Social-Technical Issues Facing the Humancentric RFID Implantee Sub-culture through the Eyes of Amal Graafstra

Amal Graafstra,[1] Katina Michael,[2] M.G. Michael[2]
[1]*Amal.net,* [2]*School of Information Systems and Technology, University of Wollongong*
amal@amal.net, {katina, mgm}@uow.edu.au

Abstract

Radio-frequency identification (RFID) tags and transponders have traditionally been used to identify domesticated animals so that they can be reunited with their owners in the event that they stray. In the late 1990s, industry started to investigate the benefits of using RFID to identifying non-living things throughout the supply chain toward new efficiencies in business operations. Not long after, people began to consider the possibilities of getting RFID tag or transponder implants for themselves. Mr Amal Graafstra of the United States is one of the first, and probably most well-known 'do it yourselfer' (DIY) implantees, who enjoys building customized projects which enable him to interact with his private social living space. Since 2005, hundreds of people have embarked on a mission to interact with their mobile phones, their cars, and their house via a chip implant, providing personalized settings for their own ultimate convenience. This paper presents some of the socio-technical issues facing the RFID implantee sub-culture, namely health and safety, privacy, security, regulation, and societal perceptions. The paper concludes with a list of recommendations related to implantables for hobbyists.

1. Introduction

While some cultures embrace the practice of decorating the human body with tattoos and brands, others still perform the age-old art of scarification [1]. Of greater currency today however is the act of body piercing using a plethora of metallic materials, including titanium. Some have even opted to modify the body in outward appearance by using large subdermal or transdermal implants on their heads and forearms [2]. But beyond the purely cosmetic body modifications that some subcultures engage in [3], there are now techno-hobbyists who are transforming the manner in which they interact with their personal social living space through the use of functional high-tech devices known as radio-frequency identification (RFID) tags and transponders.

On the 22nd of March 2005, Mr Amal Graafstra was implanted with his first radio-frequency identification tag [4]. Anecdotal evidence from other do-it-yourselfer implantees agree that Graafstra has been a pioneer in this field, doing things "first" and also "better" than most other implantees meddling in the high-tech art. In the beginning of 2006 Graafstra even published a book about the applications he had built [5]. Other high profile implantees [6], some of whom preceded Graafstra, include: Kevin Warwick (University of Reading academic) [7], Scott Silverman (CEO of VeriChip Corporation) [8], Rafael Macedo de la Concha (Mexico's Attorney General) [9], Dr. John Halamka (Harvard Medical School's CIO) [10], Gary Retherford (employee at CityWatcher.com) [11], Mikey Sklar (a UNIX engineer) [12], Jonathan Oxer (a LINUX guru) [13], and Meghan Trainor (doctoral student and artist) [14]. This paper however is not concerned with professional "research-oriented" RFID implantees, such as Kevin Warwick, nor with consumers/ customers who have been implanted with commercially available VeriChip technology, nor with individuals who have used RFID for their artistic performances, such as Eduardo Kac [15]. Rather, this paper is concerned with understanding do it yourselfer (DIY) implantees who are usually technically-savvy citizens and are predominantly interested in novel convenience-oriented solutions. This paper focuses on the challenging socio-technical issues and questions that DIY implantees are faced with, related to health and safety, privacy, security, regulation and societal perceptions.

2. Literature Review

A number of academic articles and book chapters have been published on the life and works of Amal Graafstra, including his own full-length book titled *RFID Toys* [5]. Graafstra featured in his own *IEEE Spectrum* article in 2007 [16] and several other academic works about him have been written between 2008 and 2009 [17], [18]. He has also figured in hundreds of popular stories in all forms of media- print, radio and television that have received worldwide coverage, e.g. [19], [20], [21], [22]. Most recently *Fox News* wrote about him [23] and the *Discovery Channel* interviewed him. While anyone in Graafstra's position would have probably commercialized their ideas by now, Graafstra remains content in pursuing things that are 'fun' rather than things which 'make money,' although he admittedly does have an entrepreneurial streak about him. Despite the attention, Graafstra remains level-headed, and it is clear upon

speaking with him, that he is more about innovation than he is about becoming famous.

3. Methodology

This paper takes on a non-traditional ICT methodological form in that it is written in two voices; Part A is written in the first person voice of Amal Graafstra where he describes events as a participant and Part B is written in the third person voice where Michael and Michael are relating events about Graafstra, and Graafstra is relating events about others. In 2007, Michael and Michael embarked on a full-length interview with Graafstra [24]. Some two years after the interview was conducted, the interviewers requested that Graafstra reflect on his own ideas and commentary as stated in the original interview transcript [25], and make amendments as he saw fit. *Time* is a very important element when one considers new radical technologies and applications, especially those that seem to evoke a great deal of interdisciplinary debate. Take the launch of the ENIAC in 1948 for instance, and the misconceptions that ensued [26], although few could have possibly predicted that such awesome machinery would find its way into humans.

In Part A, Graafstra's story is depicted "uncut", and Michael and Michael do not interrupt the flow or stream of ideas but can be credited with evoking responses to questions that Graafstra is seldom asked. The usual media hype disappointingly focuses on whether Graafstra is the 'devil' and falls short of those all important philosophical questions about the future trajectory of technology. K. Michael has a background in information and communication technology (ICT) and law, while M.G. Michael has qualifications in philosophy, history and theology and has written on topics related to bioethics and the misuse of new technologies by society. The rich combination of backgrounds and experiences has brought about an interdisciplinary discussion between the three authors in Part B. It does not mean that the authors agree on all points, but new research should not necessarily bring about agreement, but debate toward further discussion. In some sense, this is what the *IEEE ISTAS10 Conference* is about, respecting diverse opinions and looking at new technologies in an interdisciplinary manner that may help to shed light on future developments and how society is to absorb them.

3.1. Case Study: Amal Graafstra

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, Mr Amal Graafstra. Graafstra can be considered a participant-researcher in this study while Michael and Michael act as independent observers of the subject within his real-life context.

3.1.1. Background. Amal Graafstra is the Director of Information Technology for OutBack Power Systems. He is the owner of several technology and mobile communications companies. Amal loves thinking up interesting ways to combine and apply various technologies in his daily life. A self-starter, Amal dropped out of community college and started his first company at the age of seventeen. The company was called The Guild, and it provided dial-up Internet access to customers, while small set-ups were still feasible.

Some years later, Amal started his second company Morpheus, which specialized in web hosting and web development. For some time the company did well, but as cheaper hosting services became available, it became more and more difficult to compete in the market. Amal then decided to rebuild Morpheus by supplying managed computing services to the medical industry. In parallel, Amal did some work for WireCutter, a wireless mobile messaging company that were involved in creating mobile marketing campaigns for various radio stations, sending SMS text messages to mobile phones. Graafstra decided to pour his heart and soul into the company he called txtGroups but this too was unable to make ends meet, and soon Twitter rapidly overtook txtGroups as a social text platform. His most recent employment is as the head of an information technology (IT) department where he enjoys creating novel and innovative solutions that enable the business to grow.

3.2. Interview

The interview conducted in 2007 between Graafstra (the subject) and K. Michael (the interviewer) was semi-structured and contained 25 questions. The main themes addressed included:

- Background (upbringing, schooling, qualifications, employment, age and place of residence)
- Adoption of technology habits, value proposition for RFID implants, and prospects of commercialising intellectual property around humancentric chip implants
- Motivations for going with an implantable technology as opposed to wearable or luggable device
- Self-perceptions, whether he is a hobbyist or entrepreneur and what words, terms or phrases he uses to refer to himself (i.e. cyborg versus electrophorus)
- Thoughts on implantation, who was to conduct the procedure, any barriers or challenges to overcome, and whether or not he had to ask permission to get the implant
- 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
- Attitudes and perceptions towards the application of microchip implants in humans and ethical issues, discussed in terms of specific scenarios and stakeholders

• Values on mandatory, voluntary, commercial and non-commercial and government-mandated humancentric applications pertaining to issues of consent, opting in/out
• Views on the location of implantation, the type of tag that should be used, the durability of the tag, and its potential functionality
• Experiences with Christians or civil libertarians who oppose his use of RFID and his counter-arguments to such notions as the fulfillment of prophecy/ "mark of the beast"
• Personal philosophical and spiritual perspectives
• Knowledge on the prospect of RFID implant viruses spreading, relationship impacts, potential health risks and security breaches, and other general concerns.

3.3. Ethnography and Participant Observation

Graafstra was asked by Michael and Michael to write a reflection on the original transcript, in actual fact to take on the role of a participant observer. This reflection was integrated into the original transcript, forming Part A of this paper. The reflection remains 'untouched' save for changes in formatting and expression. These are the raw thoughts of Amal Graafstra, captured in an ethnographic style [27]: "[i]t is a distinctive feature of social research that the 'objects' studied are in fact 'subjects'… unlike physical objects or animals, they produce accounts of themselves and their worlds." Michael and Michael have added relevant bibliographic sources to Part A, and in Part B the content from the original interview conducted with Graafstra is qualitatively analyzed to draw out anthropological and sociological orientations. It is here where the third person voice is used by the authors but where also, events related to Graafstra himself, are cited through direct quotation.

PART A- PARTICIPANT OBSERVATION

In Part A, Amal Graafstra tells his DIY tagger story as a participant observer. He is both the object and subject of his narrative. Graafstra takes us on a tour of where and how it all began- his early interest in computing, in what he calls fun "projects", and finally what led him to get an RFID tag implanted into his left hand in 2005. Graafstra then takes us on a journey of how he acquired his implant, and how it makes him feel to be a bearer of beneath-the-skin technology. He dedicates a great deal of space discussing health and safety issues relevant to RFID implants and concludes by emphasizing the importance for DIYers to take personal responsibility for their actions.

4. In the Beginning…

Technology has always been an interest of mine. From a very early age I was doing what lots of other inquisitive toddlers were doing… tearing things apart out of curiosity and not being able to put them back together. I was intrigued with seemingly magical things. Wood blocks can only hold one's interest for so long. But a record player or a telephone, those things just held some kind of mystery that needed exploration.

It was not until third grade however, where two very unlikely set of circumstances occurred which introduced me to the boundless potential the world of computers had to offer. I had the privilege of going to a country school. It was literally nestled in a forest, the trees of which we would build forts in during recess. It was very small with only four rooms, one for each grade. Oddly enough, the third grade classroom had a PET computer in it – the only one in the entire school. It had no disk or cassette tape storage and no operating system, just a PET version of BASIC in read only memory (ROM). For the greater part, it sat unused in the corner, a simple and momentary curiosity for most… but not to me. I turned it on and got a simple flashing cursor. What could it mean? What does it want me to type? The mystery was just too great to resist, but without any book or instruction manual, or anyone who knew anything about it at the entire school, I did not get far at all and started to lose interest.

Luckily, that year the school started a new program called Reading Is Fundamental (R.I.F.), where each student was allowed to pick out and keep a free book twice a year. I loved choose-your-own-adventure (CYOA) books, and started picking through the piles to find all the CYOA books available. I noticed there were two books in my stack of potential keepers that said "Computer Programs" on the cover. As I thumbed through those two books I saw there was "programming code" for IBM and Apple II computers, and I wondered if the PET would understand any of it. I picked one out and brought it back to the classroom, and that is when the fun began. If either the IBM or Apple code had worked perfectly "as-is", it may not have captured my imagination. The fact was, I had to ask for a PET programming book from the teacher, who did manage to track one down. With it, I could cross reference the code in the CYOA book with the PET BASIC book to make the code actually work. By the end of third grade, I was obsessed with the notion I could use a special language to tell the computer exactly what to do and it would do it. I felt like anything was possible! I immediately started begging my parents to buy a computer.

4.1. Technology and Having Fun

There is something special about the latest gadget that comes out or the next release of a fondly regarded software application. It is more than just being able to get a greater number of tasks done; it is also about exploring new possibilities. The creativity one can express through building solutions that work well and people use offers a

sense of accomplishment and even pride. That building process might turn out to require creating an entirely new technology of some sort, but for most that process is about extending existing technologies in some way.

Typically, extending a technology is done through standardized channels such as software components, libraries, software development kits (SDKs), and application programming interfaces (APIs). In the hardware realm one uses integrated circuits (ICs) with integrated functions, or entire original equipment manufacturer (OEM) hardware modules designed to be integrated into products. What I really love to do however is take an existing product and enhance it, sometimes using methods outside the typical channels. Some people might call that "hacking" but to me it is more about getting into the nuts and bolts of a product and making it do what you want it to do.

For example, I wanted to change out the deadbolt in the front door of my home to work without a key. I purchased an electronic deadbolt that worked with a key or by entering a PIN code by keypad. That was fine for a couple days, but the first time I had a handful of groceries and tried to enter the PIN code, I knew I wanted more. I wanted the deadbolt to unlock faster, without a key and without having to enter a PIN code. I just wanted it to know it was me and let me in, even if I had a handful of groceries. I ended up enhancing that electronic deadbolt to also accept RFID tags as a form of authentication. Later I expanded this idea further to allow a PC to log entries, allow me to set alerts, and even allow me to use other forms of authentication like email and text messages to unlock the door (great for letting neighbors in to check on your pets while you are away). There is no way I would be able to find a residential deadbolt that could do all that, let alone pay less than I did to build it myself.

4.2. Hobbyist or Entrepreneur?

I definitely have an entrepreneurial streak in me. I have started several service-based technology businesses and essentially worked for myself for 15 of the last 17 years or so. When it comes to RFID however, it's mostly just a hobby. I've done some consulting here and there, but when everyday people hear about my implants and the little projects I have built, they tend to ask me if I have any patents and/or plan to market some of these ideas.

The truth is most people have no idea what constitutes a good idea versus a patentable idea versus a marketable idea, or the amount of hard work and risk it takes to bring that little idea all the way to a market successfully. I have not had a good enough idea or met the right people yet with the business experience who could really take these things as far as they would need to go to be successful. Currently my now out-of-print niche market book *RFID Toys* has been the only commercial venture I have undertaken with regard to RFID, and for the time I have put into it I have basically made around $0.75 USD per hour. Not to mention the whole process was more stressful than it was fun. It seems to be a universal law that states "when you turn a fun hobby into a job, it usually stops being fun".

So at this point I am much more content with running my little RFID forum, answering people's questions as best I can, helping to solve problems, and putting out some good quality examples others can use to get a basic understanding of hobbyist RFID.

5. Getting the RFID Tag Implant

5.1. The Idea

When I think back to when I first heard about RFID implants, I was very young, perhaps seven or eight years old. I remember my mother telling me how pets were getting these new computer chips and that she did not think it was right. She, and basically everyone I grew up around, thought these things were evil and they would end up controlling humanity via satellite. I remember trodding around in the back yard contemplating the end of civilization as I knew it because of these "horrible devices". I did not doubt that point of view or those technological misconceptions for quite some time.

The thought of RFID implantation did not resurface until years later when I was faced with the decision of whether or not to implant my own pets with a "tracking chip" (a term still used by vets which does not help dislodge ever-prevalent misconceptions about RFID implantation). By then though I was much more sensible about my approach to technology, and I thoroughly annoyed the veterinarian by asking a ton of technical questions he could not answer. After doing more research (without the aid of a content rich Internet in the early 90s) and really looking into how it worked, I had my pets implanted and I came away with a much better understanding of what the technology could and could not do.

Over a decade later, in March 2005, I found myself moving heavy equipment in and out of my office almost every day. My office door had one of those latches that locked every time it closed, and I really hated having to fish around for my keys all the time. That got me thinking about how archaic the idea of a standard metal key really was. A key is nothing more than a hunk of metal, cut with a certain pattern that identifies me as "authorized". The typical key and lock system is also lock-centric, meaning the lock is the unique bit and each key that accesses it has to be duplicated from that unique key pattern. Once a unique key pattern is duplicated and distributed, tight control over that lock is essentially lost. I wanted a key-centric solution, meaning each key would be unique and

that unique key could be used with various locks. Being unique myself, ideally I wanted that unique key to be me.

I started looking into biometrics, things like face recognition technologies and fingerprint readers. The problem I ran into was the fact that these solutions, when done the right way, were very expensive and resource intensive to implement. At the time, there were also serious and valid concerns over the security and reliability of biometric solutions. Also, because I would need to put the camera or fingerprint reader outside, I was also concerned about vandalism. At the time, there were not many reliable biometric options rated for outdoor use that could tell the difference between my real face and a picture of my face, or my fingerprint versus a latex glove fingertip filled with water pressed against the sensor where the remnants of my own fingerprint left on the sensor would betray me. However, I did find a variety of very inexpensive RFID readers, and writing my own software to work with them was a no-brainer. The only down side to RFID was the fact I had to carry around an access card. That got me thinking about pet implants again, and I realized I could get the benefits of RFID without having to carry around anything.

5.2. The RFID Tag Acquisition

The first thing I did was look into getting an actual pet tag implanted, but there were a few issues with pet tags. I discovered there were many different kinds of RFID, and they did not all play well with each other. As it turned out, I could not find any cheap readers that would read the pet tags, and nothing really existed in the OEM hardware space which would have allowed me to easily integrate the pet tag into a custom built access control solution. Another issue was that pet tags have a special porous "anti-migration" coating on them that is designed to allow flesh to grow into and lock the implant in place, making removal or replacement nearly impossible.

There was another option for RFID implantation; the VeriChip. I had already heard about how the Food and Drug Administration (FDA) had approved the VeriChip for implantation into humans, but the VeriChip had the same issues pet tags had. Hardware options were very limited and expensive, and the tags also had anti-migration coating on them. I also found out that you must be registered in the VeriChip database to receive one of their implants, which I had issues with considering my goals and intended uses were all private in nature.

So, I figured I would just start with a basic keycard system and find some cheap RFID readers that were easy to interface with or were designed as OEM hardware I could easily integrate into my project. I found several reader options that read EM4102 based tags, so I started looking around for RFID tags based on the EM4102 chip. What I found just about made me jump out of my seat. I found a website that sold EM4102 based RFID tags that came in a glass ampoule form factor just like the pet tags! In addition, these did not have any coating on them. I immediately ordered the reader hardware and a few glass tags (figure 1).

Figure 1: Left hand with EM4102 implant and USB reader

While I waited for the equipment to arrive, I started calling tag manufacturers to find out what differences there might be between the glass tags I ordered (which were not designed for implantation) and implantable pet and human glass tags. It turns out there were only a few insignificant differences, the first of which was that tags did not have the anti-migration coating on them. Second, the EM4102 based tags did not use the International Organization for Standardization (ISO) animal implant data protocol, which I did not care about either. Finally, they were not manufactured or sold as sterile equipment. After several difficult conversations with various manufacturers, I found out the glass used in the tags I ordered and the animal (pet/livestock/human) implantable tags were the same stuff. That was good enough for me, so as soon as the tags arrived, I was arranging my first implant procedure. At the time I was running a managed computing service designed for medical clinics and had several doctors as clients. Once I confirmed the glass tags worked, I scheduled the implant procedure with one of my clients, a cosmetic surgeon, and started building projects. At the time, I did not tell anyone that I was scheduled for an implant procedure, partly because I was so busy creating my first access control project and partly because at the time I did not consider getting an RFID tag implanted in my left hand to be that novel of an idea. A couple days later after a five minute procedure my left hand was RFID enabled and I had a basic access control system built for my office door.

5.3. A Cyborg or an Electrophorus?

People often ask if I feel any different now, or if I can feel the tags under my skin. Over 5 years later, the answer

to both questions is no, not really. I do not feel any different, nor can I feel either implant unless I physically poke one with my finger. In fact, I often forget they are there until I have to use them.

At first it was kind of weird though, and during times of boredom I found myself mindlessly poking at them and feeling the implants under my skin. There was this kind of this cool factor to using them. I would put my hand to the front door and it would unlock, and people would be like "What!? Hold on… what just happened?" and at the time I kind of did feel like a cyborg of sorts.

But over time, the novelty wore off, and now they are just the useful tools I always wanted them to be. Even the interesting conversations I used get into with people regarding safety, security, privacy, religious concerns, and the future of the technology itself now tend to be redundant and repeat themselves constantly. Even my definition of what a cyborg is has changed.

The well-known Professor Kevin Warwick underwent the first human implantation of an RFID tag long before I even thought about doing it. He called that project Cyborg 1.0, which captured both headlines and imaginations. My definition of cyborg is a bit different however. A person with a cochlear implant or even a pace maker, those people are truly mixing technology with biology to become a cybernetic-organism (cyborg). What I have done is simply move an RFID tag from my pants pocket to a skin pocket. There is no biological interaction, and to me that interaction is what defines a cyborg. Michael and Michael [28] distinguish between what is traditionally considered a cybernetic-organism and DIY implantees who are merely "bearers" of technology (i.e. an electrophorus). I think that it is a good idea to have a term that separates us from cyborgs.

So why even bother with implanting a tag in the first place? A lot of people also ask me why "take the risk" putting it under my skin? Why not wear a watch or ring or something with a tag in it? The simple answer is- I won't wear a watch or a ring for very long without losing it. It would be like wearing a backpack everywhere you went; you would just want to take it off all the time due to it being uncomfortable. When I looked at what was possible with glass encased tags and the history these types of RFID implants had with pets, I really did not think twice about getting one implanted. Not to say that I did not do my research first [29], but the actual decision to get a tag implanted was made in a matter of seconds, and I have never regretted it.

6. Is Implanting an RFID Tag in the Body a "Safe" Practice?

Safety is a big issue, and is still a concern for every do-it-yourselfer (DIY) tagger that is considering or has already undergone an implantation procedure. Given DIY tagging is done through the sheer will of one's own accord, every tagger must take full responsibility for their decisions and actions, their health, safety, and the ultimate outcome of their RFID implantation endeavors.

As the DIY community grows, and more people get non-FDA approved glass tags implanted in non-FDA approved locations, so too the concerns over the safety of RFID implants will grow (Table 1).

Table 1. Primary Safety Concerns for DIY Taggers

Safety Concern	**Description**
Sterilization	Glass tags not designed for implantation are not manufactured, packaged, or sold in a sterile fashion.
Location	The area of the body the glass tag is to be implanted.
Migration	The movement of the tag from the original implantation site may cause health and usability complications.
Structural compromise	The glass encasing the tag components fractures or is crushed while inside the body.
Removal & replacement	The ability to easily remove an implanted tag at a later date.
Cancer Risk	There has been a lot of concern over a number of studies which draw a link between RFID implants and cancer [30].

6.1. Sterilization

A common method for sterilizing medical equipment is to place it into an autoclave, where heat and pressure destroy any pathogens. The temperature reached inside an autoclave however, is well above acceptable operational and storage specifications for most RFID tags. Due to this, I did not autoclave my glass tags. Both my implants were sterilized by soaking them in a liquid antiseptic for a few minutes before the implantation procedure. As others learnt of what I had done and expressed interest in getting a RFID implant, I suggested they avoid using the autoclave to sterilize their tags as the heat may damage them.

I later performed a test, placing five 2x12mm EM4102 based glass tags in an autoclave for a full one hour cycle. All five tags came out sterile and in working order. On the *RFID Toys* forum, other users reported similar success with the autoclave and EM4102 tags, leading me to now suggest purchasing at least two tags and putting them through the autoclave prior to implantation. Of course, testing the tags after the sterilization process and before implantation is strongly suggested.

I believe read-only EM4102 tags are able to withstand the high temperatures of the autoclave because the IC chips typically have their unique IDs laser etched into

ROM at the factory. Other tag families such as the Philips HITAG with writable memory blocks may not fare as well with such high temperatures, and significant damage to the writable blocks may occur.

6.2. Location

For his Cyborg 1.0 project, Professor Kevin Warwick decided to implant a glass encased tag into the upper inside of his left arm, beneath the inner layer of skin and on top of the muscle [31]. The location seemed to offer a safe haven for the fragile glass casing. Nine days later the tag was removed without complication.

Unlike the typical VeriChip or pet identification applications where a handheld reader is brought in close proximity to the implant, I use my implants in applications where the tag must typically be brought to a fixed reader. Because the normal operational range of small cylindrical glass tags is anywhere from one to four inches, I chose to implant both my tags (one in each hand) into the webbed area between my thumb and index finger, just under the dermis layer. This location allows me to easily position my RFID tags very close to a reader, while still providing an amount of soft tissue to cushion and protect the tags from blunt force impact. Being just under the skin and not in muscle tissue also allows for easy removal or replacement. Most, but not all, DIY taggers have chosen the same location for their implants.

6.3. Migration

Glass encased RFID tags which are designed for implantation in animals or humans typically have an anti-migration coating of some sort affixed to the glass casing. This porous material allows the implantee's flesh to grow into the material which stops the tag from moving around in the body.

The primary purpose of keeping the glass RFID tag located at the selected implantation site has more to do with consistency and ease of use than potential health risks. Veterinarians need to be able to reliably scan the same area on every pet to determine if the animal has a microchip. If tags were able to migrate from their implantation site, vets may fail to successfully scan and identify a tagged pet. In the case of tagging livestock, you do not want to accidentally have a tag migrate into a piece of meat that ends up on the consumer dining table or in scrap pieces of carcass which may be rendered for a variety of food chain-related uses.

Like myself, the DIY tagger community has taken to using glass tags which are not designed for implantation, and as such do not utilize this coating. The lack of coating allows tags to be removed or replaced much more easily than if they had this coating, and after five years neither of my tags have migrated from their implant sites. This may be due to the fact that my tags rest in congruous elastic skin tissue rather than fibrous muscle tissue which is bundled into separate strands that an implant could move between.

6.4. Structural Compromise

The thought of a glass capsule being crushed into small sharp shards while it is still inside one's body does not produce feelings of excitement or enthusiasm. Concern over the structural resilience are warranted, since the cylindrical glass capsules encasing the RFID tag's electrical components (IC, antenna coil, etc.) have very thin walls and are easily crushed using common medical instruments like forceps.

The FDA initially considered the VeriChip as a class II device which requires special control testing [32]. However this testing did not include any sort of structural integrity test. No crush/penetration tests were performed, and key factors such as lateral stress or compression limits. are unknown. Later, the FDA reclassified the VeriChip [33], placing it in the type III group of devices which has even fewer controls. The health risks specifically identified in the K033440 reclassification include [34]; adverse tissue reaction, migration of implanted transponder, failure of inserter, failure of electronic scanner, electromagnetic interference, electrical hazards, magnetic resonance imaging incompatibility, and needle stick. No mention of glass casing fracture or structural compromise.

After five years using my own implants and talking to many DIY taggers who have followed suit, I have not heard of anyone having any issue with crushed or compromised tags. Still, the concern is valid, and the choice of implant size, location, orientation, proximity to bone and other inflexible tissues all play a role in avoiding structural compromise.

6.5. Removal and Replacement

At the time of this writing, I have not observed any accounts of DIY taggers getting their implants removed or replaced. However, the implantation of glass tags that do not make use of a polypropylene polymer based anti-migration coating should enable the tags to remain detached and separate from the body, making removal easier.

Rather than implanting tags deep into muscle tissue, which would require invasive surgery to locate and remove, DIY taggers tend to prefer shallow implantation just under the skin. This reduces both the complexity of locating and the size and nature of the incision required to remove the tag. It also means the body is less prone to inflammation and infection-related side effects.

6.6. Cancer Risk

What started off the recent cancer discussion surrounding animal identification RFID implants was a paper published about a French bulldog who received an RFID "pet microchip" implant in September of 2003 at age 9. In April of 2004 he was examined and found to have a "lump" at the implant site [30]:

> "[o]n April 2004, Leon, a 9-year-old male French Bulldog, was examined by the referring veterinarian, based in Guelph, Ontario (Canada), for the sudden growth of a subcutaneous 3X3-cm mass located on the dorsal midline of the neck, just cranial to the shoulders. The dog was regularly vaccinated against the most common canine infectious diseases and rabies, and was microchipped (Indexel, Merial, Lyon, France) in September 2003."

This news spread quickly, and older studies were dug up revealing similar links in laboratory mice and soon the firestorm was in full swing. I started getting all kinds of concerned emails from DIY taggers, media interview requests, and more hate mail from concerned members of the public. After reading the studies however, it became clear to me that the risks were not as exaggerated as the media and RFID critics made them out to be.

For example, many articles citing the above-mentioned study claimed the French bulldog "had a giant tumor surrounding the implant" and that the dog had died "an untimely death" from that cancer. Upon simply reading the paper I found both those assertions were false [30];

> "The microchip was found, not embedded within the tumor, but immediately adjacent to it, surrounded by a very thin fibrous wall (approximately 1 mm thick) and some fresh hemorrhage."

Reading further I found [30];

> "After surgery, the dog was not vaccinated or microchipped again. Up to now, the dog is well, and no recurrence has been observed."

So basically the dog was doing fine two years later when the study was published in 2006, and the paper calls out various other possible causes such as postinjection fibrosarcoma (a well-known pathologic entity) characterized by inflammatory peritumoral infiltration, multinucleated giant cells, and myofibroblastic cells.

The plainly published facts did not seem to matter though. Both mainstream media and RFID critics alike jumped all over the academic paper and dug up other studies from which to pull completely out of context findings. However, other papers cited within that French bulldog study do point out implants which were embedded in the center of neoplasms. So what is going on here? I started looking into other studies after visiting sites like antichips.com [35] publishing statements like the following:

> "[i]n almost all cases, the malignant tumors, typically sarcomas, arose at the site of the implants and grew to surround and fully encase the devices. These fast-growing, malignant tumors often led to the death of the afflicted animals. In many cases, the tumors metastasized or spread to other parts of the animals. The implants were unequivocally identified as the cause of the cancers."

The bottom line for myself and other DIY taggers was simple: should we be concerned about this? For the most part, what I found after digging into many of these studies was that these laboratory mice were either genetically prone to cancerous growths or subjected to radiation and/or chemical carcinogens in an effort to intentionally stimulate cancerous growth. So now the question becomes, what would cause cancer to grow around an implant? There could only be two things; the glass used to encase the RFID tag or the anti-migration coating used to lock the implant in place in the flesh. In both instances more research is needed, however it is my personal opinion that the porous coating will likely be revealed as the leading factor in stimulating cancerous growth in the area immediately surrounding implantation sites in predisposed specimens.

6.7. Taking Personal Responsibility

While I believe everyone today needs to take a bit more personal responsibility when it comes to the decisions they make, for a DIY tagger this is especially true. A draft DIY tagger code is depicted in Table 1.

Table 1. DIY Tagger Code

A DIY Tagger must;
1. Take responsibility for doing their own research. Even if other taggers have done what you are about to, nobody is able to guarantee its safety, features, or function.
2. Figure out what tags have the features you are looking for. Research encryption technologies and their weaknesses. Find out if the reader hardware that supports those features is available and affordable.
3. Learn all you can about the tag you want to implant. Check into the type of glass used. Ask about structural integrity. Review other people's experiences.
4. Determine the size of tag you want. Find out if it will work with the reader hardware you have identified and that it will provide the read range you desire.
5. Decide where you want to implant the tag in the body. Discern the pros and cons of each particular location, including issues related to ease of use. Get advice on orientation and depth.
6. Before implanting, thoroughly test the tag, its features, and read range with the reader hardware you have obtained. Ensure it will work properly with the applications you intend to implement post implantation.
7. Research the best sterilization techniques for the particular type of tag you plan on implanting. Some have had success with autoclaves, while many have relied on liquid antiseptics. Verify the pros and cons of each sterilization method available to you and how they apply to the type of tag you have chosen.
8. Decide on implantation technique. A glass tag can be implanted

using several different methods. Discuss the pros and cons, and decide on a suitable method that you are comfortable with.
9. Take full responsibility for your decision. Some taggers perform the implantation procedure themselves however, most choose to use a third party. If a third party will perform the procedure, do your research. Find out if they have worked with subcutaneous implants before and they are comfortable doing the procedure you are asking them to perform. Release them of any liability using a suitable release form [36]. Being a DIY tagger, more than likely you will not be getting a FDA approved tag and it is in no way honorable to blame someone else for your decision should something go wrong.
10. As a member of this small but growing community, it is important that you share your experience(s). Get involved in forums, comment on blogs, and post your projects so that collective knowledge can grow.

PART B- SOCIO-TECHNICAL ISSUES

In Part B, Michael and Michael relate events about Graafstra, and Graafstra relates events about others. The whole Part is written in the third person voice. Where direct quotes are used, Graafstra's sentiments and interview responses are captured verbatim. In this part the main socio-technical issues facing RFID implantees is discussed, including security, privacy, data ownership (personal versus commercial), social issues (e.g. religious responses and socio-political concerns), law and policy. Due to space limitations the authors do not go into great detail in each of the socio-technical issues addressed, rather, this remains the aim of a future work-in-progress. Part B concludes by acknowledging the role of all the stakeholders in the feedback mechanism towards social innovation.

7. RFID, Implantees and Security

RFID is a very broad term that encompasses a plethora of technologies that are all designed differently but do one thing; identify something via radio frequency (RF) communication. That includes everything from the World War II identification friend or foe (IFF) systems to implantable tags to RFID enabled credit cards. As recent as 2006, the United States Department of Homeland Security (DHS) was debating the use of RFID for humans. In reports [37] and [38], it is clear that while one DHS full committee found that deployment of RFID for human identification should be done with caution, the second report by a subcommittee ruled that the practice was inappropriate [39]. The recommendation by the DHS subcommittee read [38]:

> "[t]here appear to be specific, narrowly defined situations in which RFID is appropriate for human identification. Miners or firefighters might be appropriately identified using RFID because speed of identification is at a premium in dangerous situations and the need to verify the connection between a card and bearer is low. But for other applications related to human beings, RFID appears to offer little benefit when compared to the consequences it brings for privacy and data integrity. Instead, it increases risks to personal privacy and security, with no commensurate benefit for performance or national security. Most difficult and troubling is the situation in which RFID is ostensibly used for tracking objects (medicine containers, for example), but can in fact be used for monitoring human behavior… For these reasons, we recommend that RFID be disfavored for identifying and tracking human beings. When DHS does choose to use RFID to identify and track individuals, we recommend the implementation of the specific security and privacy safeguards..."

Many RFID technologies are insecure by design, or employ weak or flawed encryption methods. However, that is not to say that an RFID system using an insecure RFID technology is itself insecure by default. Despite the early 2006 findings of the DHS reports, there are U.S. RFID-based schemes which are now in widespread use. Graafstra points to the "trusted traveler" RFID-enabled NEXUS card as an example [40]. The NEXUS card is a U.S. government issued travel card that has an ultra high frequency (UHF) RFID tag inside, which does not employ any encryption technology. Any Generation 2 (Gen 2) UHF reader can read the unique code stored in the tag. The RF technology used by the NEXUS system is insecure, but the NEXUS system that allows one to travel across various borders is not inherently insecure, so one's identity is theoretically not at risk. Graafstra elaborates: "[t]he Gen 2 ID stored in my card is a unique number, but that number in no way gives up any information about me to an attacker who may be able to read it- it is just a number. The systems that link that ID number to actual important information about me are secured in far superior ways than the systems that store your library card account, or in some states, even your driver license information."

Like NEXUS travel cards, the VeriChip medical implant does not employ encryption in any way. Any passive 134 kHz reader capable of understanding the VeriChip data protocol can read the ID of any VeriChip implant. Even though these IDs are tied to medical records, the ID itself is useless to a random attacker because access to those records also requires both access to a medical network and a health professional's account password. Systems that employ encrypted RFID tags have, in the past, relied heavily on the crypto algorithms in the RFID tags themselves to secure the system in which RFID technology was integrated into.

Graafstra uses the example of ExxonMobil's pay-at-the-pump SpeedPass system and the many vehicle immobilizer systems that make use of the 134 kHz TI DST tag, which secures communication through a

challenge/ response mechanism. The problem with these systems Graafstra outlines is that because they do not possess any other security mechanisms outside of the RFID tag's encryption, the systems are vulnerable to fraud by cracking the encryption algorithm used by tags to generate proper responses to the challenges issued by commercial readers. Once the DST tag crypto had been cracked [41], ExxonMobil had to redesign their SpeedPass payment system to implement credit card style fraud detection to detect and prevent fraudulent transactions. Other tag chipsets that employ encryption mechanisms like MiFare and HITAG S have also been compromised, leading systems designers to rethink security and start balancing RFID encryption with other security mechanisms.

Graafstra points to the fact that his left hand contains an EM4102 tag, which by design does not utilize any security measures. The tag ID is readable by any 125 kHz reader able to understand EM4102 tags and get close enough to read the tag. He comments, "[e]ven so, I use that tag to unlock my back door when I get home from work. Many would argue that my home is completely insecure because my implanted tag is not secure. I do not disagree, but I also do not believe that I am at any greater risk of home invasion as a result."

7.1. Security Context

Quite often people think security is a pass/fail scenario. Either something is secure or it is not. In reality, a security policy is a collection of systems, methods, and procedures that protect an asset by removing enough value and/or applying enough deterrence that a potential attacker will not even bother or quit trying. To get to the heart of the matter, you have to start with the premise that nothing is truly secure. If there is enough desire, determination, and resources available to an attacker, they will eventually succeed.

The inherent lack of encryption in many RFID tags impacts DIY taggers building personal use applications differently than it does commercial enterprises like VeriChip, ExxonMobil, and VISA/MasterCard with their public use applications. Graafstra argues that despite the fact that he uses an insecure RFID tag to unlock the back door of his house, if a random attacker were to get close enough to read the ID of the EM4102 tag implanted in his left hand, they would not have any way to derive his identity (e.g. name), his home location (e.g. where he lives), or his phone number. This is however discounting the simple fact that one can be covertly followed in a public space. Graafstra believes an attacker intent on entering his home would generally use more mundane approaches such as breaking a window, than going to the effort of a technical approach. Graafstra's observations are quite correct, for the time being, until more and more DIY taggers start to rig up their personal living spaces with readers.

7.2. Designing with Security in Mind

7.2.1 RFID Cards in the Corporation. Assuming the encryption algorithms used by "secure tags" today have been or will soon be cracked, system designers need to shift from exclusive reliance on tag encryption and incorporate other features to make their systems more secure. Starting with the RFID tag itself, several businesses integrate RFID access control tags with their employee name badges. These can be constructed with a simple push button membrane or switch that connects the RFID antenna to the tag IC. Graafstra recommends that given the user already has to handle their name badge in order to place it close enough to a reader to get a valid read, why not require a simultaneous press of a switch while doing so? For Graafstra, such a simple design change would eliminate almost every possibility for a non-consensual read by malicious users.

Access control systems can also be designed with more intelligence than they currently possess. Graafstra relates the following scenario with respect to physical access control to a corporation. Assume Dave of XYZ Corp has been the victim of a malicious card scan. The attacker intends to emulate Dave's card ID to gain access to the building by mixing in with the morning rush of people. Dave enters the building first, and then the attacker enters five minutes later. Dave goes to his desk by way of the elevator and a couple of other security doors where his badge is used. The attacker takes a different route to his target, using his emulated Dave badge. The system should be able to recognize the odd access pattern through validation and alert security, possibly offering up an employee photo along side a time stamped video of the various RFID access events. Security personnel could then quickly determine if there was an attempted security breach they needed to address. If so, they could lock down Dave's badge so it no longer functioned, and even set up real-time mobile alerts to tell roving security guards if and where the badge was trying to be used. In theory, Graafstra is correct, system designers for the greater part are not thinking foolproof security blueprints but the reality is that budgeting and security staff resourcing would possibly not allow for such sophisticated security interventions; detection is one thing, acting on an email or mobile alert is another.

7.2.2. RFID Implants and DIY Tagger Protection. Graafstra has spent a great deal of time thinking how DIY taggers could protect themselves from what he terms "casual" security attacks. He has documented his solution as follows. Using the read/write memory blocks that many types of tags have is a good way to increase both the risk and the amount of effort an attacker would have

to exert in order to successfully execute an attack. For example, the HITAG S 2048 tag in his right hand uses 40 bit encryption to protect the contents of its 255 byte read/write memory blocks. The 40 bit encryption will not stop a serious attacker but it will diminish the casual attacker's ability.

Graafstra elaborates in detail: to enhance the security of a system, the memory space can contain a pseudo-random rotating hash which is used in conjunction with the tag's read only unique serial number to confirm authorized entry. The hash is generated based on a secret key that only your system knows, coupled with an incrementing counter used to salt the hash. When the hash is read, the system uses much more powerful encryption algorithms to calculate and match the hash stored on the tag than the tag itself is capable of utilizing. The counter value is derived and checked against the system counter to ensure the encrypted hash is correct for the tag IDand to ensure the counter value is moving forward and not staying still or moving backward. Upon successful authentication, the counter is updated and a new hash is written to the memory blocks. If an attacker were able to break the 40 bit encryption to gain access to the memory contents, a successful attack is still orders of magnitude more difficult to pull off than plainly emulating an unencrypted tag. Also, a successful attack would provide a very small window of opportunity as any use of the original card would invalidate the cloned tag's counter/ hash combination.

8. RFID Implantees and Privacy

8.1. Misconceptions about RFID Technology

There are a lot of misconceptions in the general community about how various RFID technologies work, prompting unfounded fears of global positioning system (GPS) satellites tracking embedded tags and implants. This is not to say that in the future RFID tags will not be able to interface with a number of different mobile technologies but for now this kind of global tracking is unavailable. And this not because it is not technically feasible to do so, but rather because large-scale agreements have not yet been entered into between a variety of stakeholders.

Active RFID tags can transmit data very long distances, anywhere from a few feet to 10 miles or more, but they use battery power to do so and are bigger and bulkier than passive RFID tags. Inversely, passive tags like those used in retail inventory applications and glass encased implants are typically smaller. They do not have internal power sources, and can generally communicate with readers from only a few inches to a few feet away depending on chipset, size, and frequency used. Certain experiments have shown, under ideal conditions, that passive UHF tags can be read from several hundred feet, but those are special test cases not practical real-world scenarios. Even so, the prevalent fear amongst every day consumers is that, somehow, carrying an RFID tag of any kind will allow "them" (e.g. government agencies) to track your every move.

Today, people's activities are logged constantly. From every non-cash purchase you make to every RFID "fast pay" toll booth archway driven under to every phone call made, something somewhere is logging that activity. Graafstra points out the potential for data mining through a variety of sources, emphasizing that "[n]obody is upset about this type of information gathering as they are about RFID technology… [and that] the backlash from specific segments of the public seems to center on embedded tags, whether they are embedded in clothes, in driver license cards, or people's bodies." For Graafstra, the stated concerns indicate people believe RFID is capable of more than it really is, and that those perceived capabilities culminate as fear of massive privacy invasion on an unprecedented scale.

8.2. Some Consumer Concerns Warranted

Although Graafstra does acknowledge that some consumer concerns with respect to RFID are valid, he believes the concern is misdirected at the technology itself rather than on human factor issues, e.g. consent. He emphasizes that unobtrusive reads amount to privacy problems, and that to some extent history has already proven that this is a valid concern. Clothing manufacturer Benetton, for example, was found to be embedding RFID tags into women's garments in an effort to quickly identify past customers as they walked into their storefronts [42]. Graafstra also singles out the idea of function creep, inferring that consent given for one use may be extended at a later date as the application grows. People who have to travel over toll roads and bridges may opt to use an RFID tag permanently affixed to their windscreen for automatic payment may find that the terms and conditions they originally signed up for have changed, and in some instances without warning. For example, some state governments collect data from RFID tollway tags to monitor traffic patterns on their roadways without notifying users. Furthermore, logs of which tags passed what checkpoint at what time are kept for undisclosed periods of time and log data could potentially be shared with an unknown number of requestors. Graafstra questions whether the next step will indeed be to issue speeding fines based on how fast people have traveled from checkpoint A to B.

8.3. RFID Tags: Personal versus Commercial Use

Now let us take a hypothetical look at RFID privacy in a hostile environment, and the differences between

personal use and commercial use contexts. When you sign up for a commercial service that utilizes RFID in some way, you surrender your personal information which is tied to that unique tag ID. Assuming the company does not share your tag ID or your information with any other person or company, your information is still associated with that tag ID and could be used to violate your privacy through nonconsensual reading of the tag. The problem gets worse if that company sells or shares that data with other companies or people.

In a personal use context, you never surrender your personal information to anyone, and your tag ID is in no way associated with you. The best any snoopy corporation or government could do would be to aggregate non-identifiable data together to determine patterns of anonymous tag IDs. Of course, there is always the concern that associations could be made through other means. For example, suppose a checkpoint was set up that could read a large cross-section of tags from RFID enabled credit cards, access cards, various tag types in UHF, high frequency (HF), and low frequency (LF) frequency ranges, etc. A properly read and decrypted RFID credit card will reveal the cardholder's name, and if other tag IDs always showed up in logs when "Dave's" unprotected RFID-enabled credit card did, then one could assume that all those RFID tags resided in Dave's wallet with his credit card. While this fact may be disconcerting, Dave can still take measures to protect himself, by choosing to shield his tags and cards [43], or even leave them at home. But what about implanted RFID tags? Leaving those at home is not possible and shielding them could be socially awkward (always explaining why you're wearing tin foil gloves), even though increasingly sentinel jackets are coming onto the market.

Implantable tags like VeriChip which are sold to the public for use within commercial systems do present different privacy challenges than the glass tags implanted by DIY taggers. A commercial system means uniformity when it comes to things like implant location, type of chip, data protocol, and frequency. Since the implant location is common to all users (e.g. in the case of the VeriChip it is the triceps muscle of the right arm), Graafstra believes that a simple reader can be set up at typical arm height in a doorway to casually capture tag IDs from passers-by. With enough people using a common system and enough readers placed in enough doorways, unique traffic profiles could be created for each tag ID much more easily.

9. RFID Implantees and Society

9.1. Pet and Animal Identification Systems

Whether people like to admit to it or not, society today is full of RFID tag and transponder technologies embedded in buildings, in vehicles, in packages, in clothing, in animals, and in people's wallets. This diffusion will continue to grow annually with predictions that 26.1 billion units will be sold in 2011 alone [44]. Passive RFID tags designed to be implanted into animals have been around since the early 1980s. After being widely tested by several companies in the early 1990s (such as Destron's LifeChip [45]), the number of pets with implanted RFID tags has skyrocketed as local councils and state governments move to make the chipping of domesticated animals compulsory [46]. To date this practice, above all else, has done more to raise public awareness of the positive applications of implantables than any other use of implantable RFID tags.

Today RFID tags, both passive and active, are used to keep tabs on everything from pets to livestock to wild animals on land, in the air, and in the sea. Graafstra notes, that the U.S. Fish and Wildlife Service uses "microchipping" in its research of wild bison, black-footed ferrets, grizzly bears, elk, white-tailed deer, giant land tortoises and armadillos. New developments in sensors, RF, and power harvesting technologies are also leading the way to "implantable" RF enabled sensors embedded into trees (e.g. orchards). These "tree tags" relay information about the health of the tree, the surrounding forest environment, and raise an alarm in the event of a forest fire [47].

9.2. Is it Hip to Get the Chip?

Since Michael and Michael began their research into non-medical ICT implantables in the mid-1990s, they were preoccupied by the question of diffusion, and predominantly the notion of who influenced whom within the context of an actor network. For example, who was the first DIY tagger implantee? What inspired them to get an implant? How did they come to know of other implantees? When Graafstra received his first implant, he knew he was not the first. Professor Kevin Warwick had long since completed his Cyborg 1.0 project, and VeriChip had received FDA approval and was already implanting customers. Graafstra believes what he embarked on in early 2005 created such a media interest because he got the implant on his own accord, and he self-reported it all using photographs and video via the web. He also was comprehensive in his documentation of what he planned to do with his implant, and quickly demonstrated its functionality. Finally, he also believes implanting a RFID device in the hand, and not in the upper arm, sparked more intrigue and inquiry.

Since that time VeriChip (now PositiveID [48]) have been marketing their products, and to date allegedly have between 1000 and 2000 people registered in their medical implant database, although some estimates are much lower and some much higher. The size of the DIY community is, by its very nature, unknown. Yet shortly after news of Graafstra's implant became public, he was

contacted by lots of members from the general community who wanted to know how to obtain an implant themselves. Graafstra is frank, when he states: "today, anyone can buy glass encased RFID tags and watch self-implantation procedures online, and then go to their local piercing shop to get it done". One is left pondering, however, whether DIYers are engaged in the act of blueprint copying or idea diffusion, and the repercussions that this might have on how RFID implants are utilized in the future. Jared Diamond describes blueprint copying as the act of copying or modifying an available detailed blueprint. At the opposite end of the spectrum lies idea diffusion, which is when one receives little more than the basic idea and has to reinvent the fine details [49].

Graafstra estimates there could be roughly 200 or 300 DIY taggers around the world who have opted to get a non-commercial RFID implant. Graafstra is reflective, that while he does not know the exact number of DIYers, he does know (or at least understands) the inner motivations of some DIYers to get an implant is less than technical. He said:

> "I've been contacted by 16 year old kids who have had to wait until they are 18 to get this done due to – what I think are – valid parental concerns. On my *RFID forum*, I have repeatedly suggested that it is not worth taking even a minor health risk to get this done if you do not really know why you want it and what your goals are once you have it. Even so, when I asked a couple of these kids why they wanted to get an implant and what they were going to do with it, in both cases their responses were something along the lines of "because it's cool" and "I'm not sure what I'm going to do with it". I have also been contacted by body-*modders* who, after getting their fifteenth cosmetic subcutaneous silicone implant, wanted something different… something that was actually functional in some way, even if they did not have any plans to actually use it."

However most DIY taggers tend to view their implant as a utilitarian tool to be used in daily life with projects they have built themselves. In this loose-knit community [50] of practical DIY taggers, one could argue it is actually "hip to get the chip," even though the best place for it is unanimously the hand!

9.3. RFID Implants for Families: Peace of Mind?

When considering the applications that Applied Digital Solutions were marketing in 2003, and those that were subsequently marketed by the VeriChip Corporation, Graafstra circumspectly calls the "brochureware" confusing from a marketing perspective at least. For Graafstra, any sort of communication that misleads the public about pinpoint location positioning via the RFID chip is widely fantastical and utterly disappointing. He does not understand, how on the basis of a commercial vision, the Mexican Attorney General allowed himself and some of his staff to be VeriChipped with an "anti-kidnapping chip". Parents, like that of Jeffrey and Leslie Jacobs were also lead to believe, probably through mainstream public misconceptions about the function of RFID, that getting a VeriChip implant would provide their whole family with security and "piece of mind" [51].

The fact is, no RFID implant can provide that kind of security and "traceability" that certain members of society are looking for or are afraid of. The best an RFID implant can do today, is identify the *person* sitting two inches away from the scanner. That may help identify a corpse, but it will not help find missing persons. This is not to say that in the not-to-distant future, technological convergence might enable very sophisticated applications to be built. The idea of implanting prisoners, persons on parole or persons on extended supervision orders (ESOs), or military service-people with digital implantable dog tags has been considered but has yet to take place. Again, Graafstra points to public polls where consumers believe that implanting prisoners or parolees would make society "safer" because it would make implantees easier to track down and keep in confined zones if required, but he is adamant that these kinds of solutions are not yet possible using implanted RFID tags. The permanency of FDA approved implantables is especially disconcerting as they possibly do not give one-time offenders, or once military service personnel, an opportunity to rehabilitate or move onto other professions [52]. For Graafstra this is a violation of service terms, since imposed subcutaneous FDA approved commercial implants are long lasting physical remnant of requirements that have long since expired, and no longer valid.

9.4. RFID Implants for Employees and the Law

To date, no employer has required an employee or potential employee to obtain an RFID implant in order to become or remain employed. Critics jumped on inaccurate media reports that CityWatcher.com, a now defunct municipal surveillance company, had required employees to get implants to access sensitive datacenters. The fact is three employees did receive VeriChip implants and the company paid for their procedures [53]. However, five employees opted to simply carry around an access card to access those same areas. Implantation was optional, not compulsory. There was a similar optional implantation of employees at the Baja Beach Club in Barcelona, Spain but this was not really publicized.

As a preemptive measure several states in the U.S.A passed laws that banned enforced implantation by employers [54]. For Graafstra the problem has more to do with laws and regulations which target a technology than the very 'act' of surveillance. Graafstra notes the law

passed in California (Senate Bill 362) that banned employers from mandating that employees or potential employees must get an identifying implant in order to perform their work [55]. The law is written with a heavy slant toward a "radio frequency device", but an argument could be made that this law also covers biometric technologies and other location based mobile technologies. Intentional or not, the definitions section states;

> *"Identification device" means any item, application, or product that is passively or actively capable of transmitting personal information, including, but not limited to, devices using radio frequency technology.*
>
> *"Subcutaneous" means existing, performed, or introduced under or on the skin.*

For Graafstra such laws do not do anything for employee workplace rights as a plethora of other technologies exist to determine the whereabouts of workers within campus-based facilities like manufacturing plants. For Graafstra, it has less to do with implantables, and more to do with employee privacy.

9.5. Is Getting an RFID Implant Evil?

Many people believe that RFID implants will harm society and/or humanity in some way. The two most vocal groups are people expressing their religious views, and people expressing their socio-political fears [56]..

9.5.1. Religious Concerns- "Mark of the Beast". The interpretation of the *Book of Revelation*, the last book of the New Testament, by some Christians has caused Graafstra to be the target of backlash by some members of the believing community. Graafstra points to the following verses that RFID critics with a religious orientation invariably point to (Revelation 13:16-18):

> *"Also it causes all, both small and great, both rich and poor, both free and slave, to be marked on the right hand or the forehead, so that no one can buy or sell unless he has the mark, that is, the name of the beast or the number of its name. This calls for wisdom: let him who has understanding reckon the number of the beast, for it is a human number, its number is six hundred and sixty-six."*

From the correspondence that Graafstra has received, he has deduced that some Christians believe that "the devil" will require all of humanity to receive a mark of some kind in order to be able to participate in day-to-day societal transactions. And that furthermore, wise people will recognize that mark and attempt to refuse it. Those who are most vocal about such beliefs have gone so far as to insult and threaten Graafstra, and other DIY taggers about their involvement in ICT implants. Graafstra has spent some time reviewing the passages himself countering:

> "[s]ince so many people seem to take the Bible so very literally, in my opinion there are a few things they are either ignoring or do not realize. In verse 16, it says "he causeth all" which means everyone will receive "the mark" regardless of whether they want it or not. In verse 17 it says "no man might buy or sell [without the mark]", meaning absolutely nobody will be able to do this, even if you are living in an igloo on the North Pole trying to do it illegally. In verse 18 it says nothing about wise people refusing the mark or even being able to, it only discusses how to recognize it."

There are, however, a number of places in Revelation (16:2, 19:20, 20:10) where it seems evident enough that people will indeed have to make a choice, viz., "the mark". This was certainly the interpretation of all the *early church* exegetes who dealt with the prophecy [57]. For Graafstra, however, the mark and the beast are potent warnings about willing subscription to oppressive systems, and how using the tools of those systems will only strengthen such systems. It is very important to distinguish between oppressive systems that use technologies to subjugate a people, and technologies that liberate them, or those being used in a private, personal context.

9.5.2. Socio-Political Fears. Some people believe that RFID implants may one day be mandated on the general populace, instituted by totalitarian governments and other authoritarian regimes [58]. Such persons, firmly believe that RFID technology, particularly implant technology, will in some way enslave humanity and cause a major digital divide. These groups generally point to the involvement of large-scale corporations in the conception, development and implementation of RFID implant technology, and to some extent generate conspiracy theory-like scenarios about the future.

Graafstra also notes that he has been threatened both directly and indirectly by some people harboring socio-political fears. He elaborates:

> "I have been accused of aiding the government and private corporations in their efforts to deploy RFID implants on a wide scale. I very strongly feel it is a priority to attempt to engage these accusers in civil discussion and attempt, however futile, to impart a bit of knowledge so they might understand how these implants function and ultimately the difference between and separation of DIY taggers from commercial solutions by corporations like VeriChip."

Simply put, some advocacy groups are not helping the debate and whatever valuable insights they might have is lost in a host of "background noise". The practice of

'attracting' hate mail is common among implantees (both in academia and DIYers), and as Graafstra emphasizes, it often does not encourage a healthy exchange of ideas, although it does alert developers to the social realities that may be stifling adoption and potential ethical liabilities development make need to address.

10. RFID versus Other Technologies

In Graafstra's opinion it is not so much that consumers should be wary of what RFID can do, but of the widespread diffusion of powerful biometrics and pinpoint positioning technologies. Despite that biometric identification is used extensively all over the world to identify and log all kinds of things, Graafstra notes that it does not receive the same amount of attention that RFID does from advocacy groups. Graafstra sums it up very well when he reflects:

> "I think the reason for this is that RFID requires a tangible object carried by or implanted in the object to be identified. Biometric identification does not require this because the identifier is your own body. As biometric monitoring devices get more and more unobtrusive and fade further into the urban landscape, I fear lack of motivation will continue to get worse until a series of very serious civil rights violations occur, but by then we might have a social environment so riddled with circumstances where privacy and basic rights have been traded away for the illusion of security that the general public may actually be afraid to turn off and live without these systems."

Today's biometric technology can identify you by your full body [59], face, voice, fingerprints, chemical scent, gait mechanics, emotional expressions, your DNA, and even your own shadow [60]. Video cameras are very cheap and easy to deploy, and developments in video processing enable face recognition systems to accurately identify entire crowds of people much faster and more accurately than ever before. If your face is not visible, gait analysis systems can still tell it is "you", based on the way you walk or your body language. The U.S. military, among others, have been working with satellite imaging to successfully identify key targets based on the shadow they cast on the ground [61].

But beyond biometrics, there is now a plethora of positioning technologies entering the market at different levels of precision [62], [63]. Even the mobile phone (whether 3G-enabled or not) has become a potential privacy-invasive tool. In the U.S., President Barrack Obama recently suggested that U.S. citizens have "no expectation of privacy" with respect to their mobile phones, even when not making a call [64]. Graafstra is not alone in his belief that the idea that anyone from local police to government agencies should be allowed to request- without a warrant- your phone's location at any time (even if it is sitting idle in your home) "is a very scary step that moves the U.S. further toward a surveillance state". The question as Graafstra has rightly put it is why are these issues not receiving the same attention as RFID tags and implantables? There is an obvious mismatch between *perceived* encroachments in privacy and *actual* encroachments in privacy. Advocacy groups might be lobbying for "no RFID implants" but what is here "now" is far worse.

10.1. Opting Out of Commercial ID Systems

If one wishes to opt out of an RFID-based system, users can issue requests to any third parties they enrolled with to have their account information destroyed. While this process and its full compliance is entirely in the hands of those third parties, destruction of the RFID tag is within the control of the users themselves. Tags can be returned to vendors, left at home, thrown out, physically destroyed, or in the case of implants physically removed from the body. However, removal of some RFID implants is more difficult than others. According to the company's product documentation, the FDA approved VeriChip is designed for permanent human implantation. Its Bio-Bond® anti-migration coating and the implantation procedure which seats the tag very deep into muscle tissue create a painful and expensive removal experience. The lack of anti-migration coating on the glass tags used by DIY taggers and their typically shallow implant locations allow easy removal that, in an emergency, could even be done with a sharp knife by the taggers themselves. With biometric systems however, the process of opting out is entirely handled by the third parties whose systems you have been enrolled in. Identifying all of these parties can be impossible if you have passively been enrolled in one or more systems without your knowledge. Furthermore, changing or destroying your biological identifiers can be extremely difficult, expensive, painful, or just plain impossible with today's technology.

11. Conclusion

There is some truth in the belief that technology can be used for well intentioned purposes and not-so-well intentioned purposes alike; see for example the differences between two opposing schools of thought-technological determinism and the social shaping of technology. Graafstra believes that most, if not all technologies are neutral: "[i]t is the people who implement and use a particular technology that determine its effect on humanity." In that regard, Graafstra is one of the first to acknowledge why some people might have a fear of the potential for wide-scale use of RFID implants, especially when claims are made by persons with limited knowledge of what the technology is capable of, or in

other circumstances persons who are completely ignorant of technological capabilities.

In reality, people who rise up so fervently to speak out against RFID do provide valuable feedback to the social innovation process. Graafstra knows too well that there will always be people who can and will build and/or use technology in a way that may be or become oppressive to end-users. The role of the critic is to help in the provision of a balanced view and to ask the very questions that may have been ignored during the development process. Perhaps, in the end, it is even quite irrelevant that some of these opponents understand the technology's true capabilities or limitations. The challenge rather to technologists is to usefully harness the criticism, the feedback, in order to build into their products and solutions design safeguards that mean that identified "potential" threats or harms are minimized or eradicated. Religious advocates against RFID, or those that have socio-political fears about the potential uses of RFID, should attempt to enter into intelligent dialogue rather than burn energy in campaigning against global computer giants or writing disrespectful messages to individual persons who are said to be aiding in the fulfillment of prophecy. The same can be said for law and policymakers, who must be open to discussion and who must arrive at intelligent legislation and industry regulation that targets behavior and the misconduct a technology might enable, not the technology itself. For example, some anti-chipping laws in the U.S. only refer to "injectable" RFID implants but we already have swallowable sensor technologies being patented, and what of the future of nanotechnology for healthcare? Policy that singles out technology as the problem, only limits the scope and effectiveness of the policy per se, while not addressing the real issues lurking beneath the surface.

12. References

[1] C. Grognard, *The Tattoo: graffiti for the soul*. Spain: The Promotional Reprint Company, 1994.

[2] K. MacKendrick, "Technoflesh, or "Didn't That Hurt?"" *Fashion Theory: The Journal of Dress, Body & Culture*, vol. 2, pp. 3-24, 1998.

[3] C. R. Sanders, *Customising the Body: the art and culture of tattooing*. Philadelphia: Temple University Press, 1989.

[4] A. Graafstra. (23 March 2005) One small step for hand: My first RFID implant, *Blog*. [Online]. Available: http://blog.amal.net/?p=8

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

[6] RFID Gazette. (19 September 2006) 10 People Or Groups Who Have Been Microchipped, *RFID Gazette*. [Online]. Available: http://www.rfidgazette.org/2006/09/10_people_or_gr.html

[7] K. Warwick. (2010) Professor Kevin Warwick, *University of Reading*. [Online]. Available: http://www.kevinwarwick.com/

[8] J. C. Havens. (1 June 2006) "Hear and Know" -- Scott Silverman and VeriChip -- (RFID) Security Under The Skin, *Association for Automatic Identification and Mobility*. [Online]. Available: http://www.aimglobal.org/members/news/templates/template.aspx?articleid=1279&zoneid=45

[9] W. D. Gardner. (15 July 2004) RFID Chips Implanted In Mexican Law-Enforcement Workers [Online]. Available: http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=23901004

[10] J. Halamka, A. Juels, A. Stubblefield, and J. Westhues, "The Security Implications of VeriChip Cloning," *The Journal of the American Medical Informatics Association*, vol. 13, pp. 601-607, 2006.

[11] T. Lewan. (22 July 2007) Chips: High tech aids or tracking tools?, [Online]. Available: http://www.usatoday.com/tech/products/2007-07-21-928096800_x.htm

[12] A. Leo. (2 May 2006) RFID Tags: Convenient Technology or Path to Government Monitoring? Users of RFID Technology Grapple With Concerns, [Online]. Available: http://abcnews.go.com/Technology/story?id=1913574&page=1

[13] J. Oxer. (2010) Blog, [Online]. Available: http://jon.oxer.com.au/

[14] M. Trainor. (2010) RFID Art, [Online]. Available: http://meghantrainor.com/index.html

[15] E. Kac. (11 November 1997) Time Capsule, [Online]. Available: http://www.ekac.org/figs.html

[16] A. Graafstra. (1 March 2007) Hands On: How radio-frequency identification and I got personal, *IEEE Spectrum*. [Online]. Available: http://spectrum.ieee.org/computing/hardware/hands-on

[17] R. Ip, K. Michael, and M. G. Michael, "Amal Graafstra The Do-It-Yourselfer RFID Implantee: The culture, values and ethics of hobbyist implantees," presented at Cultural Attitudes Towards Technology and Communication (CATAC08), Nimes, France, 2008.

[18] K. Michael and M. G. Michael, *Innovative Automatic Identification and Location Based Services: From Bar Codes to Chip Implants*. Hershey, PA: IGI Global, 2009.

[19] K. Heim. (1 March 2006) Man grips future with microchip implants in hands, *Seattle Times*. [Online]. Available: http://seattletimes.nwsource.com/html/localnews/2002835871_chipimplant01.html

[20] Sun Staff. (9 January 2006) Implants turn humans into cyborgs, *Vancouver Sun*. [Online]. Available: http://www.canada.com/vancouversun/news/story.html?id=d4f47afb-6ee3-460d-b4e3-834770fa886b&k=85038

[21] Reuters Staff. (6 January 2006) Computer chips get under skin of US enthusiasts, *ABC News Online*. [Online]. Available: http://www.abc.net.au/cgi-bin/common/printfriendly.pl?http://www.abc.net.au/news/newsitems/200601/s1542754.htm

[22] A. Bahney. (2 February 2006) High Tech Under the Skin, *New York Times*. [Online]. Available: http://query.nytimes.com/gst/fullpage.html?res=9F05E0DB1F3FF931A35751C0A9609C8B63&sec=&spon=&pagewanted=2

[23] G. J. Koprowski. (14 May 2010) Where's Jimmy? Just Google His Bar Code, *FOXNews.com*. [Online]. Available: http://www.foxnews.com/scitech/2010/05/14/radio-frequency-rfid-implant/

[24] A. Graafstra. (24 May 2007) Interview with Katina Michael... *Blog*. [Online]. Available: http://blog.amal.net/?p=36

[25] K. Michael and A. Graafstra, "Interview 14.2: The Do-It-Yourselfer RFID Implantee," in *Innovative Automatic Identification and Location Based Services: from Bar Codes to Chip Implants*, K. Michael and M. G. Michael, Eds. Hershey, PA: Information Science Reference, 2009, pp. 427-449.

[26] C. D. Martin, "The myth of the awesome thinking machine," *Communications of the ACM*, vol. 36, pp. 120-133, 1993.

[27] P. Atkinson and M. Hammersley, *Ethnography: principles in practice*. Abingdon, Oxon: Routledge, 1995.

[28] K. Michael and M. G. Michael, "Homo Electricus and the Continued Speciation of Humans," in *The Encyclopedia of Information Ethics and Security*, M. Quigley, Ed.: IGI Global, 2007, pp. 312-318.

[29] A. Graafstra. (16 March 2009) I take credit for that one…, *Blog*. [Online]. Available: http://blog.amal.net/?p=516

[30] M. Vascellari, E. Melchiotti, and F. Mutinelli, "Fibrosarcoma with Typical Features of Postinjection Sarcoma at Site of Microchip Implant in a Dog: Histologic and Immunohistochemical Study," *Veterinary Pathology*, vol. 43, pp. 545-548 2006.

[31] Wired. (2000) Cyborg 1.0, *Wired: Issue 8.02*. [Online]. Available: http://www.wired.com/wired/archive/8.02/warwick.html

[32] FDA. (10 December 2004) Guidance for Industry and FDA Staff (Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information), *U.S. Department of Health and Human Services Food and Drug Administration Center for Devices and Radiological Health General Hospital Devices Branch Division of Anesthesiology, General Hospital, Infection Control and Dental Devices Office of Device Evaluation*. [Online]. Available: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm072191.pdf

[33] FDA. (12 October 2004) K033440, *US Department of Health and Human Services*. [Online]. Available: http://www.accessdata.fda.gov/cdrh_docs/pdf3/K033440.pdf

[34] Google. (2010) Google Search "K033440", [Online]. Available: http://google2.fda.gov/search?q=K033440

[35] K. Albrecht. (19 November 2007) Microchip-Cancer Report, *AntiChips.com*. [Online]. Available: http://www.antichips.com/cancer

[36] A. Graafstra. (8 December 2009) Release form for RFID implantation, *Blog*. [Online]. Available: http://blog.amal.net/?p=2108

[37] DHS. (6 December 2006) The Use of RFID for Human Identity Verification (Report No.2006-02), *Department of Homeland Security, Data Privacy & Integrity Advisory Committee*. [Online]. Available: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

[38] DHS. (2006) The use of RFID for Human Identification. A draft report from DHS Emerging Applications and Technology subcommittee to the Full Data Privacy and Integrity Advisory Committee, Version 1.0, *Department of Homeland Security*. [Online]. Available: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf

[39] G. M. Køien. (February 2007) RFID and Privacy, *Telenor R&I (Network Technologies Group)*. [Online]. Available: http://www.telenor.com/en/resources/images/077-083_RFID-Privacy_tcm28-36799.pdf

[40] CBP.gov. (14 December 2009) Trusted Traveler Programs, *US Department of Homeland Security: U.S. Customs and Border Protection*. [Online]. Available: http://www.cbp.gov/xp/cgov/travel/trusted_traveler/

[41] S. Bono, M. Green, A. Stubblefield, A. Rubin, A. Juels, and M. Szydlo. (29 May 2007) Analysis of the Texas Instruments DST RFID, [Online]. Available: http://rfidtoys.net/downloads/rfidanalysis.org/rfidanalysis.pdf

[42] RFID News. (12 March 2003) Benetton to Tag 15 Million Items, *RFID Journal*. [Online]. Available: http://www.rfidjournal.com/article/view/344/1/1

[43] Focus. (2010) RFID blocking sleeves and holders, *Smart Card Focus*. [Online]. Available: http://www.smartcardfocus.com/shop/ilp/se~102/p/index.shtml?gclid=CLWixrPx36ECFQcupAodL1BuKA

[44] RFID. (7 February 2008) RFID Chip Market to Grow 63% Annually Through 2011, *RFID Update*. [Online]. Available: http://www.rfidupdate.com/articles/index.php?id=1538

[45] Destron. (2010) Welcome to LifeChip, *Destron LifeChip*. [Online]. Available: http://www.lifechip.com.au/index.php

[46] CCAC. (1998) Companion Animals Act 1998, *Compulsory microchipping in NSW*. [Online]. Available: http://www.dlg.nsw.gov.au/dlg/dlghome/dlg_InformationIndex.asp?areaindex=CA&index=311

[47] J. Sidén, A. Koptyug, M. Gulliksson, and H.-E. Nilsson, "An Action Activated and Self Powered Wireless Forest Fire Detector," in *Wireless Sensor and Actor Networks*. Boston: Springer, 3 December 2007, pp. 1571-5736.

[48] ID. (2010) Positive ID, [Online]. Available: http://positiveidcorp.com/about-us.html

[49] J. Diamond, *Guns, Germs and Steel: A Short History of Everybody for the Last 13,000 Years*. London: Vintage, 1997.

[50] Cliff. (3 May 2006) Social Consequences and Effects of RFID Implants? , *SlashDot*. [Online]. Available: http://ask.slashdot.org/article.pl?sid=06/05/04/0030212

[51] J. Scheeres. (2 June 2002) They Want Their ID Chips Now, *Wired*. [Online]. Available: http://www.wired.com/politics/security/news/2002/02/50187

[52] K. Michael, M. G. Michael, and R. Abbas, "The Dilemmas of Using Wearable Computing to Monitor People: An Extended Metaphor on the Tracking of Prison Inmates and Parolees," presented at Australia and New Zealand Society of Criminology Conference: Crime and Justice Challenges in the 21st Century, Perth, Western Australia, 2009.

[53] M. C. O'Connor. (22 August 2006) Tag Implants May Be Dangerous for Security Apps, Says Group, *RFID Journal*. [Online]. Available: http://www.rfidjournal.com/article/articleview/2607/2/1/

[54] A. Friggieri, K. Michael, and M. G. Michael, "The Legal Ramifications of Microchipping People in the United States of America- a State Legislative Comparison," presented at International Symposium on Technology and Society, Arizona, 2009.

[55] (12 October 2007) SB 362, Simitian. Identification devices: subcutaneous implanting, *Filed with Secretary of State*. [Online]. Available: http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0351-0400/sb_362_bill_20071012_chaptered.html

[56] K. Michael and M. G. Michael, "The social, cultural, religious and ethical implications of automatic identification," presented at Proceedings of the Seventh International Conference in Electronic Commerce Research, Dallas, Texas, 2004.

[57] M. G. Michael, "The Canonical Adventure of the Apocalypse of John: An Eastern Orthodox Perspective," in *Faculty of Theology and Philosophy*, vol. Doctor of Philosophy. Brisbane, Queensland: Australian Catholic University, 2002.

[58] G. Nikolettos. (2010) We the People Will Not Be Chipped, [Online]. Available:

http://www.wethepeoplewillnotbechipped.com/main/news.php

[59] D. Welch. (11 January 2010) US raises full body scanners in fly-by visit over terrorism, *Sydney Morning Herald*. [Online]. Available: http://www.smh.com.au/national/us-raises-full-body-scanners-in-flyby-visit-over-terrorism-20100110-m0u6.html

[60] A. Graafstra. (19 September 2009) I'm in "Tagged", a New Canadian Documentary, *Blog*. [Online]. Available: http://blog.amal.net/?p=1476

[61] A. Stoica, "Towards Recognition of Humans and their Behaviors from Space and Airborne Platforms: Extracting the Information in the Dynamics of Human Shadows," presented at ECSIS Symposium on Bio-inspired Learning and Intelligent Systems for Security, Edinburgh, Scotland, 2008.

[62] K. Michael and A. Masters, "Realised Applications of Positioning Technologies in Defense Intelligence," in *Applications of Information Systems to Homeland Security and Defense*, H. Abbass and D. Essam, Eds. Hershey, USA: Idea Group Publishing Press, 2006, pp. 167-195.

[63] K. Michael and A. Masters, "The Advancement of Positioning Technologies in Defense Intelligence," in *Applications of Information Systems to Homeland Security and Defense*, H. Abbass and D. Essam, Eds. Hershey, USA: Idea Group Publishing, 2006, pp. 196-220.

[64] D. McCullagh. (11 February 2010) Feds push for tracking cell phones, *cnet news*. [Online]. Available: http://news.cnet.com/8301-13578_3-10451518-38.html.