2008

Amal Graafstra- The Do-It-Yourselfer RFID Implantee: The culture, values and ethics of hobbyist implantees: a case study

R. Ip
University of Wollongong

Katina Michael
University of Wollongong, katina@uow.edu.au

M G. Michael
University of Wollongong, mgm@uow.edu.au

Publication Details

This conference paper was originally published as Ip, R, Michael, K, & Michael, MG, Amal Graafstra The Do-It-Yourselfer RFID Implantee: The culture, values and ethics of hobbyist implantees: a case study, Cultural Attitudes Towards Technology and Communication (CATAC08), Nimes, France, 24-27 June, 2008, pp. 1-15.

Amal Graafstra- The Do-It-Yourselfer RFID Implantee: The culture, values and ethics of hobbyist implantees: a case study

Abstract
This paper provides insights into the culture, values and ethics of do-it-yourself microchip implantees. Microchip implantees are people who have opted to bear a radio-frequency identification (RFID) device beneath their skin for particular electronic applications. This paper uses a single case study of the most prominent hobbyist microchip implantee, Mr Amal Graafstra of the United States, to explore the preliminary motivations for being implanted, the actual chip experience, and the subsequent repercussions of being an implantee. The data for this paper was collected using two main techniques, a primary interview with the case subject, complemented by secondary documentary evidence available mainly in online form. The outcomes of the paper indicate that hobbyist implantees are for the greater part, particularly ethically aware of the information and communication technology (ICT) implications as well as being technically competent individuals. Surprisingly the research found that do-it-yourself implantees are usually critical of commercial subscription implant applications and value highly the ideas of consent, choice, and the ability for consumers to opt-in or out of given applications.

Keywords
chip implants, culture, value, ethics, implantees, RFID, Amal Graafstra, case study

Disciplines
Physical Sciences and Mathematics

Publication Details
This conference paper was originally published as Ip, R, Michael, K, & Michael, MG, Amal Graafstra The Do-It-Yourselfer RFID Implantee: The culture, values and ethics of hobbyist implantees: a case study, Cultural Attitudes Towards Technology and Communication (CATAC08), Nimes, France, 24-27 June, 2008, pp. 1-15.

AMAL GRAAFSTRA- THE DO-IT-YOURSELFER RFID IMPLANTEE

The culture, values and ethics of hobbyist implantees: a case study

RODNEY IP, KATINA MICHAEL, M.G. MICHAEL

Abstract. This paper provides insights into the culture, values and ethics of do-it-yourself microchip implantees. Microchip implantees are people who have opted to bear a radio-frequency identification (RFID) device beneath their skin for particular electronic applications. This paper uses a single case study of the most prominent hobbyist microchip implantee, Mr Amal Graafstra of the United States, to explore the preliminary motivations for being implanted, the actual chip experience, and the subsequent repercussions of being an implantee. The data for this paper was collected using two main techniques, a primary interview with the case subject, complemented by secondary documentary evidence available mainly in online form. The outcomes of the paper indicate that hobbyist implantees are for the greater part, particularly ethically aware of the information and communication technology (ICT) implications as well as being technically competent individuals. Surprisingly the research found that do-it-yourself implantees are usually critical of commercial subscription implant applications and value highly the ideas of consent, choice, and the ability for consumers to opt-in or out of given applications.

1. Introduction

In 1998, academic and cybernetics researcher Professor Kevin Warwick of the University of Reading conducted the first official RFID implant trial which he called Cyborg 1.0. Using the RFID transponder implant in his left arm, Warwick was able to interact with the "intelligent" building that he worked in. With the implant he was able to do things automatically, like open doors which otherwise required smart card access, activate light upon entering an office space, and even have his computer greet him with a message and the number of emails awaiting response (Warwick, 2003). Around about the same time this 9-day experiment was taking place in the United Kingdom, Mr Amal Graafstra who was in his mid-twenties was considering the potential possibilities of implants. A self-confessed technology-savvy hobbyist, Graafstra was thinking about how he could interact more conveniently with household objects and space, including his vehicle. It did not take long before the hobbyist had one tag implant injected between the web of his thumb and forefinger, and then a second on the other hand. Graafstra was more concerned with the "cool" things he could with his implants like not requiring a physical key to enter his house or car, than the potential implications for mass market electronic applications. In 2006, Graafstra wrote about the applications he had created in

a popular book titled *RFID Toys*. The aim of this paper is to investigate what led to Graafstra's self-implantation, how he felt during and after the chip experience, and the subsequent repercussions that ensued.

2. Background

The 21st century has revealed a new "underground" movement (Bahney, 2006). Like graffiti artists, individuals are ignoring criticism from various conservative groups to implement and practice the new body art of RFID implanting. Contemporary body art has taken many forms, among these we can include tattooing, scarification and body piercing (Grognard, 1994). Today's new form of body art may be broadly termed chipification (Michael & Michael, 2006). The 'chipified' are an underground movement of people, who identify themselves by such names as "Cyber punks," "Do-it-yourselfers" (Graafstra, 2007, p. 16), "Hobbyists" (Foster & Jaeger, 2007, p. 23), "Midnight Engineers" (Bahney, 2006), "Taggers" (Graafstra, 2007, p. 19) and "RFIDs". The taggers have suffered criticism from diverse groups including, privacy activists, Christian sects and civil libertarians for implanting RFID chips into their bodies and developing functional systems for personal use. However, the taggers are not an organization, but instead are unrelated individuals around the world making use of RFID implants to accomplish tasks in their everyday life. No different to any other hobby group of the 21st Century, the taggers share their ideas and experiences via a publicly accessible Internet forum titled "Tagged". One such hobbyist that participates in this forum is Amal Graafstra, who recorded the very first correspondence on the forum with a fellow implantee going by the name of "Chris".

3. Previous Studies

In 2005, the term developed by the authors to describe recipients of RFID implants was "Electrophorus" (Michael & Michael, 2005). In Michael and Michael (2007, p. 318), an electrophorus is defined as:

> "a human bearer of electricity. The root *electro* comes from the Greek word meaning "amber," and *phorus* means to "wear, to put on, to get into". When an Electrophorus passes through an electromagnetic zone, he/she is detected and data can be passed from an implanted microchip (or in the future directly from the brain) to a computer device.

Studies conducted specifically on the cultural values and ethics of RFID implantees have been scarce, save for insights that have been recorded by implantees themselves. These latter pieces of evidence have taken a variety of forms including online web sites, newspaper articles, multimedia recordings (i.e. informal audio-visual interviews), and limited formal writings like books and journal articles. We can learn a great deal from writings such as Graafstra (2007), 'Hands on: How Radio-Frequency Identification got Personal' but these contributions are limited.

4. Conceptual Approach and Methodology

4.1 CASE STUDY

According to Yin (1984, p. 23) a case study "investigates a contemporary phenomenon within its real-life context". The case study in this paper is of a human subject. To date, numerous papers using a case study approach have been written focused on humancentric RFID applications as the main unit of analysis (e.g. Masters & Michael, 2007), but none on the recipients of implants and their personal motivations and experiences.

4.1.1. Who is Amal Graafstra?

Amal Graafstra is the owner of several technology and mobile communications companies located in Bellingham, Washington, and has a strong interest in photography as well as the latest interesting technology to hit the market. However, one thing sets him aside from typical 31-year-old males; he is the proud bearer of two RFID transponders implanted into his right and left hands. The transponders were implanted independently from any commercial or research organization and without any approval from the Food and Drug Administration of America, which regulates RFID implants for medical purposes (Lewan, 2007). "I wanted to be able to access my office door without getting my keys out of my pocket" (Solomon, 2007, p. 2). Graafstra states interest as the primary reason for getting microchip implants embedded into his hands (K. Michael, 2007): "[b]asically, it really depends, for me, if it's going to be any fun… and I don't necessarily do the legwork that I should to make sure I make a lot of money from it." Graafstra's motivation for why he did it is similar to many other "do-it-yourselfers" and therefore represents the aforementioned hobbyist case effectively.

4.2 INTERVIEW

A two hour interview was conducted between Katina Michael (2007) and Amal Graafstra on the 25th of May, 2007. The interview was semi-structured and contained 25 questions. The main themes addressed in the interview included:

- Amal's background including his upbringing, schooling, qualifications, current employment status, age and place of residence
- Amal's adoption of technology habits, value proposition for RFID implants, and prospects of commercialising intellectual property around humancentric chip implants
- Amal's motivations for going with an implantable technology as opposed to wearable or luggable device
- Amal's perceptions of himself, whether he is a hobbyist or entrepreneur and what words, terms or phrases he uses to refer to himself (i.e. the difference between a cyborg and an electrophorus)
- Amal's thoughts on implantation, who was to conduct the injection, any barriers or challenges that had to be overcome, and whether or not he had to ask permission to get the implant

- Amal's feelings on the actual implant process, how it made him feel, whether it was painful or painless and how he dealt with the aftermath of the implantation
- Amal's attitudes and perceptions towards the application of microchip implants in humans and ethical issues, discussed in terms of specific scenarios and stakeholders
- Amal's values on mandatory, voluntary, commercial and non-commercial and government-mandated humancentric applications pertaining to issues of consent, opting in/out etc.
- Amal's views on the location of implantation, the type of tag that should be used, the durability of the tag, and its potential functionality
- Amal's experiences with Christians or civil libertarians who oppose his use of RFID and his counter-arguments to such notions as the fulfilment of prophecy and the "mark of the beast"
- Amal's personal philosophical and spiritual perspectives and reflections
- Amal's knowledge on the prospect of RFID implant viruses spreading, relationship impacts (e.g. his spouse also has an implant), potential health risks and security breaches, and other general concerns.

4.3 DOCUMENTATION

Documentary evidence was obtained by conducting academic journal searches and targeted online searches using the subject's name. Of relevance specifically were direct comments made by Mr Amal Graafstra to journalists or friends and family, found in secondary sources.

4.4 DATA ANALYSIS

The paper is an exploration and therefore has been loosely coupled to address a number of themes as documented in the interview. The paper is characterized by thick description and original quotations deliberately to shed light on the culture, value, and ethics of RFID implantees.

5. Graafstra's Motivations Towards Self-Implantation

An interview with Graafstra reveals that he became interested in technology and the mechanics of how computers worked at an early age. His technology savvy personality combined with the observations he made from RFID tags implanted in pets were the stimuli that inspired Graafstra to introduce RFID tag implants into his own life. He told Shaw (2006):

> "I'm a project, gadget-builder kind of guy and I saw cats and dogs getting these tags and I spent a few years thinking about the different ways they could be used."

In 2005, Graafstra was working for a medical facility in Seattle where he had to carry around almost 100 different keys (Graafstra, 2007, p. 16):

> "That bulky key ring got me thinking. It struck me that modern keys are just crude identification devices, little changed in centuries… Now, if the tag is implanted in your body so much the better: it's impossible not to have it when you need it."

Graafstra was hoping to move beyond traditional keys by eliminating the consequences of depending on a remote key: "If I'm in the alley naked, I want to still be able to get in [my house]" (Reuters, 2006). By receiving a chip implant, tasks in his everyday life are made more convenient while providing the novelty of not having to use external keys.

Although Graafstra's initial motivation to get a chip implant was for the convenience that eliminating keys can provide, he has expressed in the interview (K. Michael, 2007) that he would not have implemented the RFID system into his life if it didn't provide a recreational experience for him:

> "Basically it really depends, for me, if it's going to be any fun. There are a lot of things that could be put together but it takes a lot of work and it's not all really fun in the end."

Graafstra's recreational pursuit in this particular case demonstrates the recreational nature that exists within most hobbyist implantees.

6. Social Networking

Part of Graafstra's recreational pursuit comes from sharing with others his own methods of implementing RFID implant systems. It is of a hobbyist's nature to share with others their experiences and methods within their common interest as it creates a sense of social recreation (Cohen, 2004, p. 271). This type of activity can be found from weekly meetings or lessons, forums, conversations or through writing books. In 2005, when Graafstra implanted his first RFID transponder into his left hand, he posted pictures of the implant process on a photo sharing website. The initial aim of this was to share the photos with his friends. However, due to the nature of the Internet, it was not long until he grabbed the attention of industry players, book publishers and news reporters (Graafstra, 2007, p. 18).

Graafstra authored *RFID Toys* to share his experiences with others. The book describes how to go about getting an RFID implant, and how to build a functional system that can be integrated with a home or business network. For example, Graafstra documents, how humancentric RFID can be used to unlock doors both at home and in the car and also for logging into the computer using RFID implants (Heim, 2006). *RFID Toys* invites those that are interested to become hobbyist implantees themselves and provides the knowledge to do it. Due to the significant exposure of Graafstra's book, the possible number of "do-it-yourselfer" implantees can be speculated to be large. There is no official account of the number of implantees available but Graafstra estimates that "[the] community is probably around 200 to 1000 people, but it's really hard to track." However, Graafstra does mention, "at least 20 of [his] tech-savvy pals have RFID implants" (Reuters, 2006). One of the few possible ways of estimating the number of "hobbyist" implantees is by looking at the number of users of an Internet discussion forum that was created for chip implantees by Chris Rigby, another RFID implantee

(Graafstra, 2005). The forum http://tagged.kaos.gen.nz exists as a communication medium for hobbyist RFID implanters and implantees to discuss their "tagging" experiences and new methods that they have discovered. Graafstra was one of the first of two participants of this discussion forum and he says that after this, "it exploded".

7. The Chip Experience

In March 2005, Graafstra asked his close friend, a surgeon, to implant a RFID transponder into his left hand (Bahney, 2006). Graafstra himself emphasizes that the soreness from the implantation was gone within a few hours; and with the bandage still wrapped around his hand from the incision, he was writing software to make use of his new implant soon after the injection (Graafstra, 2007, p. 18). Graafstra's first implant was inserted through an incision into the webbing between his index finger and his thumb on his left hand (Graafstra, 2007, p. 16). He used an EM4102 tag that he purchased from Phidgets USA, now known as Trossen Robotics. These tags were un-sterilized and not intended for implantation into the human body, so Graafstra had to organize the sterilization of the chip on his own (Graafstra, 2007, p. 16). His second implant used a different RFID transponder known as the Philips HITAG 2048S. This tag contains encryption for security purposes and also 255 bytes of read/write memory storage space, allowing a wider range of possible applications with more security (Graafstra, 2005). The technique of the second implantation was synonymous to how pets are implanted. Using an AVID injector kit it was implanted straight into the hand without making a surgical incision (Graafstra, 2005).

One may cringe at the thought of putting a foreign object under human skin; however Graafstra says that the whole operation "wasn't a big deal" (Shaw, 2006). In recounting the experience in the interview he recollects:

> "[i]n both instances it was a very simple procedure to do and there was very little bruising- actually there was no bruising on either hand and very little bleeding."

He also mentions that there was no pain involved in the implantation process (Ginsberg, 2005). These comments are in contrast with some messages posted to the *Tagged Forum* by other implantees however, one must consider that different people have different pain thresholds in addition to the technique applied to perform the implantation. For instance, unlicensed body piercing shops have been known to cause major infections to their clients to the point of bodily harm to the ear, lips, eyes, cheeks, and tongue (BBC, 1999). Prospective implantees should do their homework on the appropriate mechanisms to get implanted before going in blindly.

In an interview with Ginsberg (2005), Graafstra described the implant under his skin as an "odd feeling" and how it has made him realize:

> "how utilitarian our bodies actually are and how separate everything is — how separate the skin layer really is from the muscle layer under it. It really is just a rubbery protective coating. Complex and amazing, but far less mysterious to me now."

Graafstra's implant experiences have gone smoothly without any complications. Graafstra did not just rely on trial and error to conclude that putting a RFID tag into his hand would not be detrimental to his health. He and his wife, Jennifer Tomblin, conducted experiments of the tags to ensure Graafstra's health would not be put in jeopardy. In one of their experiments, the EM4102 tag was hit with a hammer at various strengths until it broke. They concluded that: "[w]hile it was possible to shatter the tag, the blunt force required to do so would also mutilate my hand. In that scenario, a little broken glass would be the least of my worries" (Graafstra, 2007, p. 18).

The everyday activities of Graafstra's life are not negatively affected due to having two RFID transponders in his hands. In 2005, when he was first implanted, Ginsberg (2005) asked if he noticed the implant at all: "Not at all, really, aside from a slight sensitivity around the implant site… I'm sure the sensitivity will pass and it will be completely unobtrusive." Two years later, in 2007 (K. Michael), when asked how the implants feel, Graafstra replied, "Now, of course, I don't feel any different. I even forget they are there until I have to use them." The novelty of poking and feeling the tags in his hand wore off, not long after the first couple of months post implantation.

8. Alternatives

While researching alternative forms of identification systems, Graafstra considered biometric identification, Applied Digital Solution's *Verichip* product, and the traditional RFID transponders designed for pets. However, all of these products and approaches had what he considered long-term drawbacks.

Biometrics uses human physiological and/or behavioral characteristics as a form of identification (Jain et al, 2000, p. 92). Graafstra (2007) found that biometrics was too expensive for the use of hobbyists. He also found that this type of identification was unreliable, clunky and difficult to program and therefore was not suitable for the locks in his home and car. It is interesting to note that Graafstra generally feels that biometric techniques instituted for government applications are more intrusive than his own beneath-the-skin RFID implants that he uses for personal applications. During the primary interview, Graafstra recounts how he and his wife once visited Disney Land and how after paying at the gate, he was asked for his hand biometric, and how uncomfortable this made him feel. For Graafstra biometrics are highly personal, like one's DNA, and they should not be stored by commercial organizations, or even by government agencies. At least with self-imposed RFID implants, he says, they are under your control and no one else has access to them. He highlights that this is one of the benefits of implants, i.e. that they cannot be stolen or forgotten or misplaced (K. Michael, 2007).

Verichip's products require doctors to register implantees in a special database, which conflicted with Graafstra's ethical values and therefore he did not choose this method of implantation (Graafstra, 2007, p. 16). The Verichip products, in Graafstra's (2007) opinion, were too expensive for the use of hobbyists and too closed in terms of the

potential to develop corresponding personalized software. In addition, the Verichip tags are regulated by the Food and Drug Administration of America and have to be implanted deep in the upper arm (Graafstra, 2007, p. 16). In Graafstra's opinion, this was "awkward to use with door access… it's a lot easier to unlock your car by waving your hand rather than wiggling your bicep." Graafstra has a point here- an implant in a bicep is not at all practical for opening one's own front door when the knob is down lower. Being a commercial product, another downside to this chip was that it was not hackable, meaning it could not be customized for personal use. Graafstra sees implants for one main use, in this instance ehealth, as defeating the purpose of creating a comfortable personalized interactive space. For hobbyist use, Graafstra states that the tags needed to be cheap, harmless, removable and customizable: "I was more interested in just getting something simple, cheap, and fun to play with" (Ginsberg, 2005).

An attribute that Verichip tags and pet tags have alike is that they both have anti-removal coating. This coating attaches to the skin and makes it hard to remove the chip without a lot of pain and also presents other health risks (Foster and Jaeger, 2007, p. 22). Graafstra is vocal about the importance of humancentric implants not possessing anti-removal coating. He does not like the idea of permanency, despite the fact that he has chosen glass tags that are highly durable and should last a lifetime of reads. Anti-removal coating means that implantees do not possess the ability to choose to remove an implant if they no longer want it. Of the VeriChip scenario, he says, what happens if a subscriber no longer wants the implant after 3 or 6 or 12 months of receiving it, how can they get it removed when it pretty much has fused with the body, without causing some health problem in their upper arm? With regards to chip implants in pets, the American Veterinary Medical Association (AVMA, 2007) recently warned that: "removal of the chip is a more invasive procedure and not without potential complications."

9. Ethics and Security

As well as considering the price and customizability of the RFID implant, Graafstra is noticeably aware of the security and ethical issues associated with having the tag. Because of this, he has opted for, in his view, the best type of transponders that do not jeopardize his ethical views or personal security. One of the major downsides that Graafstra noticed associated with biometric technology is that once a user participates in a biometric system it becomes very hard to opt out of it. He told Ginsberg (2005):

> "Given the choice of Orwellian societies, I'd rather live in one based on RFID tags than fingerprints, DNA, or facial structure; an RFID tag system is easy opt out of, whereas DNA sampling or facial recognition, well, isn't."

Graafstra highlights the importance in being able to opt out of an identification system; for this he chose the EM4102 pet tag over any other tag as it lacks the anti-removal coating (Graafstra, 2006, p. 19; K. Michael, 2007; Ginsberg, 2005):

> "[T]he important thing for me is that if the technology became oppressive whether the government was using it to oppress people and or require it to buy stuff, I would remove them, I would be the first to opt out."

When the question arose of what Graafstra thought about implantable RFID transponder technology, his reply was (K. Michael, 2007):

> "[m]y concern is not about the actual technology, I love the technology. I think that it is great; I hope it's developed and used for good. My concerns are the people. A bomb is no worse than a flower, if no one presses the button."

Graafstra does not ignore the possibility of implantable RFID transponder technology being used for adverse applications in which he is often accused as being the endorser of such practices. Graafstra believes that it is not the "hobbyist" user of this technology that will lead to adverse applications, but more so the "system" that controls the data and manages the transponders that could abuse their power, shown when he states (K. Michael, 2007):

> "[y]ou might be an excellent driver but you still have to trust that the other person isn't going to come over the line and kill you. The same is true with this type of scenario where you're getting an implant to opt into the system. You have to basically trust the system, that power will not be abused."

On the contrary, Graafstra believes that it is the hobbyists that are preventing unethical applications from taking place. Hobbyists understand the technology intricately, they know how to make it work, how to break it, how to remove it, where it should and should not be applied. In a sense, they live and breathe the technology so know its benefits and pitfalls better than anyone else. Even as far back as 2001, Millanvoye (2001) reported that one punk known by the name of "Z.L", who was an avid reader of MIT specialist publications like *open|DOOR MIT* magazine on *bioengineering and beyond* (Millanvoye, 2001) anticipated a revolution where technology would be integrated within the body and had already taught himself how to do surgical implants and other operations. The punk told Millanvoye:

> "The state uses technology to strengthen its control over us… By opposing this control, I remain a punk. When the first electronic tags are implanted in the bodies of criminals, maybe in the next five years, I'll know how to remove them, deactivate them and spread viruses to roll over Big Brother."

Graafstra believes that if more and more people learn about the technology it will allow society to gain more control over it. He told Heim (2006):

> "Basically people are learning about the technology, which could never be a bad thing… If it ever became oppressive, it's the people learning about it now who would be equipped to fight it."

He encourages self-experimentation in the hope to expose society to the myths that surround the use of the technology.

The security of RFID technology is always being jeopardized due to the increasing popularity of this technology and the increasing benefits of hacking such a system (Graafstra, 2007). However, to combat these threats, Graafstra's second implant was implanted to guarantee a more secure system. In an interview with Ginsberg (2006) he reveals that his system is more difficult to intrude as people think:

> "[W]ith the read range being only an inch, stealing my RFID tag ID would be a rather personal encounter. Getting that tag ID duplicated would be another difficult task for your average carjacker — it would honestly be easier to just smash my window."

With his current RFID system, Graafstra is noted saying that reading his chip can be compared to randomly finding his house key on the ground and that "[t]he information can't be used in a way that would compromise my money or my medical data or anything like that" (Heim, 2006).

The act of implanting RFID transponders under the skin has been criticized by religious groups as being "The Mark of the Beast" referred to in the Book of Revelation in the *New Testament*. Such critics of implantees believe that the RFID implant version of the "Mark of the Beast" (i.e. as opposed to bar codes or biometrics) may become a requirement to lead a normal life and conduct business in the future (Graafstra, 2007, p. 18). Graafstra (2007), raised as a Christian, dispels these claims, arguing that numeric identifiers like social security numbers have "borne a similar stigma," yet everyone has adopted these into their lives. Graafstra defends what he is doing and explains that the criticism is being directed at the wrong people (K. Michael, 2007):

> "I think it's just the option of me using it for my own purposes and not having to deal with those things [that] kind of brings to life a point that the bible is making, it's not the specific mark, whatever that might turn out to be; it's the act of being involved in that system and worshipping it."

10. Discussion

RFID "do-it-yourselfers" in the United States may be opting-out of adopting commercial RFID implants, such as those sold by the VeriChip Corporation, but they are not exempt from federal and state anti-chipping laws. To some degree RFID "do-it-yourselfers" should also ensure that they are abiding by the general Food and Drug Administration (FDA) regulatory guidelines for humancentric applications, for their own sakes. This 'underground' movement has the propensity to encourage new unskilled entrants into the market who are not well-versed in the act of chipification, increasing the likelihood of infection and serious illness in persons who have not researched the implant procedure properly. The very same thing has occurred with tattooists who have taken on the art of body piercing with little, if any, training. As a result, widespread health risks amongst the "tagged" does remain a real possibility if we are to believe researchers like Covacio (2003), despite the rejection of these concerns by many implant recipients. Most hobbyists who have spoken publicly about their implant have stated that in the beginning they can feel the tag as a "lump" or "bump" beneath their skin, but that before too long they forget it is even there and cannot feel or sense it.

At a minimum, health-wise, the implantee is at risk of infection, especially if the device being implanted is not sterile. There is also the problem of tag or transponder removal. Unlike body piercing where jewelry can be removed relatively easily depending on the piercing location, tags or transponders with anti-migration coating cannot be removed

with ease if they have been in the body for more than just a couple of weeks. The implant becomes enmeshed by tissue in the subcutaneous layer of the skin. An implantee would incur significant bodily harm if they attempted to remove their own anti-migration coated tag after this duration without the assistance of a doctor. You are literally at this point "carving out" the implant. While implantees consider passive tags and transponders to be relatively harmless, it is predicted that active tags which have numerous technical advantages will be used before too long to push application development even further, especially to achieve longer read/write distances. The potential for batteries to leak in the human body then becomes an issue with unknown consequences, including the possible birth of new forms of cancer (Lewan, 2007) or transmission of person-to-person viruses. It should also be noted, that for hobbyists there is no insurance claim that can be made if things go wrong. The question of how many individual implants, hobbyists will subject their body to is also a matter for discussion. While Graafstra has two implants (i.e. one in each hand), there is nothing to stop others from housing up to *n* implants.

There is also the scenario where implantees may wish to "transfer" or "exchange" their implants to be privy to new interactive spaces or to share in personalized settings. This can happen in two ways depending on the context: (i) by adding a new user to the software developed by the hobbyist; or (ii) by physically exchanging implants. In the latter way, it should be noted, that implants injected into the webbing between the thumb and index finger are much easier to exchange than those injected in the wrist, forearm or shoulder. As an example, consider a minor who wishes to gain illegal entry to a VIP club lounge that relies solely on RFID implants, so he temporarily "exchanges" implants with an older member. And what of, the case where a perpetrator may try to steal an implant to gain uninterrupted physical access to an implantees home or belongings or credit? The consequences of "forced entry" then become dangerous, as persons with implants become a magnet for theft and attention. It is no longer about handing over a "key" to the trespasser so that they can get into the car or the apartment but about 'lending your arm' and implant to get in (Masters and Michael, 2007).

And what of the potential for implant IDs to be "reapplied" to contexts outside the implantees control or knowledge? Implants may be rigged to allow the third party implanter control over the implantee; a type of hi-jacking of an identity for maybe a couple of hours, a couple of days or indefinitely. Typically we are talking about "duping" a system or someone engaging in the act of forgery. Persons who are without much technical know-how, as in the case of 'white-hats' that receive implants because of the 'cool' factor, may well find themselves oblivious to dubious goings-on. They may even be acting to assist in a miscarriage of justice without realizing. The educational level, background and technical expertise of 'hobbyists', therefore, plays a part in how implants are applied. Anything is possible, motivations in people for implant usage differs, even within the hobbyist community. RFID implants are not immune to counterfeiting and by their very nature are less secure than biometrics or smart cards. The fact that implants are contained beneath the skin, also imparts a false sense of security to the unsuspecting user.

With regards to federal and state laws, the question arises whether people who have implants have indeed voluntarily requested them (Michael & Michael, 2007). In commercial implants, the question arises whether Alzheimer's sufferers who have adopted certain RFID transponder technology have indeed "requested" implants voluntarily or have in some way been coerced into adopting them for their own safety by carers. For example, Wisconsin Act 482 which was enacted on 30 May 2006 and is titled: "Prohibiting the required implanting of microchip in an individual and providing a penalty" reads:

> "(1) No person may require an individual to undergo the implanting of a microchip. (2) Any person who violates sub. (1) may be required to forfeit not more than $10,000. Each day of continued violation constitutes a separate offense" (SECTION 1. 146.25).

In underground implants there is really no way of ensuring whether a chip was voluntarily adopted or was enforced. Consider a tech-savvy parent who requests their son or daughter be implanted in order to gain access into the front door of their home, as they wish to do away with manual techniques such as keylocks (Michael, Fusco & Michael, 2008). Further contemplate the potential for time stamps to be instituted upon entry/exit and we have a person surveillance system for the home- a type of *gatekeeper*- which can chronicle the basic movements of family members and provide auditing capabilities. The point here is that hobbyist implantees are not exempt from the law because they have adopted the technology using their own ingenuity and not that of a commercial entity.

RFID implant hobbyists often state their association with interactive systems as being "just for fun", otherwise they would not be involved. While fun it may be to those inclined to "cutting code" or spending hours and hours constructing home automation features, there is the question of "value". How much additional benefit does implant technology actually provide the hobbyist beyond the satisfaction of having things happen 'automatically'? And what of the value of RFID implant application development to the broader community? Being able to program your mobile phone to remotely raise and draw curtains or to have a computer say your name after it detects your implant when you enter your office, does not seem like such an incredible gain or timesaver. It may be slightly more convenient and kind of "cute" to have things happen 'automatically' and remotely but one is left to ponder, how much more convenient? All technology is prone to failure, RFID is not any different. When a power outage occurs in the home, for whatever reason, backup generators can kick in (for a limited time) before the owners need to resort to the manual 'lock and key'. And what happens when systems malfunction?

If we assume for a moment, that RFID implant hobbyists are harmless because they are simply experimenting on themselves, one needs to think about the impetus that these 'harmless' experiments provide the broader inventor community. While hobbyists are not necessarily interested in making money from the applications they develop or going through the complex patenting process, they do plant the first seeds of a future vision for the technology and how it might be used. Having said that, hobbyists tend to have an intimate understanding of the technology and its consequences- they are in no way

prejudging ethics, they are living with the technology and can state categorically what the benefits, costs and limitations are to them as individuals. What they cannot do is speak on behalf of a populace to identify all the consequences and social implications that might present themselves in a variety of contexts.

Graafstra and others like him, consider themselves to be well-rounded individuals. They do not shy away from broader discussions on matters pertaining to implants and philosophy, religion, national security or even human rights. It shows that they have spent time contemplating and deliberating issues to do with legislation, civil liberties, and even the apocalyptic, outside the realm of purely technical matters. It also demonstrates that apocalyptic language and/or eschatological paradigms can now be legitimately used and applied in relevant information and communication technology (ICT) discussions without the normal accusations of fundamentalist or chiliastic readings of *end-time* literature. Implants seem to be the first step in the so-called *quest for immortality* through technology, if we are to believe Peter Cochrane (1999) who wrote of the Soul Catcher chip. In the near-term however, it will be "pharmacy-on-a-chip" implants that will be used for drug delivery purposes (The Lab, 1999), but that will likely pave the way for a black market cybernarcotics trade.

11. Conclusion

Some RFID implant hobbyists like Graafstra, are acutely aware of the backdrop to which they are inventing. It is here that we can make the observation that the hobbyist is an inventor-user who is not concerned about financial remuneration through royalties but is more concerned with getting things to work from an enthusiast's perspective. This is in direct contrast with the inventor-employee or inventor-researcher implantee who has very different motivations for experimenting with RFID implants. Because humancentric RFID has a market the size of the world's population, the forecasted business for the device and its related systems and applications is significant (Marburger et al., 2005). Electronic passports currently being distributed to citizens world-wide, may just be the first large-scale "trial" of an RFID technology that will herald in a business case for ID-passports to be implanted in people in the future. Such "apocalyptic" metaphors bombard us daily from the advertising world showcasing ICT and the subliminal "cutting edge" intent of these advertisers cannot go unnoted. More importantly, potential scenarios (including a nuclear holocaust) described in the world of revelatory writings are no longer outside the realm of possibility given our technological advancement. This is something which of course, discerning 1960s cinema-goers of Stanley Kubrick's black comedy, *Dr. Strangelove: How I Learned to Stop Worrying and Love the Bomb* (1964), were keenly aware of. What part implants will play in the future is yet to be fully grasped given the patchy diffusion of the technology both commercial and non-commercial since its official inception in 2003. However what is certain is that the application of RFID implants for humancentric applications can be used to do both good and bad, i.e. to save lives and to help people but also to segregate, enslave and control, depending on the context.

Acknowledgements

The authors would like to thank Mr Amal Graafstra for accepting to conduct an interview with Katina Michael. This research on the social and ethical implications of location-based services was funded by the IP Location-Based Services Research Program in the Faculty of Informatics at the University of Wollongong, NSW, Australia.

References

AVMA. (13 September 2007). Breaking News: Statement on Microchipping. *American Veterinary Medical Association* Retrieved 5 October, 2007, from http://www.avma.org/aa/microchip/breaking_news_070913_pf.asp

Bahney, A. (2006, February). High Tech, Under the Skin. *New York Times,* p. G.1.

BBC. (1999). Tongue piercing 'can be fatal'. *BBC News* Retrieved 11 January, 2008, from http://news.bbc.co.uk/1/hi/health/399218.stm

Bernus, J. S., & Chase, M. A. (1990). Decision making in a networked environment. In H. Eschenauer, J. Koski & A. Osyczka (Eds.), *Technology and Communication* (pp. 376-396). Berlin: Springer-Verlag.

Cohen, S. M. (2004). Online Social Networking Tools. *Public Libraries, 43*(5), 271.

Cochrane, P. (1999). *Tips For Time Travelers: visionary insights into new technology, life, and the future on the edge of technology.* New York: McGraw-Hill.

Covacio, S. (2003). Technological Problems Associated with the Subcutaneous Microchips for Human Identification (SMHId). *InSITE-Where Parallels Intersect*, June, 843-853.

Forum. (2007). Tagged. Retrieved 7 August, 2007, from http://tagged.kaos.gen.nz

Foster, K. R., & Jaeger, J. (2007). RFID Inside: The murky ethics of implanted chips. *IEEE Spectrum, March*, p. 23.

Ginsberg, J. (2005). One small step for hand. *Body Modification Ezine* Retrieved 7 August, 2007 from http://www.bmezine.com/news/presenttense/20050330.html

Graafstra, A. (2005). Graafstra's RFID Implant page. Retrieved 24 April, 2007, from http://amal.net/rfid.html

Graafstra, A. (2006). *RFID Toys: 11 Cool Projects for Home, Office, and Entertainment*. New York: John Wiley & Sons.

Graafstra, A. (2007). Hands on: How Radio-Frequency Identification got personal. *IEEE Spectrum, March*, 14-19.

Grognard, C. (1994). *The Tattoo: graffiti for the soul*. Spain: The Promotional Reprint Company.

Heim, K. (2006). Man grips future with microchip implants in hands. *Seattle Times* Retrieved 7 August, 2007, from http://seattletimes.nwsource.com/html/localnews/2002835871_chipimplant01.html

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification *Communications of the ACM, 43*(2).

Lewan, T. (2007). Chip Implants Linked to Animal Tumours. *The Associated Press* Retrieved 24 October, 2007, from http://www.washingtonpost.com/wp-dyn/content/article/2007/09/08/AR2007090800997_pf.html

Marburger, A., Coon, J., Fleck, K., & Kremer, T. (2005). *Implantable RFID for the Health Industry.*

Masters, A., & Michael, K. (2007). Lend me your arms: The use and implications of humancentric RFID. *Electronic Commerce: Research and Applications, 6*(1), 29-39.

Michael, K. (25 March 2007). Interview with Mr Amal Graafstra.

Michael, M. G., Fusco, S. J., & Michael, K. (2008). A research note on ethics in the emerging age of überveillance [Electronic Version]. *Computer Communications*. Retrieved 6 March 2008 from http://dx.doi.org/10.1016/j.comcom.2008.01.023

Michael, K., & Michael, M. G. (2005). Microchipping people: the rise of the electrophorus. *Quadrant, 49*(3), 22-33.

Michael, K., & Michael, M. G. (2006). Towards Chipification: The Multifunctional Body Art of the Net Generation. In F. Sudweeks & C. Ess (Eds.), *International Conference on Cultural Attitudes towards Technology and Communication* (pp. 622-641). Tartu, Estonia: Murdoch University.

Michael, M. G., & Michael, K. (2007). A Note on Überveillance. In K. Michael & M. G. Michael (Eds.), *From Dataveillance to Überveillance and the Realpolitik of the Transparent Society: The Second Workshop on Social Implications of National Security* (pp. 9-26). Wollongong.

Millanvoye, M. (2001). Teflon under my skin. *UNESCO* Retrieved 29 November, 2001, from http://www.unesco.org/courier/2001_07/uk/doss41.htm

Minsk, M. L. (1990). Process models for cultural integration. *Journal of Culture, 11*(4), 49-58.

Reuters. (2006). Computer chips get under skin of US enthusiasts. *ABC news online* Retrieved 28 August, 2007, from http://www.abc.net.au/news/newsitems/200601/s1542754.htm

Shaw, G. (2006). Implants turn humans into cyborgs: Radio frequency identification chips replace house keys. *Canada.com* Retrieved 7 August, 2007, from http://3.canada.com/components/print.aspx?id=d4f47afb-6ee3-460d-b4e3-834770fa886b&k=85038

Smythe, J. S. (Ed.). (1990). *Applications of Artificial Intelligence to Communication*. Berlin: CMP and Springer-Verlag.

Solomon, S. (2007). When patients take surgery into their own hands: Extreme body modification divides physicians along ethical lines. *National Review of Medicine, 4*(9).

The Lab. (1999, 28 January). Microchip implants for drug delivery. *ABC: News in Science*, from http://www.abc.net.au/science/news/stories/s18502.htm

Warwick, K. (2003). Professor Kevin Warwick– Home. *University of Reading* Retrieved 20 September, 2003, from http://www.rdg.ac.uk/KevinWarwick/html/project_cyborg_1_0.html

Yin, R. K. (1984). *Case Study Research: design and methods*. Sage: London.