to know the exact frequency of your RFID-SM as well as the physical location thereof. S/he will need to carry a compatible reader with him/her to scan your RFID-SM. After going through all the effort, the person with malicious intent may find that the information s/he tried to retrieve is protected by multi-level security factors and not usable (Brown, 2016).

Objection 1:

It may be argued that storing personal information on an RFID-SM is risky because the microchip can be read silently, over a distance and without the necessity of line of sight (Foster et al., 2007:28; Garfinkel, Juels & Pappu, 2005).

Rebuttal:

People may not always be aware that the RFID luggables they carry around in their pockets, handbags or wallets, wearables worn on their clothes or bodies daily, use the same technology as RFID-SM's. Examples of luggables and wearables that may have RFID tags for identification purposes embedded in them are ID documents, passports, access cards, bank cards, loyalty cards, car keys, key cards, membership cards and fitness trackers.

Where RFID luggables and wearables are manufactured and issued out in bulk by the government, commerce and the banking industry, the user does not have a say regarding the specifications used. It is possible that the micro-chip embedded in a plastic card in your wallet can be accurately read over a distance of 30m if not protected. In contrast to this, the read range of an RFID-SM can be decreased by the frequency chosen. The fact that it is implanted in the body where it is surrounded by body fluid also reduces the read range. The deeper the micro-chip is tucked away inside the body, the smaller the read range. The longest read distance of an RFID-SM is still shorter than that of luggables or wearables.

Depending on the micro-chip specifications, the most accurate read results are sometimes only retrieved when the RFID-SM is held very close to a compatible reader or, even better, when the RFID-SM is pressed against the reader (Grauer, 2018).

The objection to unobtrusive reading of RFID-SM’s is thus not a very powerful objection.

Objection 2:

It may also be argued that a stronger reader will increase the read range substantially and thereby increase the risk of RFID-SM's being read unobtrusively (Lupton, 2015:312-313).

Rebuttal:

You may be able to increase the read range slightly, but the maximum read range is worked into the specifications. You can compare readers with reading glasses. To have optimal eyesight, you need glasses made according to your unique requirements and needs. If the glasses you wear are too strong, the images that you see will be distorted. The stronger glasses will not damage your eyes. A reader that is too strong for a specific micro-chip will retrieve unusable, distorted information. However, the reader will not damage the passive RFID-SM implant, injure the skin or cause radiation problems (Gasson et al., 2013:273; Patel, 2017:546).

Conclusion:

With an implanted RFID-SM, that replaces the luggables in his/her wallet, pockets and handbag, a person will be able to travel lightly without the fear of losing, misplacing or forgetting valuable luggables like keys and credit cards.

3.2 Control (Tracking and Tracing):

3.2.1 Workplace:

One of the oldest known cases where human RFID-SM's were used for identification purposes for access control in the workplace is where the Attorney General of Mexico and 18 staff members received RFID-SM's. This happened in 2004, and the aim was to allow only these implantees access to a restricted area where criminal records, containing sensitive information, were kept (Foster et al., 2008:45; Rotter et al., 2012:38).

More recent workplace-related use cases are the Swedish company Epicenter that has offered employees RFID-SM's since 2015. The RFID-SM's enable them to make payments at the cafeteria and open doors with a mere wave of the hand. In 2017 the American based company Three Square Market started to implant consenting employees with RFID-SM's. They offer employees that do not want an implant the option of a wearable. The RFID-SM they use enables employees to open doors, unlock phones, log into computers, operate photocopy machines, store crucial medical information, share business cards, do purchases in the break room and payments at RFID terminals. At NewFusion, based in Belgium, RFID-SM implanting also started in 2017. Employees use the RFID-SM for access purposes - to the building as well as computer systems. The companies mentioned above are all high-tech companies that specialize in digital marketing and innovation. Implanting happens at what are called "chipping parties" (Darrow, 2017; Gauttier, 2018:6; Rodriguez, 2019:1581-1582).

Objection:

A concern around workplace-related RFID-SM's is that employers will be able to track employees' movements after work hours outside the workplace as well (Foster et al., 2007:27).

Rebuttal:

It will be difficult for an employer to track the movements of employees outside the workplace via RFID-SM's. The RFID-SM works effectively where it is set up as part of a purpose specific RFID enabled environment (Heffernan et al., 2016:56). Movement can only be registered as an implantee passes through reader scan points whilst performing their daily routine tasks (Spector, 2014:6). If you are at home and your home is not RFID enabled (nor networked), the RFID-SM will remain inactive. If you visit a retail outlet that is RFID enabled, but the unique 16-digit ID number of your RFID-SM is not registered on their RFID system and you pay with cash for your purchases, the reader(s) you pass may be able to read the unique 16-digit ID number on your

RFID-SM, but due to encryption, the information will not be interpretable by the owner(s) of the reader(s).

If you are able (and allowed) to make payments with your work RFID-SM and you do use it for that purpose outside the workplace, the RFID enabled retail store where your RFID-SM is registered and where you use it for payment purposes will be able to identify you and take note of your presence as well as the things you purchase at a given time. The fact that you wandered around visiting places and even used your workplace RFID-SM for payment at a retail store will not be known to your employer. The transaction information belongs to the retail outlet and not your employer. Unless your employer owns or has access to compatible readers placed all over the town, city, province, country or even globally, s/he will not know your whereabouts outside the workplace based on your RFID-SM. Suppose an employer wants to know the whereabouts of employees after work. In that case, it will be much easier and cheaper to monitor employees via social media, vehicle or cell phone tracking.

Conclusion:

Latest generation RFID-SM's can be used for identification as well as authentication due to the integration of multi-level security factors. This makes RFID-SM's ideal for access control purposes within workplaces, especially where there are highly secure, restricted areas that should be accessible to only a few employees (Lupton, 2015:309).

3.2.2 Identification and Location Purposes after a Disaster or Death:

Humans are more mobile than ever before (Covid-19 aside), and identification for forensic purposes is sometimes problematic. A person never knows where s/he will be located when a disaster strikes - whether it is kidnapping, murder, human trafficking, an accident or a tsunami

(Gadzheva, 2007:220). The downside of this is that thousands of people are kept in morgues and eventually cremated or buried, either in single or mass graves, without ever being identified.

If a person with an RFID-SM containing identifiable information goes missing and is found later on, either in a state of shock, badly hurt, unconscious, or dead, the person/body can be accurately identified and reunited with family and loved ones. Some families spend vast amounts of money, resources and time over many years, without ever finding closure on what happened. Identification through an RFID-SM may bring closure to the family to carry on with their lives again.

Dentures have been used as a form of forensic identification for many years. RFID-SM's in dentures bring a new dimension to this proven form of identification. At the Catholic University of Leuven, Belgian scientists embedded an RFID-SM into a molar to store private information like a name, date of birth, gender and nationality. The information on the RFID-SM's can be read post-mortem and used for identification purposes by forensic scientists. This is especially helpful after natural disasters or terrorist attacks where there usually are numerous victims (Gadzheva, 2007:220). An added benefit to an RFID-SM implant with a more extended read range (up to 10 m) is that the bearer may be located if buried under some rubble or in a shallow grave.

It happens pretty often that the wrong body is handed over to the wrong family for burial purposes. RFID-SM's (e.g. in dentures) will ensure accurate identification that will prevent body mix-ups at mortuaries where families often grieve over and bury the wrong person (Brown, 2016).

After the 2004 tsunami in Indonesia, hospitals and morgues were unable to cope with the number of casualties and corpses. There were more than 200 000 dead bodies with severe injuries and in different stages of decomposing. These bodies had to be stored indefinitely in several cold-storage facilities and retrieved at later stages. Because of the disaster's extent and prolonged

timeframe, the usual way of marking body bags was inadequate. The bodies were implanted with RFID-SM's in a predetermined location in the bony structure of the skull. Even though bodies were stacked upon each other in cold-storage facilities, they were easily identifiable via RFID technology, using handheld scanners. Implanted RFID-SM's are functioning well between 80°*C and* -18°*C*. Traditional ways of marking the body bags deteriorate quickly and become unusable and illegible. Mass body identification by RFID-SM's proves to be very effective and successful (Meyer, Chansue & Monticelli, 2006:168-170).

Conclusion:

RFID-SM's allow accurate identification over a predetermined distance without the need to touch. Their use for identification purposes after a disaster of some sorts proves to be beneficial.

3.2.3 Long Term Care Facilities:

Facilities (or homes) that care for people with cognitive impairments and dementia, like Alzheimer's can be RFID enabled with RFID readers placed at strategic points for optimal use. Young and old are free to move around within the secure demarcated area. An alarm will sound whenever someone leaves or is removed from the safe zone without permission. Depending on the functionality of the RFID-SM chosen and the infrastructure put in place, caretakers can be alerted when a patient has fallen, did not take his/her medication or is unconscious (Masters et al., 2005; Rotter et al., 2012: 31).

The use of RFID-SM's may enhance the quality of life of people with cognitive impairments substantially. For them, (as impairment progress) it may be the preferred way of living. Living with and RFID-SM is more liberating than being locked up in a room or being strapped to a bed (Niemeijer & Hertogh, 2008:50-51).

Although the same RFID functionality can be packaged in a luggable, wearable and implantable format, the fact is that Alzheimer patients get to a point where they forget what the purpose of things are. They may become annoyed with a wearable and try to remove it. They may succeed, rendering the wearable useless. They may even hurt themselves in their effort to get rid of it. Where this is the case, a purpose-specific RFID-SM may be a solution to the problem. RFID-SM's soon become part of a person's body and allow seamless movement through RFID enabled spaces (Gasson et al., 2013:260).

Caring for people with cognitive impairments and dementia, like Alzheimer's is challenging, time-consuming and emotionally draining. A family member or caretaker can't be everywhere and know everything. The fact that family members or caretakers will be alerted when something goes wrong will contribute to peace of mind. The use of RFID-SM's will soften the burden on all of them. They will have freedom to re-charge so that they can perform their work with the necessary empathy and patience that is needed for the job.

Objection:

Depending on the mobility and level of impairment of the person, s/he may accompany a family member or caregiver to a shopping mall, to visit a doctor or other family members. The person with cognitive impairment may "wander" off, and may not know how to get home again. This can lead to distress and anxiety (Niemeijer et al., 2008:50).

Rebuttal:

An RFID-SM containing unencrypted crucial personal information provides a safety net for a situation like this. The unencrypted information on the RFID-SM can be read by a public official with a compatible reader and the person can be returned to the safety of his/her home quickly.

Conclusion:

RFID-SM implants allow safe, seamless, dignified, free movement within an RFID enabled area. This is ideal for people with dementia, Alzheimer's and other cognitive impairments. The RFID-SM is safely tucked away inside the body where its existence won't bother the patient. The patient is unable to remove it accidentally, leaving him/her vulnerable to getting lost.

3.2.4 Inside a Hospital Environment:

Within an RFID enabled hospital environment, it is possible to keep track of a patient with an RFID-SM as s/he moves from one ward or section to another, e.g. Emergency Room to Radiology (Lupton, 2015:311). It is also possible to avoid and control unauthorized access to wards, rooms and cupboards with restricted access (Rotter et al., 2012:33).

The purpose of use determines the read range of the most applicable RFID-SM. New generation RFID-SM's have space to store crucial information on the RFID-SM itself. If it is a re-writable RFID-SM, you can update the information on the micro-chip regularly. Medical information stored on an RFID-SM implanted at birth can be updated when necessary to ensure up to date information on pertinent issues related to a specific patient. In addition to the information on the RFID-SM itself, the 16-digit unique ID number of the RFID-SM can still be linked to a database where more detailed information on the patient is stored.

Staff may leave a written file behind at a specific bed, and another patient may be placed in that bed without staff noticing that the file does not belong to the patient in the bed. With crucial information on the RFID-SM itself, the chances of correct operations and correct medication being given to the right patient are increased - especially when a patient is moved from one bed to another or from one ward to another.

With a newborn, an RFID-SM can contain crucial medical information on the baby as well as identification detail of the baby and the biological parents. This will reduce mix-ups where the wrong medication is administered or where babies are being handed over to the wrong parents. Just as in the case of care facilities mentioned before, the wards where babies, young children, and other vulnerable patients are treated in hospitals can be RFID enabled. Whenever a baby, child or other vulnerable person leaves or is removed from the ward without permission, an alarm will sound (Masters et al., 2005).

Conclusion:

In a hospital setting, there is always the risk of mistakes being made, some irreversible and some even fatal. The use of RFID-SM's may limit these risks.

3.3 Safety and Care:

3.3.1 Personalized Firearms:

While it would be better if we had fewer guns, guns are an unfortunate fact of life. In some countries where crime is rife, firearms are often stolen from innocent citizens as well as public officials and used for criminal activities. Innocent citizens and public officials are hurt, permanently debilitated or even get killed during altercations with criminals.

Small children can get hold of somebody's firearm and hurt or kill someone by accident. It also happens that teenagers get hold of a family member's gun and commit suicide with it or take it to school and commit murder. Incidents like this leave scars for life.

Browning and Smith & Wesson are working on firearms that can only be fired when the owner is identified via his/her RFID-SM and thus prevent abuse of the firearm. With a personalized

weapon, the RFID-SM is implanted in the hand, and the reader is installed in the grip of the gun (Brown, 2016; Rotter et al., 2012:34-36).

Objection:

It is argued that under certain circumstances, it may be necessary for another member of the household (military/police/security) to use the same firearm (Heffernan et al., 2017:60).

Rebuttal:

This is not difficult to overcome as the RFID-SM can be cloned under secure circumstances and implanted in the other person's hand for positive recognition and identification purposes. Another possible solution is to allow multiple user ID's on the reader.

Conclusion:

A personalized firearm that can reduce the potential inadvertent harm posed by guns is to be welcomed with open arms.

3.3.2 VeriMed Project:

After the VeriChip RFID-SM was approved for medical use by the FDA in 2004, there was an effort to market the RFID-SM as a possible life-saving device in emergencies. Potential candidates include people with diabetes, seizure disorders, cognitive impairments, heart diseases, and cancer (Foster et al., 2008:45; Gadzheva, 2007:219). The VeriChip is part of the first-generation RFID-SM's with minimal storage capacity on the RFID-SM itself. The VeriChip itself only holds a unique 16-digit ID number for accurate identification of a specific person.

This unique 16-digit ID number, when read by a compatible, authorized reader, serves as a link to a computer containing a VeriMed database with unlimited up to date data on the patient.

Information stored in the database pertains to medical history like treatment received, life threatening illnesses, allergies, do-not-resuscitate request, living will and donor status (Foster et al., 2008:45). Identification information like name, address, age, blood type, ID number, medical aid is recorded in the database (Foster et al., 2008:45; Gadzheva, 2007:219). By scanning the VeriMed RFID-SM with a special VeriMed reader at an emergency scene, you can retrieve fast, accurate and reliable information from the database (Lupton, 2015:309). Paramedics can give the correct, potentially life-saving treatment from the beginning without having to search through clothing and other possessions for medical and identification information. This would especially apply if the patient is unconscious and unable to speak for him/herself (Foster et al., 2007:27).

Objection 1:

It is mentioned that where the 16-digit ID number of the RFID-SM is used for accurate identification of a specific person, it calls up memories of Nazi concentration camps where people were "branded like cattle". Privacy advocates fear that RFID-SM's will reduce innocent citizens to a single number (Catherwood et al., 2015:5; Niemeijer et al., 2008:5).

Rebuttal:

In real life, citizens have different identification numbers assigned to them during various stages of their lives. Examples of this include ID number, passport number, social security number, staff number, medical aid number and even license plate number. These numbers exist in the public domain and can be used to access databases that contain information about them. Yet, people accept these numbers as a necessary part of their lives and are not utterly concerned about them. The 16-digit ID number of the RFID-SM can be controlled and confined to the private domain if only used for private transactions and not networked. If the 16-digit ID number has to be used in the public domain, it can be encrypted and password protected to ensure confidentiality.

Some people do implant more than one RFID-SM in their bodies. Each of these have its own unique 16-digit ID number. A counter-question may then be – which one of these numbers (from the public or private domain) do you choose to be the one that will reduce you to a single number? It may be that the concern about being branded like cattle is rather about the possibility of abuse of power than the number being assigned to an RFID-SM.

A possible solution to the fear of being branded like cattle is to download a unique identifier (key) for each system you use, onto the RFID-SM, instead of adding the unique 16-digit ID number of the RFID-SM to the system that you use (Heffernan et al., 2016:56).

Objection 2:

People may also argue that despite the FDA's approval of the VeriChip, a list of potential hazards was published as a warning to be cautious. The list includes "adverse tissue reaction, migration of implanted transponder, compromised information security, failure of the inserter, failure of the electronic scanner, electromagnetic interference, electrical hazards, magnetic resonance imaging incompatibility and needle stick" (Foster et al., 2008:45; Gadzheva, 2007:223).

Rebuttal:

These concerns are not relevant to new generation RFID-SM's anymore. New generation RFID-SM's are made of "bio-inert" material that is safe to use in the human body (Heffernan et al., 2016:54). Older generation RFID-SM's were implanted into the upper arm, where it was problematic to find them if they moved slightly. If not findable or not readable, they cannot perform the task they are meant to perform (Masters et al., 2005). Depending on the use, in order to avoid un-traceability of the RFID-SM later on, the place of the implant in the body should be consistent and carefully selected beforehand. At this stage, the implant's preferred location is in the hand's web, between the thumb and index finger. Once inside the body, the RFID-SM is unlikely to break

(Grauer, 2018). Older generation RFID-SM's are covered in Bio-Bond and attach to the flesh to prevent migration in the body. Removal is difficult (they are supposed to be permanent fixtures) and require expert medical intervention (Lupton, 2015:308). Newer RFID-SM's are not covered in Bio-Bond anymore. This makes removal quite simple as newer RFID-SM's do not bind with the flesh as older RFID-SM's did. During the same session, under hygienic circumstances, the old RFID-SM is removed and the new one implanted – just like sub-dermal contraceptives (Foster et al., 2007:29; Grauer, 2018). Over the past few years, the RFID-SM technology has improved, and security features, e.g. encryption, biometrics, and password protection have been added to RFID-SM's, readers and databases. The newer generation human RFID-SM's are not detected by metal airport scanners and are well-suited to use with MRI machines (Grauer, 2018; Madrid et al., 2012:202). RFID-SM's are also building up long-time credibility as more people have them for many years without any problems.

Objection 3:

Another concern that is raised is that the database's information (as used within the VeriMed project) is not updated regularly and that the database may not contain the latest information (Monahan & Fisher, 2010:373).

Rebuttal:

Over 900 hospitals on the East Coast of the USA signed up for the VeriMed project. More than 1 100 patients received the VeriChip implants at the cost of $200 for the RFID-SM as well as a further $100 annual membership fee specifically for the upkeep of the database (Kahn, 2015:4; Lupton, 2015:311). A control method was thus in place to minimize the risk of wrong or outdated data. Furthermore, if the database was not up to date, the RFID-SM could not be blamed since it only served as a link to the database.

Objection 4:

Fear is also expressed that medical practitioners will start to trust the information in the database more than they trust what the patient tells them and compromise the doctor/patient relationship (Monahan et al., 2010:373).

Rebuttal:

The truth is that the VeriMed plan was never to implant everybody but rather to implant patients with high-risk medical conditions, those with existing communication problems and those that are unconscious and therefore unable to communicate (Foster et al. 2007:28).

It is even possible that the database may be a safety net (for any patient) as it may contain a small detail that is crucial but long forgotten.

Objection 5:

The VeriMed project was terminated and the technology sold to Positive ID in 2010. In 2014 it was sold to VeriTeQ (Mass, 2014:2). Currently the technology is in the hands of various Bio-hackers that are busy with their own developments. There are several different brands of RFID-SM's available on the marketplace, each requiring special infrastructure and a special reader that is compatible to the specific brand and frequency of the RFID-SM. Lack of standardization will have an effect on the readability of RFID-SM's on emergency scenes

Rebuttal:

The VivoKey, one of the latest generation RFID-SM's is in the process of obtaining FDA approval. The VivoKey makes use of NFC technology. It has a short read range of 1cm to 2cm and a smart phone with NFC capability can act as a reader of unencrypted information that is stored on the

NFC-SM itself. Crucial medical information (or instructions) can thus be stored on the NFC-SM itself. Since you want people to be able to access this potentially lifesaving information easily, you will choose freely to leave it unencrypted. Examples of this may be allergies like penicillin, a bee sting or peanut butter, diabetes, the fact that you take anti-blood clotting medication, or epilepsy. With some of these conditions, even an innocent bystander (while waiting for an ambulance) can assist if s/he knows what the problem is. Sometimes a life can be saved by something as simple as a cube of sugar or an antihistamine tablet that can be in the pocket or handbag of the patient.

Many citizens with severe medical conditions, such as chronic cardiovascular diseases, diabetes or seizure disorders, might value this technology. “It will be difficult to argue against the legitimate right to protect oneself against injury or danger” (Gadzheva, 2007:219).

Conclusion:

RFID-SM’s have improved over the past few years and their use within emergency situations can be beneficial.

3.3.3 Monitoring Function:

RFID-SM's are not to be confused with implantable ICT medical devices like Cardiac Pacemakers (with or without defibrillators) that restore heart rhythm, retinal implants that restore vision, cochlear implants that restore hearing or insulin pumps that can administer the exact dose of insulin needed at a specific stage. These are battery-powered devices where the aim is to restore lost ability and not to augment above the average level. Some of these devices may, however, have RFID capability. In addition to the foregoing, bio-sensors with RFID capability can be implanted into prosthesis.

The purpose of these RFID-SM's is to monitor bodily functions and communicate findings to the person self or to a medical practitioner. This can be done on an ad hoc basis, regularly or permanently. Examples of bodily function feedback can be oral health via dental implants, fertility for family planning, body temperature to detect infections early, toxin levels, blood pressure, blood glucose, heart rate, respiration rate and cholesterol levels (Al-Janabi, Al-Shourbai, Shojafar & Shamshirband, 2017: 114; Masters et al., 2005).

Real-time, accurate information can be communicated from where the RFID-SM is situated inside the body. The information can be transmitted automatically and wirelessly (via a computer or smart phone with an Internet connection) from any place in the world to a predetermined entity, e.g. healthcare professional (Al-Janabi et al., 2017: 115). Based on this information the healthcare professional can make decisions, change medication or start lifesaving treatment where needed. As early warning systems these RFID-SM's allow potential medical problems to be detected early. It may be possible for a medical practitioner to derive from the data that a patient will have a heart attack or stroke soon, and s/he can administer preventative treatment timely and successfully.

> It seems likely that utilization of RFID implants for medical applications will expand, and the potential advances for the individual user might well outweigh privacy and security risks in certain cases (Gadzheva, 2007:222).

Conclusion:

RFID-SM's for monitoring purposes are especially convenient where long term monitoring is necessary. They become part of the body and allow seamless movement and peace of mind because you will not lose them, misplace them or forget them. You can be anywhere in the world, and your medical practitioner can monitor your bodily functions if or when needed.

3.3.4 Digital Identity

The VivoKey NFC-SM wants to establish a digital identity by linking a person's biological identity to his/her digital identity. VivoKey is capable of encryption and password protection. It makes use of private and public key infrastructure. It is marketed as being safe enough to handle payments and Bitcoin transactions (Grauer, 2018). Where real-life identity is based on, e.g., an ID number, social security number or passport number that forms part of the public domain and is not difficult to obtain, the digital identity is based on a unique digital ID number that is part of the private domain. The public key that is available in the public domain enables someone to send the owner of the public key a message that is encrypted. The private key is not known in the public domain. The owner of the public key that receives the encrypted message can decrypt the message by using his/her private key. A digital identity makes identification as well as authentication possible.

In the digital world, the innocent person does not always know who s/he is transacting with as everything s/he sees may be based on a lie. It is easy to mislead people by creating a profile using a fake username, password, a photo of somebody else or of a cute pet. A man can present himself as a woman, or a person can present him/herself as a much younger or a much older person. The VivoKey wants to bring a solution to criminal activity stemming from fake identities in the digital world.

Objection:

The digital identity implant establishes a permanent link between a person's real life identity and his/her digital identity. This will have a negative impact on anonymity and privacy in the digital world (Rotter et al., 2012:35).

Rebuttal:

Yes, there is an ethical dilemma between being anonymous and hiding behind a fake identity from where a person can do evil things versus having a secure digital identity. A digital identity will make transactions over the Internet a lot safer because you will know that the person you are transacting with is a real person and is in fact who s/he says s/he is. A digital identity will bring honesty and transparency back into online transactions.

A further advantage is that the digital identity NFC-SM only makes a digital identity possible where identification and authentication are needed. On web pages where authentication is not required, a person can still remain anonymous even if s/he has a digital identity NFC-SM.

Conclusion:

Latest generation RFID-SM's (like the VivoKey) that include multi-level security factors, make identification and authentication possible. They are ideal for establishing a digital identity to combat digital fraud.

We have a moral right to privacy and a moral right to protect our privacy. Some ICT deplete us of privacy. RFID-SM's if used correctly may protect us from those with malicious intent and it may give some control over privacy back.

Conclusion Part 3:

RFID-SM's have developed considerably from the first generation to the latest generation. Repetitive tasks (e.g., opening and closing as well as switching on and off) can be automated. This can especially be beneficial to disabled persons.

RFID-SM's have purpose-specific frequencies and functionalities. They have shorter read ranges than luggables and wearables, and they have more storage capacity on the RFID-SM itself than before. They are now more secure, capable of encryption and password protection. They are available in the re-writable format, so information can be uploaded and removed as needed. A small document or crucial personal information can be uploaded to the RFID-SM. The functionality of luggables usually carried around in your wallet, pocket or handbag can be uploaded to purpose-specific RFID-SM's. This brings convenience to a new level as it allows you to navigate lightly and seamlessly through daily activities without the fear of forgetting, losing or misplacing essential luggables like keys, credit/debit cards, ID cards and access cards

RFID-SM’s allow dignified, free movement within an RFID enabled area. This is ideal for people with cognitive impairments. Within a medical environment, the use of RFID-SM’s can contribute to fast, accurate, preventative and possibly lifesaving treatment. A personalized gun has the potential to prevent or limit harm to self and others. Latest generation RFID-SM’s include multi-level factors. They can be used for identification as well as authentication. RFID-SM’s are moving towards establishing a digital identity to combat fraud in the digital world.

Various objections have been raised against the use of RFID-SM’s. They have been responded to. These objections do not undermine the virtues of RFID-SM’s.

4 Autonomy, Coercion and RFID-SM Implants:

4.1 Autonomy and Coercion:

Autonomy is the moral right that allows a citizen in a liberal democracy the freedom and independence to make his/her own life choices. People do this to the best of their ability and according to their personal circumstances, needs and wants. Some choices may be right, and some may be wrong, but it is the person's unfettered choice.

Autonomy permits and justifies voluntary informed consent. In terms of the use of RFID-SM's in a liberal democracy, there must be respect for autonomous decisions, whether it is for or against RFID-SM implants.

Informed consent can only be given by a person that has access to applicable information and possess the cognitive capability to understand the functionalities, capabilities and limitations of RFID-SM's. True autonomous, voluntary informed consent is only possible in the absence of coercion and interference (even where it is well-intentioned) of the RFID-SM as well as the potential threats it poses to privacy to be able to give informed consent.

Where a person had the cognitive ability to make informed decisions, but lost the ability, a living will that was created when the person was still capacitated, can speak on behalf of him/her.

Where voluntary informed consent was obtained and the implantee changes his/her mind, s/he must have the freedom to opt out and remove the RFID-SM.

Where there is an imbalance of power or the possibility of receiving some kind of reward, it is difficult to determine whether consent to an RFID-SM is truly voluntary and informed. Forced and

coerced implantation is unethical and can be seen as a form of assault. Therefore it may be prudent to have legislation in place that restrict government, workplaces and commerce in terms of what is permissible where it comes to RFID-SM implant projects. If the option is closed off, citizens are freed from pressure as they will not receive a request from aforementioned groups to be implanted. Where it comes to autonomy and informed consent around RFID-SM implants citizens should always be treated with dignity and respect.

4.2 Possible Coercion in Different Sectors:

The anti-RFID activist group Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), organized several protest actions against the use of RFID technology on item-level in retail environments. When RFID-SM's became available on the marketplace, they added fuel to the fire. Fears around privacy of information, tracking and tracing of people were rife and RFID-SM's attracted a lot of negative publicity. The public backlash and low acceptance rate that followed was not what was expected (Catherwood et al., 2015:5).

It was as if the marketers of RFID-SM's had a product in which millions were invested, and they needed a place in the market to go to with it. Marketers may have been over-eager to sell their product to an already scared/fearful client base. Disrespect for autonomy, inadequate information, misrepresentation of the capabilities of RFID-SM's coercion and involuntary implantation may have been part of the equation. Mistakes were made, and trust between producers, marketers and potential buyers were broken.

4.2.1 Parents and Guardians:

4.2.1.1 Children:

Parents and guardians are allowed to take control and make choices on behalf of their own children and children they have custody of. The problem is they do not always make decisions that are in the best interest of these children. Some decisions they make on behalf of these children may benefit them more than what it benefits the children. Sometimes parents and guardians may not be educated sufficiently on a specific topic. This may have an impact on their decision making capabilities around RFID-SM's and it raise the question whether there should be limitations as to what choices parents and guardians may make on behalf of children. There is fear around the threat to autonomy and the possibility of coercion of children.

Response:

Around 2004, some of the elite in Mexico gave consent to implant their children with RFID-SM's in order to combat widespread kidnapping. This is the only known use case where children were involved in receiving RFID-SM implants.

This exercise is based on a misperception of the functionalities of the RFID-SM. Maybe the parents did not understand the capabilities or limitations of RFID-SM's entirely, or they have been misguided by marketers of RFID-SM's. RFID-SM's are not the right kind of technology to use for the 24/7 tracking of kidnapped people. They are passive micro-chips with a limited read range and no built-in GPS. Unless there is an extremely extensive network of compatible readers in place, RFID-SM's can merely identify a kidnapped or injured person once s/he is found (Gasson et al., 2013:262; Grauer, 2018; Lockton et al., 2005:224; Spector, 2014:5).

The fact that parents and guardians were coerced and unable to make informed decisions around the proper use of RFID-SM technology should not reflect negatively on the technology itself. This is in line with Lomas' quote (page 1).

CASPIAN suggests an age restriction of 18 years for RFID-SM's and in California they also want to restrict the use of RFID-SM implants in children (Malone, 2006:1).

I would rather suggest a case by case evaluation based on voluntary informed consent. RFID-SM's, if used properly, have the ability to contribute positively to the quality of life of children with physical and/or mental disabilities.

4.2.1.2 The Cognitively Impaired:

People with cognitive impairments and dementia like Alzheimer's may feel compelled to accept RFID-SM's because they feel that they are a burden to the people who care for them. The fear is that RFID-SM's may benefit caregivers and family members more than the implantee. If this is the case, the decision to get an RFID-SM is not fully un-coerced and voluntary.

Response:

Implanting people with cognitive impairments and dementia like Alzheimer's is a complicated issue. Nobody has the right to track anybody else without his/her informed consent. To obtain informed consent from the mentioned, vulnerable groups of people depend on their cognitive capabilities. In some cases, that is virtually impossible (Foster et al., 2008:46).

When a person is severely cognitively impaired, s/he is not really autonomous any more. It is impossible for this person to make life directing decisions like an independent person can. Autonomy can be preserved in a living will, drafted while the patient is still healthy enough to give

permission. Where this is the case, the person can be implanted with consent. If there is no advanced directive in place, permission can be obtained from the legal guardian. The person can then be implanted, not against his/her will, but independent of his/her will (his/her will is compromised).

CASPIAN would like to restrict guardians from consenting to RFID-SM implants. They would prefer 'in person' consent only. Persons with cognitive impairments may wish to be implanted with an RFID-SM and experience the benefits of living safely inside secure RFID enabled care facilities or homes. It is most unfortunate that such a wish may be locked inside a person that is unable to communicate it. It would be sad if we withhold something that can preserve and maybe even restore some dignity to this vulnerable group of people – especially if it is done because of unproven fears and conspiracy theories (Grauer, 2018).

4.2.2 Workplace:

It is argued that employers may coerce employees by offering benefits (e.g. a salary increase or promotion) if the employee agrees to an RFID-SM implant that will be used within the workplace. Employees may accept the RFID-SM due to fear around job security and the possibility of discrimination within the workplace. It is possible that a person can be asked during a job interview if s/he has an implant and whether s/he would accept one. Aforementioned fears are mostly due to the power imbalance that exists between the employer and employee (Mass, 2014). Colleagues that already have implants may make it seem as if it is commonplace to use them in the workplace. Where new (and other) employees make a decision to get an RFID-SM based on worry or obligation, consent is not autonomous, free, un-coerced or voluntary (Gauttier, 2018:8).

Response:

It may not be ethical for an employer to expect an employee to implant an RFID-SM in his/her body for work purposes. CASPIAN would prefer a total ban on the use of RFID-SM's in the workplace and several states in America have legislation in place to restrict their use in the workplace. A golden rule around using RFID technology in the workplace, for e.g. access purposes, may be to insist on a choice between a luggable, wearable and RFID-SM. If the implant is the employee's preferred choice of packaging, s/he should ensure that s/he purchase and pay for a re-writable, purpose-specific RFID-SM. By doing this, the employee ensures that s/he has ownership and control over use (within reasonable expectation). When an employee retires or leaves the employer for some reason, privileges within the workplace can be revoked by deleting the 16-digit ID number form the RFID system (Grauer, 2018). The person is then free to employ his/her RFID-SM exclusively for private use.

Where RFID-SM's are used within the workplace, the purpose of use should be stipulated clearly in a contract between the employee and employer to prevent scope creep and abuse. By adding autonomy preserving protection to the process, voluntary, informed consent is not necessarily compromised by the use of RFID implants in the workplace.

4.2.3 Commerce:

There is fear that commerce will coerce clients to get RFID-SM's by making promises of preferential treatment for those with RFID-SM's. The unease extends to the possibility that extensive use of RFID-SM's within the retail sector may favour those with implants to such an extent that those without RFID-SM's feel inconvenienced or discriminated against because they cannot shop where they want, or they may have to pay more for services at certain places. If a person agrees to have an implant on these grounds, consent is not un-coerced anymore.

The following is an example within the retail environment where implantees voluntarily agreed to have RFID-SM implants.

The Baja Beach clubs in Spain and the Netherlands and the Bar Soba in Glasgow offer consenting, highly valued customers an RFID-SM implant. With the implant comes VIP status and a feeling that they (the implantees) are superior and different (Foster et al., 2007:27; Lockton et al., 2005:224; Rotter et al., 2012:31-32).

The nightclubs are RFID enabled, with several readers placed at strategic points throughout the buildings. The moment a VIP guest with an RFID-SM enters the nightclub, s/he is accurately identified and introduced to the other guests. The name of the implantee flashes on a screen, and everybody in the club at that stage knows that the implantee is an important, probably rich guest. The implantee is now not a stranger to other guests anymore, and they can greet and chat with the implantee. From the RFID system, employees can see the implantee's credit balance at the club. The implantee's favourite drink is prepared immediately without him/her having to ask for it. A mere wave of the hand in front of a reader makes payment possible. As a VIP guest, the implantee has access to certain otherwise restricted areas and do not have to queue for anything (Gadzheva, 2007:220).

It is clear that there is a considerable amount of coercion involved in this example. The implantees may not have been well informed around risks and consequences. The benefits received as well as instant fame experienced is costly in terms of autonomy. Abuse in the form of additional amounts taken from the account when the implantee is incapacitated is possible. The amount of identifiable private information that commerce can harvest over time within a scenario like this is limitless and potentially harmful (Rotter et al., 2012:31).

Response:

Luckily the aim here is promotional - to attract more people to the nightclubs and not to harvest private information. Whether the implantees understood the possible impact on autonomy and un-coerced, informed consent is unknown. Overall the publicity stunt is perceived as a 'cool' and 'feel good' experience, and there is no harm reported.

4.2.4 Government:

There is a lot of fear that governments will make RFID-SM's mandatory for certain groups of people. Minority groups mentioned around mandatory implants are asylum seekers, illegal immigrants, refugees, seasonal and temporary workers (Lupton, 2015:309). It is argued that implantation cannot be out of free will if poverty makes it necessary to seek work in another country to put food on the table back home. To make RFID-SM's a requirement for any of the aforementioned groups is highly distasteful in terms of human rights (Foster et al., 2008:47).

Talk about possible RFID-SM implants for minority groups spike fear that government may start with programs that mandate RFID-SM's for everybody in order to track, trace, monitor and document everyday movements and behaviour. The suspicion is that the government may use the 'common good', like better security against terrorist threats, the elimination of free riders from the public system and better public health, to motivate and implement RFID-SM implantation programs and that citizens may not have a choice or say in this.

Another concern that is brought up is that voluntary use of RFID-SM's today can become mandatory use tomorrow. The fear is that implants will be used in such a way that it diminishes freedom of choice. In terms of autonomy, this is totally unacceptable in a liberal democracy (Gadzheva, 2007: 221-222; Kahn, 2015:4).

Response:

Although there is a lot of talk, fear and even conspiracy theories around mandatory implants and the possibility of an Orwellian scenario, to date, none of them have materialized. RFID-SM's are too small to add GPS tracking functionality, and it is impossible to pick them up by satellite. RFID-SM's are passive devices with a short read-range and without batteries of their own. Batteries will need constant charging and replacement after a few years. There is neither standardization nor the extensive, compatible infrastructure (e.g. every square metre) to allow surveillance of this kind. Not locally, nationally or globally. Newer RFID-SM's are not covered in Bio-Bond anymore. This makes them too easy to remove and unsuitable to be implanted into people that government want to track. They are not the right kind of technology to be used as a government security device for people that need 24/7 or frequent surveillance (Aubert, 2011:676; Grauer, 2018). In addition to this, CASPIAN would prefer a total ban on the use of RFID-SM's by government. Several states in America have legislation in place to restrict governments' of them.

An RFID-SM implant is a tool for autonomous, obeying citizens that want to use it voluntarily and with informed consent. They are most suited for specific personal uses and purposes where they contribute to convenience, independent living and quality of life (Werber et al., 2018). The decision to get an RFID implant that is safely tucked away inside a person's body is a personal one for personal use and there is no reason to doubt that it will remain like that.

Conclusion:

Unfortunately, human RFID-SM's are surrounded by conspiracy theories, non-transparency, fear and trust issues. These ethical concerns are frequently based on errors made in the past, misperceptions of the capabilities of RFID-SM's, as well as negative and coercive publications (Grauer, 2018).

In a liberal democratic society, innocent citizens that make a voluntary, informed choice to implant an RFID-SM should not be intimidated not to have it if it is beneficial to them and not harmful to others. At the same time, RFID-SM's should never be mandatory for innocent citizens. Where possible, citizens should be allowed to choose freely between a luggable, wearable and implantable. There should always be an option to say no, to exit and remove the RFID-SM when not needed or wanted anymore - even where informed consent was obtained before the implant. Banning the use of RFID-SM's would be morally unacceptable because people have a moral right to this kind of technology unfettered by legal prohibition.

5 Unlimited Surveillance and Informational Privacy:

The most urgent criticisms of, or worries about, RFID-SM's concern their threat to informational privacy.

5.1 Informational Privacy:

Private information includes personal as well as sensitive information.

Personal information is information that is generated in the private and public spheres and that can easily be linked to a specific individual. It includes things like name, address and ID numbers (Van den Hoven, 2006:224).

Sensitive information is not the kind of information you like to share or be known, and it should not be harvested without consent (Lupton, 2015:316). Sensitive information includes age, gender, political opinions, race, religious beliefs and sexual orientation. It is possible to infer sensitive information where there is sufficient information collected on a specific individual.

Private information can be seen as part of ourselves or as an extension of ourselves. Informational privacy is about the control we have over our private information. This means that we should be able to decide what information about ourselves we want to make available, to whom, when, and to what extent. If we give too much of our private information away, we start to give parts of ourselves away. There must be some balance between what government, commerce and other entities know about us, the money (benefits) they make out of our private information and the gain we get out of it.

Although we have a moral right to privacy, as RFID-SMs' critics maintain, and we want to safeguard our private sphere, privacy is not an absolute right. We always have to weigh what we are prepared to share with what society (public sphere) needs or has a moral right to know in terms of the common good. Simply because RFID-SMs can undermine informational privacy to an extent, that doesn't necessarily undermine their worth, nor serve as an argument (by itself) to the effect that they should be banned.

In the paragraphs that follow, I will discuss the threat that RFID-SM use pose to informational privacy in comparison to other privacy invasive ICT.

5.2 The Impact of the Use of RFID-SM's on Unlimited Surveillance in Comparison to Other Privacy Invasive ICT:

5.2.1 Public Spaces:

In a liberal democratic society, the government needs sufficient information to keep citizens safe from potential harm emanating from malicious intent. They also need to know what services and infrastructure they need to provide to fulfil the needs of citizens in order to serve them best, e.g. public schools, hospitals, and roads.

Citizens are well documented by the government – from birth to death. These documents are all part of the public domain and probably available in digital format where they are easy to locate and access. Examples of the government's identifiable information are ID documents, passports, marriage certificates, divorce certificates, birth certificates, death certificates, criminal records, education levels, and qualifications. Although these documents are created in the public sector and perceived as public, it is also the private information of specific individuals. Citizens do not want these documents to be available to everybody everywhere because they value their private information.

We do not want what is available in the public sphere to be duplicated again and again. There is growing fear in society regarding the over-availability of private information in the public domain.

Despite existing documents available in the public domain, the government persistently harvest additional information on citizens. Authorities make use of closed-circuit television (CCTV) cameras that are strategically placed in public places. In some cases public officials wear body cameras to take footage of their interaction with citizens.

Citizens themselves contribute to what is available in the public domain. They post footage taken by cell phones (photos/videos) or dash cameras on social media. This footage can either be of officials that overstep their boundaries or of fellow citizens that offended them or committed crimes.

With the help of facial recognition software, it is possible to accurately identify individuals in the mentioned cases. The ethicality of surveillance and publication of private information is questionable where citizens are unaware that they are being surveilled, where they are not asked for consent nor given the opportunity to decline.

Some governments request big ICT developers to build in backdoors so that they can access citizens' personal information when needed. Backdoors can give access to cell phone conversations, e-mails, CCTV footage, social media, and Google searches. Governments also do GPS tracking via cell phones. All this is done in terms of the common good, to prevent harm or solve cases where harm was done.

Regarding RFID technology, there is fear that RFID readers will be embedded or affixed to park benches, garbage cans or lamp posts in public spaces (e.g. bus stations, airports, restrooms,

museums or sport arenas) and that any RFID enabled luggable, wearable or RFID-SM, may lead to accurate identification, tracking and tracing of innocent citizens. RFID-SM's have the potential to worsen the situation regarding surveillance considerably.

Response:

Surveillance in public is not new or unlawful and it will never stop. It may even intensify as ICT gets more invasive. There should be a notice somewhere stating that citizens are under surveillance. Surveillance in public spaces benefits the common good because it motivates citizens to obey laws and helps with law enforcement. Some people may feel that it is impeding on innocent individuals' privacy rights, but, as mentioned above, privacy is not an absolute right. It is always weighed against other rights. If public surveillance is done for the common good, it is more justifiable than if it is done by someone with malicious intent.

It is clear from the aforementioned that different sources and different ICT contribute to unlimited and continuous surveillance of citizens. Suppose an RFID-SM is only used in the private sphere for things like unlocking doors and switching on lights, and it is not linked to any network where it can become publicly known. In that case, it will be tough for the government to identify the implantee by his/her RFID-SM.

For RFID-SM's to contribute to unlimited surveillance and availability of private information, the unique 16-digit ID number of the RFID-SM should be registered on a public RFID system. Only then, a compatible public domain reader will be able to recognise and interpret the unique 16-digit ID number of the RFID-SM.

If the ID number and any other crucial information that is stored on the RFID-SM is encrypted and password protected, access to information on the RFID-SM can be controlled by the implantee and made available on a need to know basis only.

Due to limited storage capacity, the RFID-SM is not ideal to use as a storage device for dark secrets. The government may not even be interested in RFID-SM's for surveillance purposes.

5.2.2 Semi-Public Spaces:

5.2.2.1 Retail Establishments:

Commerce needs sufficient information to have the right stock in the right quantities available at the right price. They need to do this according to the needs and wants of potential clients in order to maintain a competitive edge. If they want to send out targeted advertisements, commerce needs to know who their potential clients are, e.g. who is in the market to buy a car or house, who is pregnant, who has children that go to school for the first time and what are the hobbies and interests of potential clients. To maximize profit, they must minimize theft. This is done by using CCTV cameras and by performing security checks at exit points.

Some retail environments are now doing item-level tagging. This means that consumers may come into regular contact with RFID tags. Tags can be attached to an object or embedded in an object that is for sale. If a tagged item is purchased by an implantee that is registered on the RFID system of a retail outlet and the tag of the purchased item is not de-activated/killed at point of sale, readers placed at the entrance and exit of the retail establishment where the tagged item was bought, can uniquely identify consumers carrying or wearing these tagged items when they are re-visiting the retail outlet where the item was purchased or even when they visit a retail outlet at another location that belongs to the same retail chain. Passive tags that are not de-activated

can forever communicate with compatible readers in close vicinity to them. The whereabouts, behaviour and purchasing habits of a specific, identified individual can then be studied over a very long time. There is a concern that a link between the real-life identity and the tagged object can be established (Lockton et al., 2005:223-224; Lupton, 2015:312; Malone, 2006:2-3).

Within an RFID enabled retail environment, both tags and readers can easily be hidden due to their small size and discreet functionality. Readers can be embedded or affixed to doorframes, under floor tiles, or they can seamlessly incorporate them into retail shelving and counters (McIntyre et al., 2015:14). Consumers can be surveilled, and their behaviour studied while touching tagged items shelved on RFID enabled "smart shelves". Video recordings can be made by hidden cameras and studied remotely by staff members without the consumer's knowledge or consent (Clarke et al., 518, 520).

Where RFID-SM's are implanted in humans, privacy advocates fear that RFID-SM's are even more privacy invasive than luggable and wearable tags because of the permanent link that is established between the real-life identity of the implantee and the RFID-SM as well as the possibility of harvesting identifiable private information, directly linkable to a specific individual (Gasson et al., 2013:262).

It is argued that where an RFID-SM is registered on a specific retail outlet's RFID network, it is possible that the implantee can be accurately identified upon entering the premises. Personal information recorded on an existing database on that person can be called up. Additional information on the whereabouts, behaviour, preferences and habits of that person can be tracked, traced and recorded inside the retail outlet before, during and after the sale – until the person exits the retail outlet. The fear is that this can be done without obtaining explicit consent from the client and that according to what is visible on the computer system, an implantee can be

discriminated against and maltreated or treated extremely well (Cochran et al., 2007:220-221; Garfinkel et al., 2005:34,39; Pelsak, 2005:335; Zalud, 2016:56-58).

Response:

Retail establishments have been collecting private information on shopping habits for decades. Wherever humans leave a digital footprint as they communicate, inquire or execute transactions during their daily lives, the use of ICT makes harvesting, storing, using, analysing, transferring, and duplication of personal information easier (Cochran et al., 2007:217).

When you enter a retail establishment where there is a sign indicating that CCTV cameras will observe you and you decide to enter anyway, you give consent and waive your right not to be surveilled.

When clients accept loyalty cards or membership cards and pay by credit or debit card, they knowingly or unknowingly enter into a "contract" and thereby imply consent for their private information to be harvested. In exchange for incentives like free services, discounts and preferential treatment, people allow businesses to harvest data from their financial and other transactions as they move through life (Van den Hoven, 2006:220).

At this stage, the number of RFID-SM's that are used for payment is minimal. If you purchase an RFID-SM over the Internet and have it implanted, you would have to ask specific retail outlets to link your unique 16-digit ID number to their RFID system if compatible. Suppose your RFID-SM is registered at one particular retail outlet, and you use it for payment there. In that case, it is assumed that you give consent to harvest and use the information generated by your RFID-SM (like when you are using your credit card and loyalty card).

The CCTV footage that retail environments record can be integrated with facial recognition software for accurate identification of clients. It is easy to study and analyse habits, behaviour and preferences of clients before, during and after the sale by watching the recordings. Legitimate surveillance concerns do not apply especially, or even at all, to RFID-SM's.

5.2.2.2 Workspaces

Workplaces need information on the whereabouts of employees to ensure effectiveness, productivity, safety and security. They can do this by using access cards that restrict certain people from entering certain places, software that counts keystrokes, session statistics built into the software, CCTV cameras, security staff, and managers that observe employee activity throughout the day.

Privacy advocates fear that the use of RFID-SM's in the workplace will supplement existing surveillance methods in the workplace and lead to even more monitoring, tracking and tracing of staff.

Response:

Over decades workplaces have issued staff members with luggable or wearable access cards. Workers accept these as part of the job without questioning their functionality or experiencing fear of being monitored, tracked or traced. The truth is that these RFID enabled access tools are activated by readers fitted to, e.g. security doors. They do register a log against an employee's name wherever or whenever they use their access cards. It always was and still is possible to call up the log history of security doors and other strategically placed readers, to determine a specific individual's time of arrival, time of departure, movement through the building and time spent within a specific part of the building. Employee movements have thus been stored (maybe

without the explicit informed consent of the employees); therefore, the possibility of monitoring, tracking and tracing part is nothing new. Luggable and wearable RFID access cards have longer read ranges than RFID-SM's, so they can be more privacy invasive than RFID-SM's. If the fear is around monitoring, tracking, and tracing within the workplace, the fear should be around luggables and wearables as well and not only around RFID-SM's.

It happens quite often that a fellow employee that misplaced lost or forgot his/her luggable or wearable access card somewhere ask to borrow the luggable or wearable access card of another employee (Rotter et al., 2012:32). Since movement is trackable, the innocent employee that borrowed his/her access card to the other person can land him/herself into trouble by being in places where s/he should not be or staying too long in certain areas, e.g. the cafeteria. Although innocent, it may be challenging to prove that it was not the owner of the access card's movements that were tracked. RFID-SM's make the borrowing of access cards impossible.

Monitoring of employee movement through the workplace need not be perceived as negative only. By monitoring movement through the building, it is not only possible to establish who was where, when and for how long. It is also possible to ensure that the "right people are at the right place at the right time" (Masters et al., 2005). In case of emergency, where it is necessary to evacuate the building, it is possible to establish who is still in the building and where s/he is located. Depending on the circumstances, this can be life-saving information.

5.2.3 Private Spaces:

Within private spaces, citizens should have the best control over who has access to what information about them, and when, and to what extent. It is becoming more difficult to keep the private sphere private because of increased use of privacy invasive ICT within private sphere of our lives.

Many devices like your RFID-SM, Fit bit, home security system, fridge, freezer, and TV can be linked to a network of some kind and thereby become "smart". Your smart TV or laptop can have a camera and microphone hidden in it that can record you and your family members. These devices can generate and communicate information, take sound clips, photos and videos. They can be operated over a distance using Wi-Fi and cell phone technology. Some families install cameras to observe their nannies or cleaners when they are at work. They use this footage as evidence for abuse or theft. Whether this is morally acceptable is debatable because the workers are not asked for consent nor informed beforehand. When the cameras are installed, family members can observe other family members over a distance without their knowledge or consent.

RFID technology is an enabler of “smart” environments. RFID is seen as one of the backbone technologies of the Internet of Things (IoT) or the Internet of Everything (IoE) that includes tagged/micro-chipped objects, animals and humans. The unique 16-digit ID number assigned to each RFID tag/micro-chip is sufficient to allow 10 billion people to identify 10 000 items uniquely. With a fully functioning IoE, everybody and everything worldwide can be identified, connected and able to communicate with each other 24/7 (McIntyre et al., 2015:17; Rotter et al., 2012:30,36).

It is argued that if a person is linked to the IoE with an RFID-SM, s/he becomes a data point that can be followed and monitored. It will be possible for everybody to know everything about everybody – where a person stays, what smart appliances s/he has in the house, what vehicle s/he drives, where s/he drives to, with whom and when (Britton, 2016:5). A system as invasive as this, with all its vulnerabilities, will void a person of informational privacy.

It is possible to implant biosensors with RFID capability that monitors bodily functions. These sensors can create a constant stream of private information that can be studied and stored

somewhere (e.g. in the cloud). The information can also be shared with a medical practitioner. The fear is that this information may fall into the wrong hands and lead to harm.

A further concern is that RFID-SM's cannot be switched off or left behind. Once implanted, it will be "alive", travelling with a person and communicating with compatible readers in close vicinity as a person moves from his/her home to his/her workplace or public spaces and vice versa (Gadzheva, 2007:218; Nisbet, 2004:213).

Response:

The aforementioned may sound frightening in terms of informational privacy, but it does not mean that if you invest in technology that can be "smart", you need to make it part of the IoE. The RFID system that consists of a microchip, reader, computer and database needs to be planned and set up for maximum efficiency. As the potential owner of the RFID-SM, you have the freedom to decide what kind of functionality you want or need and what tasks or applications you want to employ it for. Only then will you be able to purchase the most secure and applicable RFID-SM in order to achieve the outcome that you expect.

When the setup is done and fully functioning, automation of processes is possible. The reader will interrogate the RFID-SM and upon recognition commands will be executed. According to permissions granted during the setup, the following scenario may be possible – the doors of your car will open, the seats and mirrors will be adjusted, and your car will start (Rotter et al., 2012:34). The same applies to RFID enabled offices and homes where a person with an RFID-SM is accurately identified and therefore capable of opening doors, switching on music, lights, fans, computers, photocopiers with a mere wave of the hand (Foster et al., 2008:45; Gadzheva, 2007:220; Warwick, 2016).

As the owner of the RFID-SM, you have the control to decide what needs to be set up on a secure Private Area Network (PAN), what on a Local Area Network (LAN) and what on a Global Area Network (GAN). This decision and the security measures incorporated will have a considerable impact on your future informational privacy. You can then control what information you want to make available to whom, when. If you value your privacy, you should keep your network as private and secure as possible.

You can use the information generated by implantable biosensors to monitor your own bodily processes or you can share it with a healthcare professional. If you have a biosensor implant with NFC capability, it can easily link to your cell phone. Bodily data that is communicated to your cell phone can be e-mailed to a medical professional via a cell phone that is networked (Kaur, 2012:101).

Self-management of your private information is essential. Choose devices that can be networked carefully and study their possible impact on informational privacy so that you can make an educated decision. It is easy for private information to start off in the private domain and end up in the public domain. Once it is in the public domain, you will never be able to get it back into the private domain. Nobody else cares as you do about your personal information, and nobody will protect it as effectively as you can (if you want to). Nobody else will be harmed the way you are if your personal information is used against you.

Conclusion:

As we have seen from the foregoing, there are authorities and non-authorities that harvest our private information every day. They are using privacy invasive ICT like social media, Google, CCTV with facial recognition software, body cameras worn by public officials, and cell phones with cameras and GPS capability. ICT like Google and Face book offers free information, but we

pay in terms of private information harvested from us. We do not mind most of the time, but over-sharing, over-harvesting, and over-profiling become problematic when it harms us.

The possibility of establishing a link between a person's real-life identity and his/her activities, habits, and behaviour is not unique to RFID-SM's. Most of the threats posed to informational privacy are not unique to implants but rather a common problem posed by ICT in general and a general disrespect for private information caused by financial gain. The only way you can avoid the harvesting of personal information is by paying in cash, staying anonymous and avoiding shops where people know you or that issue membership or loyalty cards.

The purpose of an RFID-SM is, first and foremost, to accurately identify the implantee. If you have an RFID-SM and you enter a space that is RFID enabled and your RFID-SM is not registered on their RFID network, depending on what is stored on your RFID-SM and whether the necessary security features protect it, they may not be able to retrieve any useful information.

5.3 Big Data:

There is an abundance of data available emanating from different sectors. Most of the data is stored in the form of databases for later use. Private information can be added and/or removed over many years. Databases may be limited in content, e.g. including the private information of people in a neighbourhood that share the same interests, or they can be huge, including private information of people from all over the globe that belong to an international organization, drive or scheme.

Powerful ICT makes it possible to store massive amounts of data, merge huge databases that originated in different spheres, de-identify data, and do deep mining on the data. Helpful profiles

are built and used for decision-making based on trends, habits, behaviour, and interests. The profiles are seen as the new gold and sold to interested parties.

The problem with information being processed automatically and by several unknown entities is that in the end, people do not know what information is collected by whom when they have collected it, for what purpose, where it is stored, for what period it is stored, what it is used for, who has access to it, what is combined with what, if it is re-identified, to whom it was sold, or whether it is safely stored (Catherwood et al., 2015:5).

It is evident that there are a lot of uncertainties around the harvesting and processing of personal information. Consent is not always asked nor always given. Giving consent in one instance does not mean you give up consent in all cases further down the line, but as information is re-packaged and re-sold, you lose control more and more. As we have seen from the retail environment, consent is sometimes assumed where loyalty cards or membership cards are accepted or where payments are made by credit card or RFID-SM's.

Response:

RFID-SM's are tools that make accurate identification possible. They do not contribute as much information to be harvested as other more privacy-invasive technologies. Most of the communication happens through keys (ID numbers) that are either uploaded to the RFID-SM or the 16-digit ID number of the RFID-SM that is linked to compatible external readers. The RFID-SM has the capability of encryption as well as password protection. The reader allows multi-level security features like a password and biometrics (e.g. fingerprint and facial recognition). The ID numbers on the RFID-SM can thus be well protected. Storage capacity on the RFID-SM is still limited. Storing big documents or a lot of personal information on the RFID-SM is not possible. RFID-SM's may contain crucial identification information, crucial medical information or a small

encrypted document. Where business cards are uploaded to NFC-SM's, the purpose is to share the information because you want other people to have the information.

Where information is generated via bio-sensors and shared with a medical professional, the medical condition of the person may be so severe that what is gained in terms of life-saving treatment is more beneficial than the potential loss of informational privacy.

Conclusion:

Taking everything into account, it is clear that RFID-SM's do not contribute significantly to big data.

Conclusion Part 5:

We love the convenience, connectedness and abundance of information that ICT brings to our fingertips. We are willing to sacrifice some of our informational privacy because we find it extremely beneficial. ICT is becoming more and more privacy invasive and we are surveilled on a constant basis. As the processing and networking capabilities of ICT increase, the ability to generate, harvest, store, use, analyse, combine, profile, and sell vast amounts of information faster and cheaper than ever before, also intensifies. Our informational privacy is eroded over time, and we are losing control of our valuable private information as it increasingly becomes available in the public domain. Once information is out in the open (public domain), it is impossible to get it back into the private domain. Contrary to privacy concerns around RFID-SM's are not as privacy invasive as other ICT, neither do they contribute to the problem of big data to the extent that other ICT do.

6 Illicit access to personal information: (threat to privacy by abuse)

6.1 The role of the use of RFID-SM's in illicit access to personal information:

Private information is a valuable commodity. With millions of people surfing and transacting on the Internet on a daily basis, there is a wealth of confidential information that can be harvested, analyzed, profiled and sold. The risk of illicit use of personal information in the digital world emanate from a global pool of highly skilled computer experts that may have harmful intent.

RFID-SM's make use of radio waves that are invisible to the human eye. Illegal interception of signals occurs silently, over a distance, in real-time and without the necessity of line of sight. The RFID-SM cannot be switched off, so it is argued that once implanted, the RFID-SM will always be on, communicating with compatible readers in close vicinity. The fear is that the person with the implant will never know what information is shared with whom, when, and where because there is no history kept on previous communications (Ferguson, Thornley & Gibb 2014:118).

Objection:

In order to intercept the communication unobtrusively, the existence, location and purpose of the RFID-SM should be known to the unauthorized interceptor. Just as the communication between the RFID-SM and the reader is invisible to the naked eye, so is the existence of the RFID-SM to those that do not know about it.

Bill and Melinda Gates sponsored a project on implantable contraceptives called Micro-chipS. These implants can last for 16 years under the skin, and they can be controlled by switching them on and off as needed. When a woman wants to get pregnant, it can be switched off, and after the baby's birth, it can be switched on again (Heffernan et al., 2016:54).

There has been a lot of talk around an on/off switch or a push-button that allows access to information stored on the RFID-SM's, when needed (Malone, 2006:2; Michael, 2017:6). This will give the implantee control over the device and its communication to the outside world. If it is possible to switch a sub-dermal contraceptive implant on and off, it may be possible to do the same with RFID-SM's.

It may be possible to 'switch' a re-writable RFID-SM 'off' by deleting all links to readers and databases when access to them is not needed.

An RFID-SM forms part of an RFID system where each part of the system is vulnerable to illicit access and abuse. The latest generation RFID-SM's have encryption and password protection. There is also minimal information on the RFID-SM itself. The database may be more at risk than the RFID-SM itself. In what follows, I will discuss the most critical threats posed by hacking, cloning and viral spread as they relate to the different parts of the RFID system itself – the RFID-SM, the reader and the database. The question that needs to be answered is whether RFID-SM's contribute significantly to the abuse of private information.

6.1.1 Hacking:

Hacking can be seen as unauthorized access where no right, authority or consent is given before the illicit access or abuse of personal information. The hacker can steal, damage, alter or delete valuable information. Stolen personal information can be held ransom, sold to the government, commerce or any other interested party (some of whom may have malicious intent), or it can be published in the public domain where it is "up for grabs" and open to abuse.

Possible harm includes humiliation, reputational damage, relationship problems, loss of employment, loss of insurance, identity theft and financial ruin. Tampering with the information,

e.g. medical information, to the extent that “false” unreliable information reaches the doctor, may lead to the wrong treatment and possibly even death (Al-Janabi et al., 2017:115,117).

Within an RFID system, the RFID-SM holds a unique 16-Digit ID number. A compatible, authorized reader serves as a link between the RFID-SM and a database that contains more detailed information than what is stored on the RFID-SM (Gasson et al. 2013:251-252). Hackers can easily exploit vulnerabilities in RFID-SM's, readers as well as databases.

Older generation RFID-SM’s are vulnerable to abuse because they have limited security features built into them (Lockton et al., 2011:222). The fear is that an unauthorized reader may be used to get illicit access to a database via an unprotected 16-digit ID number on an RFID-SM.

Virtually anybody can develop a database. The people who create them do not always know how to secure them properly, or security issues may not be important to them. Databases may be stored on computers that are linked to networks, e.g. PAN's, LAN's or GAN's. Depending on the database's size, the security of the database, the depth of data mining and the connectedness to other databases, illicit access to a database can lead to harm suffered by thousands of innocent, unsuspecting individuals regarding their private information (Britton, 2016:3-4).

Objection:

Older generation RFID-SM’s like the VeriChip can be protected by a 3-digit password. They have minimal storage capacity, so the only information retrievable from the RFID-SM itself is the unique 16-Digit ID number of the RFID-SM. Where the unique 16-digit ID number of the RFID-SM gives access to a medical database via an RFID reader, especially where the implantee is unconscious and/or cannot speak for him/herself, the implantee would want to make it as easy as possible for

the authorized people to gain access to the applicable information. The implantee may not want the RFID-SM to be password protected as it may complicate ease of access during a crisis.

If, for a valid reason, the 16-digit ID number is not protected by a password, the security should come from the reader. Access to the database can be linked to a password or biometric features needed by the reader. The password of a paramedic on the emergency scene should give him/her access to crucial information s/he needs to stabilize the patient and start appropriate treatment. The password of the doctor should give him/her access to all the medical information of the patient.

The database itself can be password protected and set up so that any attempt to access the database outside an emergency will flag a security alert.

Newer RFID-SM's have more storage capacity on the RFID-SM itself. They also have more security features like encryption and strong password protection. This makes it difficult to hack into them. The read range of the specific RFID-SM chosen by the implantee (with security and purpose in mind) may be limited. The transfer rate of data between devices is still slow. The aforementioned makes it challenging to intercept communication (Heffernan et al., 2016:55).

The micro-chips embedded in bank cards, ID documents and passports have a read range of around 30m. This read range is a lot longer than the read range of an RFID-SM. It is easier for a criminal to unobtrusively scan the data on the luggable in your wallet than to scan the information on an RFID-SM (Brown, 2016).

The latest readers offer password as well as biometric feature protection (fingerprint and facial recognition). Suppose in the example of the VeriChip, the medical officer gives the reader and

password to an unauthorized person, and there is abuse of personal information due to unauthorized access to the database. In that case, the RFID-SM can hardly be blamed.

The threat of hacking into databases is, however, not exclusive to RFID-SM's. It is a problem of ICT in general (Catherwood et al., 2015:3).

The fact that hackers are usually anonymous makes them feel safe, and they are good at covering up their tracks.

6.1.2 Cloning:

Cloning refers to making a copy or replica from the original RFID-SM that looks and acts the same as the original RFID-SM. Jonathan Westhues was able to hack and clone an RFID-SM in 2006. Until then, the common belief was that the RFID-SM is secure and safe, "immune to theft" (Fowler, 2019:2; Gadzheva, 2007:224).

It is argued that identity theft through cloning is a strong possibility because there is a lack of security measures within the RFID-SM. The information can be transferred to another RFID-SM and implanted in another person. The new implantee can then transact fraudulently using the identity of the original person. Irreversible reputational and financial harm can be done to the victim of identity fraud or theft (Lupton, 2015:312; van Hooijdonk, 2017:6; Van den Hoven, 2006:219).

There is fear that when people are close to you, e.g. when they sit next to you in the train, bus, aeroplane or they stand next to you in an escalator or on an elevator, they may be able to clone your RFID-SM.

Objection:

Latest generation RFID-SM's have built-in security features that make them safer to use than first-generation RFID-SM's in terms of protecting private information. Depending on the purpose, a specific RFID-SM is chosen. With a low-frequency RFID-SM, the data transfer rate can be prolonged, and only small amounts of data can be transferred between devices. On average, the read range of an implanted RFID-SM is under 10 cm. With NFC technology, the read range is even shorter (1-2cm). You have to press the micro-chip against the reader for a few seconds for communication to take place. The slow transfer rate of limited amounts of data, as well as the short read range of RFID-SM's, is beneficial in terms of security and confidentiality as it makes opportunistic cloning attempts more difficult (Aubert, 2011:677, 680; Heffernan et al., 2017:59).

If an unauthorized person succeeds in cloning the RFID-SM, what is retrieved may not be interpretable or usable due to encryption and other safety features built into the RFID-SM, the reader and the database.

No form of ICT is immune to abuse (Catherwood et al., 2015:3). If a wallet or bank card is stolen, the bank is informed, and transactions are stopped immediately. If an RFID-SM is compromised, the ID number (link) can be removed from the RFID system to prevent illicit access. This will render the RFID-SM clone useless (Grauer, 2018). Another (new) link can be uploaded to restore authorized access.

Additional security features make cloning or forceful removal more complicated and even redundant.

6.1.3 Viral spread:

The case used in the literature to demonstrate the possibility of viral spread regarding RFID-SM's is that of Mark Gasson, a lecturer at the University of Reading. In 2009 he implanted a microchip in his arm to automatically open security doors from a distance. A year later, Gasson deliberately infected his RFID-SM with a computer virus that spreads easily. This rendered certain areas of the university inaccessible to co-workers and sparked fear that RFID-SM's can easily be infected by viruses. If a virus infects an RFID-SM, the implantee may suffer harm due to distorted information. The implantee may even cause unintended harm to others in terms of their informational privacy via a virus that spread from one device to another (Spector, 2014:1).

The fear is that interconnectivity between the RFID-SM, reader, database and computer network (PAN, LAN, GAN) may lead to viral spread. The RFID-SM inside a person may become infected with a computer virus, and the infected RFID-SM may spread the virus to other computers or RFID-SM's (Gasson et al. 2013:253; van den Hooven, 2006:219).

Objection:

Although Mark Gasson was able to infect his RFID-SM with a virus, it is not that easy to do in real life, as it involves a trail of deliberate errors by different parts of the system (Grauer, 2018).

A virus, in simple terms, is a malicious instruction that is either executed under duress or inadvertently. For a virus to successfully infect an RFID system, the system would have to be instructed to execute a command received from an RFID-SM. This is not a typical use of RFID technology and would not be possible on a standard system.

Conclusion:

Between the RFID-SM, reader and database, most harm (to the innocent) and most gain (to those with malicious intent) comes from illegal access to the database. Illegal access to the microchip will mostly be an opportunistic crime because the implantee can erase and re-load certain information or apps as needed on a specific day. The person with malicious intent may not know what is available on the RFID-SM on a specific day (unless s/he observes the implantee very closely).

By choosing the most applicable, purpose-specific RFID-SM with built-in security features, shortest effective read range and slow data transfer, you can minimize the risk posed to RFID-SM's in terms of hacking, cloning and viral spread.

If the RFID-SM reader and the database are secured, the chances of abuse aimed at the RFID-SM itself or the database will be greatly reduced.

7 Final Comments/Justification:

There are several different RFID tags available in the marketplace. Different types of tags are best suited for specific predetermined uses. It is essential to differentiate between active, semi-passive, passive non-implantable and passive implantables because they all have different frequencies, capabilities and purpose of use.

The focus of this research report is on passive implantables. RFID-SM's have developed considerably from the first generation to the latest generation. They have shorter read ranges than luggables and wearables, and they have more storage capacity on the RFID-SM itself than before. They are now more secure, capable of encryption and password protection. They are available in the re-writable format, so information can be uploaded and removed as needed. A small document or crucial personal information can be uploaded to the RFID-SM. The functionality of luggables usually carried around in your wallet, pocket or handbag can be uploaded to purpose-specific RFID-SM's. This brings convenience to a new level as it allows you to navigate lightly and seamlessly through daily activities without the fear of forgetting, losing or misplacing essential luggables like keys, credit/debit cards, ID cards and access cards. Repetitive tasks (e.g., opening and closing as well as switching on and off) can be automated. This can especially be beneficial to disabled persons.

RFID-SM’s allow dignified, free movement within an RFID enabled area. This is ideal for people with cognitive impairments. Within a medical environment, the use of RFID-SM’s can contribute to fast, accurate, preventative and possibly lifesaving treatment. A personalized gun has the potential to prevent or limit harm to self and others.

Latest generation RFID-SM's include multi-level security factors. They can be used for identification as well as authentication. RFID-SM's are moving towards establishing a digital identity to combat fraud in the digital world.

We love the convenience, connectedness and abundance of information that ICT brings to our fingertips. We are willing to sacrifice some of our informational privacy because we find it extremely beneficial. ICT is becoming more and more privacy invasive and we are surveilled on a constant basis. As the processing and networking capabilities of ICT increase, the ability to generate, harvest, store, use, analyse, combine, profile, and sell vast amounts of information faster and cheaper than ever before, also intensifies. Our informational privacy is eroded over time, and we are losing control of our valuable private information as it increasingly becomes available in the public domain. Once information is out in the open (public domain), it is impossible to get it back into the private domain.

There are authorities and non-authorities that harvest our private information every day. They are using privacy invasive ICT like social media, Google, CCTV with facial recognition software, body cameras worn by public officials, and cell phones with cameras and GPS capability. ICT like Google and Face book offers free information, but we pay in terms of private information harvested from us. We do not mind most of the time, but over-sharing, over-harvesting, and over-profiling become problematic when it harms us. Contrary to privacy concerns around RFID-SM's, they are not as privacy invasive as other ICT, neither do they contribute to the problem of big data to the extent that other ICT do.

The possibility of establishing a link between a person's real-life identity and his/her activities, habits, and behaviour is not unique to RFID-SM's. Most of the threats posed to informational privacy are not unique to implants but rather a common problem posed by ICT in general and a

general disrespect for private information caused by financial gain. The only way you can avoid the harvesting of personal information is by paying in cash, staying anonymous and avoiding shops where people know you or that issue membership or loyalty cards.

Between the RFID-SM, reader and database, most harm (to the innocent) and most gain (to those with malicious intent) comes from illegal access to the database. Illegal access to the microchip will mostly be an opportunistic crime because the implantee can erase and re-load certain information or apps as needed on a specific day. The person with malicious intent may not know what is available on the RFID-SM on a specific day (unless s/he observes the implantee very closely). What is retrieved, may be very limited, encrypted and not useful at all.

By choosing the most applicable, purpose-specific RFID-SM with built-in security features, shortest effective read range and slow data transfer, you can minimize the risk posed to RFID-SM's in terms of hacking, cloning and viral spread.

If the RFID-SM reader and the database are secured, the chances of abuse aimed at the RFID-SM itself or the database will be greatly reduced.

Unfortunately, human RFID-SM’s are surrounded by conspiracy theories, non-transparency, fear and trust issues. These ethical concerns are frequently based on errors made in the past, misperceptions of the capabilities of RFID-SM’s, as well as negative and coercive publications.

In a liberal democratic society, innocent citizens that make a voluntary, informed choice to implant an RFID-SM should not be intimidated not to have it if it is beneficial to them and not harmful to

others. At the same time, RFID-SM's should never be mandatory for innocent citizens. Where possible, citizens should be allowed to choose freely between a luggable, wearable and implantable. There should always be an option to say no, to exit and remove the RFID-SM when not needed or wanted anymore - even where informed consent was obtained before the implant. Banning the use of RFID-SM's would be morally unacceptable because people have a moral right to this kind of technology unfettered by legal prohibition.

We have a moral right to privacy and a moral right to protect our privacy. Some ICT deplete us of privacy. RFID-SM's if used correctly may protect us from those with malicious intent and it may give some control over privacy back. Various objections have been raised against the use of RFID-SM's. They have been responded to. These objections do not undermine the virtues of RFID-SM's.

This research report studied some aspects around RFID-SM use from and ethical point of view. In order to draw a full conclusion around the ethical use of RFID-SM's, other aspects not studied in this research report need to be considered as well.

8 Bibliography:

Al-Janabi, S., Al-Shourbai, I., Shojafar, M. & Shamshirband, S. 2017. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal, 18:113-122*. Available **https://www.sciencedirect.com/science/article/pii/S1110866516300482**> (accessed 21 December 2020).

Al-Sebae, M. & Abu-Shanab, E. 2015. Big Issues for a Small Piece: RFID Ethical Issues. *ICIT 2015 The 7th International Conference on Information Technology.* Available <**https://www.researchgate.net/profile/Emad_Abu-Shanab/publication/277910581_Big_Issues_for_a_Small_Piece_RFID_Ethical_Issues/links/55d21f1908ae0b8f3ef777bf/Big-Issues-for-a-Small-Piece-RFID-Ethical-Issues.pdf**> (accessed 10 September 2018).

Aubert, H. 2011. Nanoscience and nanotechnologies: hopes and concerns. RFID technology for human implant devices. *ComptesRendusPhysique*, 12 (7):675-683.

Billing, M. 2019. Human chipping - will it ever go mainstream? Available <https://sifted.eu/articles/human-chipping-sweden-obsolete-before-reaching-mainstream/> (accessed 3 January 2019).

Britton, K. 2016. Handling Privacy and Security in the Internet of Things. *Journal of Internet Law*, 19 (10):3-7.

Brown, A. 2016. Human Micro-chipping: An Unbiased Look at the Pros and Cons. Human micro-chipping? What's that? Available <https://medium.freecodecamp.org/human-micro-

chipping-an-unbiased-look-at-the-pros-and-cons-ba8f979ebd96> (accessed 10 September 2018).

Catherwood, P.A., Finlay, D.D. & McLaughlin, J.A.D. 2015. Subcutaneous body area networks: A SWOT analysis. *2015 IEEE International Symposium on Technology and Society (ISTAS)*, Dublin, pp. 1-8.

Church of the Great God. 2018. Is the 'Mark of the Beast' an Implanted Micro-chip (Revelation 13:16-18)? Available <https://www.cgg.org/index.cfm/fuseaction/Library.sr/CT/BQA/k/79/Is-Mark-of-Beast-an-Implanted-Micro-chip-Revelation-1316-18.htm> (accessed 10 September 2018).

Clarke, I & Flaherty, T.B. 2008. RFID and Consumer Privacy. *Journal of Internet Commerce*, 7(4):513-527.

Cochran, P.L., Tatikonda, M. V. & Magid, J.M. 2007. Radio Frequency Identification and the Ethics of Privacy. *Organizational Dynamics*, 36(2):217-229.

Darrow, B. 2017. 'Ick Factor' and Biometrics Limit Market for Implanted Security Chips. Available < https://fortune.com/2017/08/02/implanted-chips-vs-biometrics/> (accessed 25 April 2020).

Dass, J. 2019. Etisalat introduces micro-chip implant to UAE residents. Available <https://filipinotimes.net/technology/2019/10/11/etisalat-introduces-micro-chip-implant-uae-residents/> (accessed 3 January 2019).

De Bruyn, M. 2014. The Protection of Personal Information Act (POPI). *International Business & Economics Research Journal*, 13(6):1315-1340.

DeCew, J. 2018. Privacy. *The Stanford Encyclopedia of Philosophy*. Available<https://plato.stanford.edu/entries/privacy/> (accessed 10 September 2018).

European Commission, 2018. A new era for data protection in the EU: What changes after May 2018. *European Commission.* Available <https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf> (accessed 10 September 2018).

Ferguson, S., Thornley, C., & Gibb, F. 2014. How do libraries manage the ethical and privacy issues of RFID implementation: A qualitative investigation into the decision-making processes of ten libraries. *Journal of Librarianship and Information Science*, 47(2):117-130.

Ferguson, S., Thornley, C., & Gibb, F. 2016. Beyond codes of ethics: how library and information professionals navigate ethical dilemmas in a complex and dynamic information environment. *International Journal of information management*, 36:544-556.

Foster, K.R. & Jaeger, J. 2007. RFID inside: The murky ethics of implanted chips. *IEEE Spectrum*, 44(3):24-29.

Foster, K.R. & Jaeger, J. 2008. Ethical Implications of Implantable Radiofrequency Identification (RFID) tags in humans. *American Journal of Bioethics*, 8(8):44-48.

Fowler, M.C.C. 2019. Chipping Away Employee Privacy: Legal Implications of RFID Micro-chip Implants for Employees. *The National Law Review*. Available: <https://www.natlawreview.com/article/chipping-away-employee-privacy-legal-implications-rfid-micro-chip-implants-employees> (accessed 4 January 2019).

Fried, C. 1968. Privacy. *Yale Law Journal*, 77(3):475-493.

Frith, J. 2020. Radio-Frequency Identification: The Shadow of a Once Feared Technology Looms Large. Available: < https://thereader.mitpress.mit.edu/radio-frequency-identification-shadow-looms-large/#:~:text=Subscribe-,Radio%2DFrequency%20Identification%3A%20The%20Shadow%20of%20a,Once%2DFeared%20Technology%20Looms%20Large&text=Domestic%20pets%20have%20RFID%20tags,words%2C%20RFID%20tags%20are%20everywhere.> (accessed 2 April 2021).

Gadzheva, M. 2007. Getting Chipped: To Ban or Not to Ban. *Information & Communications Technology Law*, 16(3):217-231.

Gasson, M.N. & Koops, B.J. 2013. Attacking Human Implants: A New Generation of Cybercrime. *Law, Innovation & Technology*, 5(2):248-277.

Gauttier, S. E. J. 2018. 'I've got one under my skin' – The role of ethical consideration in the (non-) acceptance of insideables in the workplace. *Technology in society*. Available: <https://www.sciencedirect.com/science/article/pii/S0160791X18301118> (accessed 9 October 2018).

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

Grauer, Y. 2018. A practical guide to micro-chip implants. Available: https://arstechnica.com/features/2018/01/a-practical-guide-to-micro-chip-implants/?comments=1&post=34566757> (accessed 2 October 2020).

Heffernan, K.J., Vetere, F. & Chang, S. 2016. Insertables: I've Got IT Under My Skin. Available: <http://interactions.acm.org/archive/view/january-february-2016/insertables> (accessed 9 October 2018).

Heffernan, K.J., Vetere, F., Chang, S. 2017. Military Insertables: Lessons from Civilian Use. *IE**EE Technology and Society Magazine**,* 36(1):58-61.

Kahn, N.A., 2015. RFID's Chip Implants and their related Ethical Issues. Available: https://www.researchgate.net/publication/280933310_RFIDs_Chip_Implants_and_their_related_Ethical_Issues> (accessed 25 September 2020).

Kosta, E. & Bowman, D.M. 2011. Treating or Tracking? Regulatory Challenges of Nano-Enabled ICT Implants. *Law and Policy*, 33(2):256-275.

Kaur, S. 2012. How are the Embedded Chips Going to Affect our Lives? *IETETechnical Review*, 29(2):101-104.

Lockton, V. & Rosenberg, R.S. 2005. RFID: The next serious threat to privacy. *Ethics and Information Technology*, 7(4):221-231.

Lomas, N. 2015. What happens to privacy when the Internet is in everything? *Tech Crunch*. Available: <https://techcrunch.com/2015/01/25/what-happens-to-privacy-when-the-internet-is-in-everything/> (accessed 3 January 2019).

Luck, R. 2014. POPI - is South Africa keeping up with international trends? *De Rebus*, May:44-46.

Lupton, M. 2015. The ethics of the VeriChip human implant. *Asian Journal of WTO & International Health Law and Policy*,*10*(1):307-320.

Madrid, C, Korsvold, T., Rochat, A. & Abarca, M. 2012. Radio Frequency Identification (RFID) of Dentures in Long-Term Care Facilities. *The Journal of Prosthetic Dentistry*. 107(3):199-202.

Magi, TJ 2011. Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature. *The Library Quarterly*, 81(2):187-209.

Malone, R. 2006. Can RFID Invade Your Privacy? Available: <https://www.forbes.com/2006/12/05/privacy-rfid-tags-biz-logistics-cx_rm_1207rfid.html?sh=147042ab5b22> (accessed 29 November 2020).

Mance, J. 2009. Human rights, privacy and the public interest-who draws the line and where? *Liverpool Law Review*, 30(3):263-283.

Mass, W. 2014. RFID Implants: The Benefits vs. the Dangers. *The New American*. Available: <https://www.thenewamerican.com/tech/computers/item/17688-rfid-implants-the-benefits-vs-the-dangers> (accessed 24 September 2018).

Masters, A. & Michael, K. 2005. Humancentric Applications of RFID Implants: The Usability Contexts of Control, Convenience and Care. *Second IEEE International Workshop on Mobile Commerce and Services*, Munich, 2005, pp. 32-41.

McCloskey, H. J. 1980. Privacy and the Right to Privacy. *Philosophy*, 55 (211):17–38.

McIntyre, L., Michael, K. & Albrecht, K. 2015. RFID: Helpful New Technology or Threat to Privacy and Civil Liberties? *IEEE Potentials*, 34(5):13-18.

Meyer, H.J., Chansue, N., Monticelli, F. 2006. Implantation of radio frequency identification device (RFID) micro-chip in disaster victim identification (DVI). *Forensic Science Journal*, 157(2-3):168-171.

Michael, K. 2016. RFID/NFC implants for bitcoin transactions. *IEEE Consumer Electronics Magazine*, 5(3):103-106.

Michael, K. 2017. Go “Get Chipped” A Brief Overview of Non-Medical implants between 2013-2017 (Part 2). *IEEE Technology and Society Magazine*, December

Michael, K. & Michael, M.G. 2010. The diffusion of RFID implants for access control and e-payments: A case study on Baja Beach Club in Barcelona. *International Symposium on Technology and Society, Proceedings*, pp. 242-252.

Michael, K., Michael, M.G. 2013. The future prospects of embedded micro-chips in humans as unique identifiers: the risks versus the rewards. *Media, Culture and Society*, 35 (1):78-86.

Monahan, T. & Fisher, J. 2010. Implanting inequality: empirical evidence of social and ethical risks of implantable radio-frequency identification (RFID) devices. *International journal of technology assessment in health care*, 26(4):370-6.

Moore, A. 2008. Defining Privacy. *Journal of Social Philosophy*, 39(3):411-428.

Nagel, T. 1995. Personal Rights and Public Space. *Philosophy & Public Affairs*, 24(2):83-107.

Niemeijer, A. & Hertogh, C. 2008. Implantable tags: Don't close the door for Aunt Millie! *American Journal of Bioethics*, 8(8):50-52.

Nisbet, N. 2004. Resisting Surveillance: Identity and Implantable Micro-chips. *Leonardo*, 37(3):211-214.

Nissenbaum, H. 1998. Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17:559-596.

O'Connor, M.C. 2009. RFID gives dementia patients their freedom. *RFID Journal*. Available: <http://www.rfidjournal.com/articles/view?4610> (accessed 24 September 2017).

OECD. 1980. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *OECD*, 1980:63. Available: <http://www.oecd-ilibrary.org/docserver/download/9302011e.pdf?expires=1496137110&id=id&accname=oci

d194738&checksum =DBA5D32B47DF7D9CCC423E89562B36F5> (accessed 14 September 2017).

Patel, Y.J. 2017. Future Scope of RFID Technology and Advantages & Applications. *International Journal of Scientific Research in Science, Engineering and Technology IJSRSET*, 3(8):542-548.

Paulin, I.M., Clark, J., O'Brien,J. 2018. The Ethics of Paternalism: Should policy makers intervene to make people stop doing things that are bad for them? Available: https://blogs.scientificamerican.com/observations/the-ethics-of-paternalism/> (accessed 27 March 2021).

Pelsak, A.R. 2005. An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics*, 59(4):327-345.

Ramesh, E.M. 1997. Time Enough - Consequences of Human Micro-chip Implantation. *RISK: Health, Safety & Environment,* 8 (4):373-407.

Rodriguez, D.A. 2019. Chipping in at work: Privacy Concerns Related to the Use of Body Microchip ("RFID") Implants in the Employer-Employee Context. *Iowa Law Review*, 104(3):1581-1611.

Rosenberg, I.B. 2008. Involuntary Endogenous RFID as a Condition of Federal Supervised Release——Chips Ahoy? *Federal Sentencing Reporter*, 21(1):23-28.

Rotter, P., Daskala, B., Compañó, R., Anrig, B. & Fuhrer, C. 2012. Potential Application Areas for RFID Implants. In: Gasson M., Kosta E. & Bowman D. (eds) *Human ICT Implants: Technical, Legal and Ethical Considerations*. Information Technology and Law Series, vol 23. The Netherlands. T.M.C. Asser Press.

SAICA, 2017. Available: <https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPersonalInformationAct/tabid/3335/language/en-ZA/Default.aspx > (accessed 14 September 2017).

Savage, M. 2018. Thousands of Swedes are inserting Micro-chips under their skin. Available https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-micro-chips-under-their-skin (accessed 17 December 2020).

Smith, A.D. 2007. Evolution and acceptability of medical applications of RFID implants among early users of technology. *Health Marketing Quarterly*, 24(1-2):121-55.

South African Government. 2018. The Constitution of the Republic of South Africa. Available <https://www.gov.za/documents/constitution/constitution-republic-south-Africa-1996-1> (accessed 10 September 2018).

Spector, D. 2014. Micro-chips will be implanted into healthy people sooner than you think. Available https://www.businessinsider.com/micro-chip-implants-in-healthy-people-2014-7?IR=T#:~:text=Micro-chips%20Will%20Be%20Implanted%20Into%20Healthy%20People%20Sooner%20Than

%20You%20Think&text=In%20March%202009%2C%20British%20researcher,into%20a%20walking%20swipe%2Dcard (accessed 25 September 2020).

Tuffley, D. & Antonio, A. 2016. Ethics in the Information Age. *Australian Quarterly,* 87(1):19-40.

United Nations. 2018. *Universal Declaration of Human Rights*. Available: <http://www.un.org/en/universal-declaration-human-rights/> (accessed 10 September 2018).

Van den Hoven, J. 2006. Nanotechnology and Privacy: The Instructive Case of RFID. *International Journal of Applied Philosophy,* 20(2):215-228.

Van den Hoven, J., Blaauw, M., Pieters, W.&Warnier, M. 2014. Privacy and information technology. *Stanford Encyclopedia of Philosophy*.

Van Hooijdonk, R. 2017. Human micro-chipping. The benefits and downsides. Available: <https://www.richardvanhooijdonk.com/en/blog/the-benefits-and-downsides-human-micro-chipping/> (accessed 10 September 2018).

Want, R. 2008. The Bionic Man. *IEEE Pervasive Computing*, 7(1):2-4.

Warren, S. & Brandeis, L. 1890. The right to privacy. Originally published in *Harvard Law Review* 4 (5):193-220. Available: <https://www.jstor.org/stable/pdf/1321160.pdf> (accessed 9 October 2018).

Warwick, K. 2016. Meet the bio-hackers who enhance their human bodies with technology. Available:

http://thescienceexplorer.com/technology/meet-biohackers-who-enhance-their-human-bodies-technology (accessed 10 September 2018).

Werber, B., Baggia, A., Znidarsic, A. 2018. Factors Affecting the Intentions to Use RFID Subcutaneous Microchip Implants for Healthcare Purposes. *Organizacija*, 51(2):121-133.

Zalud, B. 2016. The “Almost Everything” Tool. Available: <https://www.securitymagazine.com/articles/86954-rfid-the-almost-everything-tool> (accessed 29 November 2020).