2006

Lend me your arms: the use and implications of humancentric RFID

Amelia Masters
University of Wollongong, am16@uow.edu.au

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

Publication Details

This article will be published as: Masters, A & Michael, K, Lend me your arms: the use and implications of humancentric RFID, Electronic Commerce Research and Applications, 2007, (in press). The journal can be found here.

Lend me your arms: the use and implications of humancentric RFID

Abstract

Recent developments in the area of RFID have seen the technology expand from its role in industrial and animal tagging applications, to being implantable in humans. With a gap in literature identified between current technological development and future humancentric possibility, little has been previously known about the nature of contemporary humancentric applications. By employing usability context analyses in control, convenience and care-related application areas, we begin to piece together a cohesive view of the current development state of humancentric RFID, as detached from predictive conjecture. This is supplemented by an understanding of the market-based, social and ethical concerns which plague the technology.

Keywords

Radio-frequency identification, transponders, chip implants, humancentric applications, usability context analysis, location tracking, personal privacy, data security, ethics

Disciplines

Physical Sciences and Mathematics

Publication Details

This article will be published as: Masters, A & Michael, K, Lend me your arms: the use and implications of humancentric RFID, Electronic Commerce Research and Applications, 2007, (in press). The journal can be found here.

Title:

Lend me your arms: the use and implications of humancentric RFID

Authors:
Amelia Masters (University of Wollongong), Katina Michael (University of Wollongong)

Abstract:

Recent developments in the area of RFID have seen the technology expand from its role in industrial and animal tagging applications, to being implantable in humans. With a gap in literature identified between current technological development and future humancentric possibility, little has been previously known about the nature of contemporary humancentric applications. By employing usability context analyses in control, convenience and care-related application areas, we begin to piece together a cohesive view of the current development state of humancentric RFID, as detached from predictive conjecture. This is supplemented by an understanding of the market-based, social and ethical concerns which plague the technology.

Keywords:
Radio-frequency identification; transponders; chip implants; humancentric applications; usability context analysis; location tracking; personal privacy; data security; ethics

Corresponding Author:
Dr Katina Michael

Contact Details:
School of Information Technology and Computer Science
University of Wollongong
Wollongong, NSW 2522 Australia

Telephone: 61242213937
Fax: 61242214170
Email: katina@uow.edu.au
Alternate Email: katina_michael@yahoo.com

Lend me your arms: the use and implications of humancentric RFID

Amelia Masters, Katina Michael

School of Information Technology and Computer Science, University of Wollongong, Australia

Abstract

Recent developments in the area of RFID have seen the technology expand from its role in industrial and animal tagging applications, to being implantable in humans. With a gap in literature identified between current technological development and future humancentric possibility, little has been previously known about the nature of contemporary humancentric applications. By employing usability context analyses in control, convenience and care-related application areas, we begin to piece together a cohesive view of the current development state of humancentric RFID, as detached from predictive conjecture. This is supplemented by an understanding of the market-based, social and ethical concerns which plague the technology.

Keywords: Radio-frequency identification; transponders; chip implants; humancentric applications; usability context analysis; location tracking; personal privacy; data security; ethics

1 Introduction

Over the past three decades, Radio Frequency IDentification (RFID) systems have evolved to become cornerstones of many complex applications. From first beginnings, RFID has been promoted as an innovation in convenience and monitoring efficiencies. Indeed, with RFID supporters predicting the growth of key medical services and security systems, manufacturers are representing the devices as ‘life-enhancing’. Though the lifestyle benefits have long been known, only recently have humans become both integral and interactive components in RFID systems. Where we once carried smart cards or embedded devices interwoven in clothing, RFID technology is now at a point where humans can safely be implanted with small transponders.

This paper aims to explore the current state of development for humancentric applications of RFID. The current state is defined by the intersection of existing development for the subjects and objects of RFID- namely humans and implants. The need for such a study has been identified by a gap in knowledge between present applications and future possibility. Currently there is little public data relating to the existing development state. Moreover, even those employed with contemporary RFID development have a future focus [1]. On the other hand, detractors of the technology are quick to imply repression and Armageddon [2]. This study aims to overcome forecast and provide a cohesive examination of existing humancentric RFID applications. Analysis of future possibility is outside the scope of this study. Instead, a discussion will be provided on present applications, their feasibility, use and social implications.

2 Literature Review

The literature review is organized into three main areas- control, convenience, and care. In each of these contexts, literature will be reviewed chronologically.

2.1 The Context of Control

A control-related humancentric application of RFID is any human use of an implanted RFID transponder that allows an implantee to have power over an aspect of their lives, or, that allows a third party to have power over an implantee. Substantial literature on humancentric control applications begins in 1997 with United States patent 5629678 for a 'Personal Tracking and Recovery System'. Though the literature scientifically describes the theoretical tracking system for recovery of RFID-implanted humans, no further evidence is available to ascertain whether it has since been developed. Questions as to feasibility of use are not necessarily answered by succeeding literature. Reports of the implantation of British soldiers [3] for example lack the evidentiary support needed to assuage doubts. Further, many articles highlight the technological obstacles, what Eng calls "chipping blocks", besieging humancentric RFID systems. These include GPS hardware miniaturization [4] and creating active RFID tags capable of being safely recharged from within the body. Further adding to reservation, much literature is speculative in nature. Eng [5], for example, predicts that tags will be melded into children to advise parents of their location, while Wakefield [6] predicts a future where microchipping for national security is common.

Despite concerns and conjecture, actual implementations of humancentric control applications of RFID have been identified. Both Murray [7] and Eng documented the implantation of Richard Seelig who had tags placed in his hip and arm in response to the September 11 tragedy of 2001. This sophisticated technology was employed to provide security and control over personal identification information. Similarly, Canadian artist Nancy Nisbet has implanted RFID microchips into her hands in order to question and apply control in personal environments [8]. Wilson [9] also provides the example of 11-year old Danielle Duval who has had an active chip (i.e. containing a rechargeable battery) implanted in her. Her mother believes that it is no different to tracking a stolen car, simply that it is being used for another more important application. Mrs Duval is considering implanting her younger daughter age 7 as well but will wait until the child is a bit older "so that she fully understands what's happening."

2.2 The Context of Convenience

A convenience-related humancentric application of RFID is any human use of an implanted RFID transponder that increases the ease with which tasks are performed. The first major documented experiment into the use of human-implantable RFID was within this context. Pulse [10], Sanchez-Klein [11] and Witt [1] all journalize on the self-implantation of Kevin Warwick, Director of Cybernetics at the University of Reading. They describe results of Warwick's research by his having doors open, lights switch on and computers respond to the presence of the microchip. Warwick himself gives a review of the research in his article ‘Cyborg 1.0’, however this report is informal and contains emotive descriptions of “fantastic” experiences [12].

Woolnaugh, [13] Holden, [14] and Vogel [15] all published accounts of the lead-up to Warwick’s second ‘Cyborg 2.0’ experiment and although Woolnaugh’s work involves the documentation of an interview, all three are narrative descriptions of proposed events rather than a critical analysis within definitive research frameworks. Similarly avoiding critical analysis are the future visions espoused by the authors; Vogel drawing links with science fiction. Though the commotion surrounding Warwick later died down, speculation did not with Eng proposing a future where credit card features will be available in implanted RFID devices. The result would see commercial transactions made more convenient.

2.3 The Context of Care

A care-related humancentric application of RFID is any human use of an implanted RFID transponder where function is associated with medicine, health or wellbeing. In initial literature, after the Cyborg 1.0 trial, Kevin Warwick envisioned that with RFID implants paraplegics would walk [1]. Building incrementally on this notion then is the work of Kobetic, Triolo and Uhlir who documented the study of a paraplegic male who had muscular stimuli delivered via an implanted RFID controlled electrical simulation system [16]. Though not allowing the mobility which Warwick dreamt of, results did include increased energy and fitness for the patient.

Outside the research sphere, much literature centers on eight volunteers who were implanted with commercial VeriChip RFID devices in 2002 trials. Murray [17], Black [18], Grossman [19], Streitfeld [20], and Gengler [21], all document medical reasons behind the implantation of four subjects. Supplemented by press releases however, all reports of the VeriChip trial were journalistic, rather than research-based, patterns of reporting. In contrast, non-trivial research is found in the work of Michael [22]. Her thesis uses a case study methodology, and a systems of innovation framework, to discuss the adaptation of auto-ID for medical implants.

2.4 Critical Response to Literature

More recent publications on humancentric RFID include the works of Masters [23], Michael and Michael [24], Perusco and Michael [25], Johnston [26], and Perakslis and Wolk [27]. Masters approaches the subject from the perspective of usability contexts, while Perusco and Michael use document analysis to categorise location services into tag, track and trace applications. Johnston uses content analysis to identify important themes in the literature, supplemented by a small-scale sample survey on the social acceptance of chip implants. Perakslis and Wolk also follow this latter methodology. Of the other (earlier) landmark studies, the majority are concerned with non-humancentric applications. Gerdeman [28], Finkinzeller [29] and Geers [30] all use case studies to investigate non-humancentric RFID and hence our methodological precedent is set here. Of the remaining literature, the bulk is newstype in nature and the absence of research frameworks is evident. There are few exceptions to this, but they include Woolnaugh [13] who conducted an interview and Murray [17] and Eng [5] who provide small case studies. In further criticism the news articles do not demonstrate technological trajectories. Instead, many describe current events, and then speculate on potential future developments rather than possible current applications. What is more, these future developments are often utopian implementations and are not likely to be achieved by incremental development in the short to medium-term. Any real value in these news articles thus lies in the documentation of events.

3 Methodology

The primary question, 'what is the current state of application development in the field of humancentric RFID devices?' is justifiably exploratory. It entails investigation into contemporary technology usage and seeks to clarify boundaries within the research area. As such, this is a largely qualitative study that uses some elements of descriptive research to enhance the central usability context analyses. These analyses are similar to case studies as they investigate "a contemporary phenomenon within its real life context when the boundaries between phenomenon and context are not clearly evident" [31]. They also similarly use multiple sources of evidence, however are differentiated on the basis of the unit of analysis. In a usability context analysis methodology, units are not individuals, groups or organizations but are applications or application areas for a product, where 'product' is defined as "any interactive system or device designed to support the performance of users' tasks" [32]. The results of multiple analyses are more convincing than a singular study, and the broad themes identified cover the major fields of current humancentric RFID development. Further, the usability context analyses in this study are supplemented by a discussion of surrounding social, legal and ethical ambiguities. By this means, the addition of a narrative analysis to the methodology ensures a thorough investigation of usage and context.

4 Control

The usability context analysis for control is divided into three main sub-contexts-security, management, and social controls (Table 1).

4.1 Security Controls

The most basic security application involves controlling personal identification through identifying data stored on a transponder. In theory, the limit to the amount of information stored is subject only to the capacity of the embedded device or associated database. Further, being secured within the body, the loss of the identifier is near impossible even though, as has occurred in herd animals, there are some concerns over possible dislodgement. Accordingly, the main usability drawback lies with reading the information. Implanted identification is useless if it is inaccessible.

A primary commercial security application involves GPS tracking to pinpoint the location of an implantee [33]. Control here exists in both the ability to find and to be found. Suitable GPS components are currently manufactured and sold as stand-alone, wearable products by companies including Wherify Wireless [34]. Variants are available which send alerts to a nominated care-giver if a user wanders outside pre-defined boundaries or falls and remains immobile for an extended time. When combined with implanted RFID a superior level of identification is added to the application. This is especially valuable in allowing positive identification where the implantee is impaired or uncommunicative. In Japan students are being tagged in a bid to keep them safe. RFID transponders are being placed inside their backpacks and are used to advise parents when their child has arrived at school [35]. A similar practice is being conducted in the U.S state of California where children are being asked to "wear" RFID tags around their necks when on school grounds [36].

Numerous applications have also been developed to assist individuals who depend solely on carers for support. This group consists of newly-born babies, sufferers of mental illness and Alzheimer's disease, persons with disabilities and the elderly. With regard to mass market applications, one proposed use involves taking existing infant protection systems at birthing centres and internalizing the RFID devices worn by newborns. This would aid in identifying those who cannot identify themselves. Similarly, when connected to access sensors and alarms, the technology can alert staff to the "unauthorized removal of children" [37]. The South Tyneside Healthcare Trust Trial in the U.K. is a typical external-use example case. Early in 1995, Eagle Tracer installed an electronic tagging system at the hospital using TIRIS electronic tags and readers from Texas Instruments. Detection aerials were hidden at exit points so that if any baby was taken away without authorisation, its identity would be known and an alarm raised immediately. The alarm could potentially lock doors, alert the maternity ward staff and send security guards to the scene. Automatic-ID News [38] reported: "The TIRIS tags…

are securely attached to even the smallest newborn babies without causing harm or discomfort. The carrier material has been developed in such a way as to prevent the removal by anyone other than a specialist...” The trial was so successful that the hospital was considering expanding the system to include the children’s ward. The clinical director of obstetrics and gynaecology told Automatic-ID News that, “[t]he system ha[d] been very enthusiastically received by the midwives as well as the mums.”

Commentators like Martin Swerdlow, a U.K. member of the government Foresight Science and Technology Group, are using this lack of objection to external electronic tagging for newborns to highlight the idea that a national identity system based on implants is not impossible. Some believe that there will come a time when it will be common for different groups in the population to have tags implanted at birth. In Britain, chip implantation was suggested for illegal immigrants, asylum seekers and even travelers. Smet [39] argued the following, “[i]f you look to our societies, we are already registered from birth until death. Our governments know who we are and what we are. But one of the basic problems is the numbers of people in the world who are not registered, who do not have a set identity, and when people move with real or fake passports, you cannot identify them.”

This is not a new forecast however. Hewkin [40] was one of the first official accounts (in an IEEE publication) to predict that ‘subminiature read-only tags’ would be injected under human skin using a syringe to reduce problems such as fraud. This was likely in response to Dr Daniel Man’s October 1987 patent regarding a homing device implant. Called ‘Man’s Implanted’, it was the first device of its kind designed for humans. Mechanic [41] reported: “…[t]he human device runs on long-lasting lithium batteries and periodically transmits a signal that would allow authorities to pinpoint a person's exact location... the batteries... could be replenished twice a year..." Man's invention has not been marketed because the U.S. Food and Drug Administration (FDA) are yet to approve the device. For this Man will require a substantial amount of cash for miniaturisation and regulatory approval [42]. Man himself has been very vocal in his belief that the device should be used for voluntary purposes only and he is aware that many oppose the technology for cultural, philosophical and religious reasons.

4.2 Management Controls

Many smart card access systems use RFID technology to associate a cardholder with access permissions to particular locations. Replacing cards with RFID implants alters the form of the 'key' but does not require great changes to verification systems. This is because information stored on a RFID microchip in a smart-card can be stored on an implanted transponder. Readers can similarly be triggered when the transponder is nearby. This application would have greatest value in 'mission critical' workplaces or for persons whose role hinges upon access to a particular location. The implanted access pass has the added benefit of being permanently attached to its owner.

Access provision translates easily into employee monitoring. In making the implanted RFID transponder the access pass to certain locations or resources, times of access can be recorded to ensure that the right people are in the right place at the right time. Control in this instance then moves away from ideals of permission and embraces the notion of supervision. A company's security policy may stipulate that staff badges be secured onto clothing or that employees must wear tags woven into their uniforms. Some employers require their staff to wear RFID tags in a visible location for both identification purposes and access control [43]. In this regard, Olivetti's "active badge" was ahead of its time when it was first launched [44]. The tag is able to "localise each staff member as he or she moves through the premises... It is possible to automatically re-route telephone calls to the extension nearest an individual" [45].

4.3 Social Controls

In the military, transponders may serve as an alternative to dog tags. Using RFID, in addition to the standard name, rank and serial number, information ranging from allergies and dietary needs to shoe size can be stored. This purports to ease local administrative burdens, and can eliminate the need to carry identification documents in the field allowing for accurate, immediate identification of Prisoners-Of-War (POWs).

Just as humancentric applications of RFID exist for those who enforce law, so too do applications exist for people who have broken it. The concept of 'electronic jails' for low-risk offenders is starting to be considered more seriously. In most cases, parolees wear wireless wrist or ankle bracelets and carry small boxes containing the vital tracking technology. Sweden and Australia have implemented this concept and there are trials taking place in the U.K., U.S., Netherlands and Canada. In 2002, 27 American states had tested or were using some form of satellite surveillance to monitor parolees [18]. In 2005 there were an estimated 120000 tracked parolees in the United States alone [46]. Whilst tagging low-risk offenders is not popular in many countries it is far more economical than the conventional jail. Since 1994 in Sweden: “...certain offenders in six districts have opted out of serving time, choosing instead to be tagged by an electronic anklet and follow a strict timetable set by the probation service... about 700 people have taken part in the Swedish scheme, open to people sentenced to two months or less” [47]. Social benefits are also present as there is a level of certainty involved in identifying and monitoring so-called ‘threats’ to society. In a more sinister scenario in South America, chip implants are a way “to identify kidnapping victims who are drugged, unconscious or dead. In that market, the chip is being bundled with the… GPS device, Digital Angel, so police are able to track the… victim's location” [48].

5 Convenience

The usability context analysis for convenience is divided into three main sub-contexts- assistance, financial services and interactivity (Table 2).

5.1 Assistance

Automation is the repeated control of a process through technological means. Implied in the process is a relationship, the most common of which involves linking an implantee with appropriate data. Such information in convenience contexts can however be extended to encompass goods or physical objects with which the implantee has an association of ownership or bailment. VeriChip for example, a manufacturer of human-implantable RFID transponders, have developed VeriTag for use in travel. This device allows “personnel to link a VeriChip subscriber to his or her luggage… flight manifest logs and airline or law enforcement software databases” [49]. Convenience is provided for the implantee who receives greater assurance that they and their luggage will arrive at the correct destination, and also for the transport operator who is able to streamline processes using better identification and sorting measures.

Advancing the notion of timing, a period of movement leads to applications that can locate an implantee or find an entity relative to them [50]. This includes “find me”, “find a friend” or “where am I”, “where is the nearest” or “guide me to” solutions. Integrating RFID and GPS technologies with a geographic information systems (GIS) portal such as the Internet-based mapquest.com would allow users to find destinations based on their current GPS location. The nature of the application also lends itself toward roadside assistance or emergency services, where the atypical circumstances surrounding the service may mean that other forms of subscriber identification are inaccessible or unavailable.

5.2 Financial Services

Over the last few decades, world economies have come to acknowledge the rise of the cashless society. In recent years however, alongside traditional contact cards, we have seen the emergence of alternate payment processes- RFID being one of these. In 2001, Nokia tested the use of RFID in its 5100-series phone covers, allowing the mobile device to be used as a bank facility. RFID readers were placed at McDonalds drive-through restaurants in New York and the consumer was able to pay their bill by holding their mobile phone near a reader. The reader contacted a wireless banking network and payment was deducted from a credit or debit account. Of the trial, Wired News noted the convenience stating, “there is no dialing, no ATM, no fumbling for a wallet or dropped coins” [51]. These benefits would similarly exist with implanted RFID. Ramo has noted the feasibility, commenting that “in the not too distant future” money could be stored anywhere, as well as “on a chip implant under [the] skin” [52]. Forgetting your wallet would no longer be an issue.

It is also feasible that humancentric RFID eliminates the need to stand in line at a bank. Purely as a means of identification, the unique serial or database access key stored on the RFID transponder can be used to prove identity when opening an account or making a transaction. The need to gather paper-based identification is removed and, conveniently, the same identification used to open the account is instantly available if ever questioned. This has similar benefits for Automatic Teller Machines (ATM’s). When such intermediary transaction devices are fitted with RFID readers, RFID transponders have the ability to replace debit and credit cards. Warwick [53] predicted that implanted chips “could be used for money transfers, medical records, passports, driving licenses, and loyalty cards. And if they are implanted they are impossible to steal.”

5.3 Interactivity

On August 24, 1998 Professor Kevin Warwick became the first recorded human to be implanted with an RFID device. Using the transponder, Warwick was able to interact with the ‘intelligent’ building that he worked in. Over the nine days he spent implanted, doors formerly requiring smart card access automatically opened. Lights activated when Warwick entered a room and upon sensing the Professor’s presence his computer greeted him. Warwick’s ‘Project Cyborg 1.0’ experiment thus showed enormous promise for humancentric convenience applications of RFID. The concept of such stand-alone applications expands easily into the development of Personal Area Networks (PANs) and the interactive home or office. With systems available to manage door, light and personal computer preferences based on transponder identification, further climate and environmental changes are similarly exploitable (especially considering non-humancentric versions of these applications - activated by wearable RFID - already exist) [54].

Given the success of interacting with inanimate locations and objects, the next step is to consider whether person-to-person communication can be achieved using humancentric RFID. Such communication would conveniently eliminate the need for intermediary devices like telephones or post. Answering this question was an aim of ‘Project Cyborg 2.0’ with Warwick writing, “We'd like to send movement and emotion signals from one person to the other, possibly via the Internet” [55]. Warwick’s wife Irena was the second trial subject, being similarly fitted with an implant in her median nerve. Communicating via computer-mediated signals was only met with limited success however. When Irena clenched her fist for example, Professor Warwick received a shot of current through his left index finger [56]. Movement sensations were therefore effectively, though primitively, transmitted. Broadcasting emotion and thought is a much harder task and, despite research at British Telecom into mind-implantable ‘Soul Catcher’ chips, given the results of Cyborg 2.0 such communicative technology is not feasible in the current state of development [57].

6 Care

The usability context analysis for care is divided into three main sub-contexts- medical, biomedical and therapeutic (Table 3).

6.1 Medical

As implanted transponders contain identifying information, the storage of medical records is an obvious, and perhaps fundamental, humancentric care application of RFID. Similar to other identification purposes, a primary benefit involves the RFID transponder imparting critical information when the human host is otherwise incapable of communicating. In this way, the application is "not much different in principle from devices… such as medic-alert bracelets" [21]. American corporation VeriChip markets their implantable RFID device for this purpose. Approved for distribution throughout the United States in April of 2002, it has been subject to regulation as a medical device by the Food and Drug Administration since October of the same year.

Care-related humancentric RFID devices provide unparalleled portability for medical records. Full benefit cannot be gained without proper infrastructure however. Though having medical data instantly accessible through implanted RFID lends itself to saving lives in an emergency, this cannot be achieved if reader equipment is unavailable. The problem is amplified in the early days of application rollout, as the cost of readers may not be justified until the technology is considered mainstream. Also, as most readers only work with their respective proprietary transponders, questions regarding market monopolies and support for brand names arise.

6.2 Biomedical

A biosensor is a device which “detects, records, and transmits information regarding a physiological change or the presence of various chemical or biological materials in the environment” [58]. It combines biological and electronic components to produce quantitative measurements of biological parameters, or qualitative alerts for biological change. Thermal, electrochemical, mass and optical measures are most commonly monitored. When integrated with humancentric RFID, biosensors can transmit source information as well as biological data. The time savings in simultaneously gathering two distinct data sets are thus an obvious benefit. Further, combined reading of the biological source and measurement is less likely to encounter the human error linked with manually correlating data to data sources.

Implantable transponders allowing for the measurement of body temperature have been used to monitor livestock for over a decade [30]. As such, the data procurement benefits are well known. It does however give a revolutionary new facet to human care by allowing internal temperature readings to be gained, post-implantation, through non-invasive means. In 1994 Bertrand Cambou, director of technology for Motorola’s Semiconductor Products in Phoenix, predicted that by 2004 all persons would have a microchip implanted in their body to monitor and perhaps even control blood pressure, their heart rate, and cholesterol levels. Harrison [59] reported that: “Cambou has been a part of the miniaturization of microprocessors and the development of wireless communication technologies. Both would have central roles in putting computers inside the human body.” When questioned by Harrison about the effects the technology would have in the body Cambou responded: “[w]e are not aware of any current obstacles to the encapsulation and implanting of electronic devices within the body, and the transmission characteristics [of radio frequencies] through the body are well known.” The applications for this type are wide and include: chemotherapy treatment management; chronic infection or critical care monitoring; organ transplantation treatment management; infertility management; post-operative or medication monitoring; and response to treatment evaluation. Multiple sensors placed on an individual could even form a Body Area Network (BAN).

An implantable RFID device for use by diabetes sufferers has been prototyped by biotechnology firm M-Biotech. The small glucose bio-transponder, consisting of a miniature pressure sensor and a glucose-sensitive hydrogel swells “reversibly and to varying degrees” when changes occur in the glucose concentrations of surrounding fluids [60]. Implanted in the abdominal region, a wireless alarm unit carried by the patient continually reads the data, monitoring critical glucose levels.

6.3 Therapeutic

Implanted therapeutic devices are not new; they have been used in humans for many years. Alongside the use of artificial joints for example, radical devices such as pacemakers have become commonplace. The use of RFID with these devices however, has re-introduced some novelty to the remedial solution [61]. This is because, while the therapeutic devices remain static in the body, the integration of RFID allows for interactive status readings and monitoring, through identification, of the device.

There are very few proven applications of humancentric RFID in the treatment usability sub-context at current if one puts cochlear implants [62] and smart pills aside [63]. Further, of those applications at the proof of concept stage, benefits to the user are generally gained via an improvement to the quality of living, and not a cure for disease or disability. With applications to restore sight to the blind [64] and re-establish normal bladder function for patients with spinal injuries already in prototyped form however, some propose that real innovative benefit is only a matter of time [65]. Arguably the technology for the applications already exists [66]. All that needs to be prototyped is a correct implementation. Thus, feasibility is perhaps a matter of technological achievement and not technological advancement.

7 Findings

The choice of control, convenience and care contexts for analysis stemmed from the emergence of separate themes in the literature review; however the context analyses themselves showed much congruence between application areas. In all contexts, identification and monitoring are core functions. For control, this functionality exists in security and in management of access to locations and resources. For convenience, identification necessarily provides assistance and monitoring supports interactivity with areas and objects. Care, as the third context, requires identification for medical purposes and highlights biological monitoring as basic functionality.

With standard identification and monitoring systems as a basis, it is logical that so many humancentric applications of RFID have a mass target market. Medical identification for example is not solely for the infirm because, as humans, we are all susceptible to illness. Similarly, security and convenience are generic wants. Combined with similarities between contextual innovations, mass-market appeal can lead to convergence of applications. One potential combination is in the area of transportation and driver welfare. Here the transponder of an implanted driver could be used for keyless passive entry (convenience), monitoring of health (care), location based services (convenience), roadside assistance (convenience) and, in terms of fleet management or commercial transportation, driver monitoring (control).

Despite parallels and a potential for convergence, development contexts for humancentric RFID are not equal. Instead, control is dominant (Figure 1). Though care can be a cause for control and medical applications are convenient, it is control which filters through other contexts as a central tenet. In convenience applications, control is in the power of automation and mass management, in the authority over environments and devices. For care applications, medical identification is a derivative of identification for security purposes and the use of biosensors or therapeutic devices extends control over well-being. Accordingly, control is the overriding theme encompassing all contexts of humancentric RFID in the current state of development [67].

Alongside the contextual themes encapsulating the usability contexts are the corresponding benefits and costs in each area (Table 4). When taking a narrow view and analyzing a sub-context, it is clear that many benefits of humancentric RFID are application specific. Therapeutic implants for example, have the benefit of the remedy itself. Conversely however, a general concern of applications is that they are largely given to social disadvantages including the onset of religious objections and privacy fears.

7.1 Application Quality and Support for Service

For humancentric RFID, application quality depends on commercial readiness. For those applications being researched, the usability context analyses suggest that the technology, and not the applications, present the largest hurdle. In his Cyborg 1.0 experiments for example, Professor Kevin Warwick kept his transponder implanted for only nine days, as a direct blow would have shattered the glass casing, irreparably damaging nerves and tissue. Similarly, research into location based services faces technological hurdles as combining GPS with humancentric RFID involves challenges of radiation shielding, miniaturization and power supply.

Once technological difficulties are overcome and applications move from proof of concept into commercialization, market-based concerns are more relevant. Quality of data is a key issue. In VeriChip applications, users control personal information that is accessible, though stored in the Global VeriChip Subscriber Registry database, through their implanted transponder. The system does not appear to account for data correlation however, and there is a risk of human error in information provision and in data entry. Thus, who pays for errors? Who maintains liability? Such questions indicate the need for industry standards, allowing a quality framework for humancentric RFID applications to be created and managed.

Industry standards are also relevant to support services. In humancentric applications of RFID they are especially needed as much usability, adjunct to the implanted transponder, centers upon peripherals and their interoperability. Most proprietary RFID readers for instance, can only read data from similarly proprietary transponders. In medical applications though, where failure to harness available technology can have dramatic results, an implantee with a non-compatible, and therefore unreadable, transponder is no better off for using the application. Accordingly, for humancentric RFID to realize its promotion as ‘life-enhancing’, standards for compatibility between differently branded devices must be developed.

Lastly, the site of implantation should be standardized as even if an implanted transponder is known to exist, difficulties may arise in discerning its location. Indeed, of those widely reported incidences of implantation, the Jacobs family has transponders in their right arms, while Kevin Warwick opted for his left. Richard Seelig has transponders in his arm and hip, while British soldiers in unconfirmed trials allegedly carried transponders in their necks. Without a common site for implantation, and where scanning an implanted transponder requires a reading distance of no more than a few centimeters, finding an implanted RFID device can be tedious. This is disadvantageous for medical, location-based or other critical implementations where time is a decisive factor in the success of the application. It is also a disadvantage in more general terms as the lack of standards suggests that though technological capability is available, there is no social framework ready to accept it.

7.2 Commercial Viability for the Consumer

A humancentric application of RFID must satisfy a valid need to be considered marketable. This is especially crucial as the source of the application, the transponder, requires an invasive installation and, afterwards, cannot be easily removed. Add to this that humancentric RFID is a relatively new offering with few known long-term effects, and participation is likely to be a highly considered decision. Thus, despite many applications having a mass target market, the value of the application to the individual will determine boundaries and commercial viability.

Value is not necessarily cost-based. Indeed, with the VeriChip sold at a cost of $US200 plus a $10 per month information storage fee, it is not being marketed as a toy for the elite. Instead, value and application scope are assessed in terms of life enhancement. Therapeutic devices for example, provide obvious remedial benefit; but the viability of a financial identification system may be limited by available infrastructure. Similarly, is implanting for precaution against kidnapping or terrorism really worthwhile if it simply serves as a means of identification after death?

Arguably, commercial viability is increased by the ability of one transponder to support multiple applications. Identification applications for example, are available in control, convenience and care usability contexts. Likewise, one humancentric RFID-GPS system can support many location-based services. The question arises however, as to what occurs when different manufacturers market largely different applications? Where no real interoperability exists for humancentric RFID devices, it is likely that users must be implanted with multiple transponders from multiple providers. Further given the power and processing constraint of multi-application transponders in the current state of development, the lack of transponder portability reflects negatively on commercial viability and suggests that each application change or upgrade may require further implantation and bodily invasion.

7.3 Commercial Viability for the Manufacturer

Taking VeriChip as a case study, one is led to believe that there is a commercially viable market for humancentric applications of RFID. Indeed, where the branded transponder is being sold in North and South America, and has been showcased in Europe [68], a global want for the technology is suggested. It must be recognized however, that in the current state of development VeriChip and its parent, Applied Digital Solutions, have a monopoly over those humancentric RFID devices approved for use. As such, their statistics and market growth have not been affected by competition and there is no comparative data. The difference between a successful public relations campaign and reality is therefore hard to discern.

Interestingly, in non-humancentric commercial markets, mass rollouts of RFID have been scaled back. Problems have arisen specifically in animal applications. The original implementation of the 1996 standards, ISO 11784: ‘Radio-frequency identification of animals- Code structure’ and ISO 11785: ‘Radio-frequency identification of animals-

Technical concept' for example, were the subject of extensive complaint [69]. Not only did the standards not call for unique identification codes, they violated the patent policy of the International Standards Organization. Also, owing to "the existence of three conflicting patents affecting ISO 11785", the standards infringed antitrust law in several countries. Even after the ISO standards were returned to the SC19 Working Group 3 for review, a general lack of acceptance equated to limited success. Moreover, in recent times, moves have been made to ban the use of implantable transponders in herd animals. In a high percentage of cases the transponder moved in the fat layer, raising concerns that it might be later consumed by humans. Further, the meat quality was degraded as animals sensing the existence of an implanted foreign object produced antibodies to 'attack' it [23].

Where humancentric applications of RFID have been influenced by and built upon non-humancentric applications, the cessation of non-humancentric trials and the reduction in herd animal implantation is not a positive sign for the humancentric industry. It instead shows the niche functionality of the technology and suggests that gaining long-term commercial viability will be fraught with problems.

8 Discussion

A natural corollary to humancentric applications of RFID is the great range of social, legal and ethical issues [24] which besiege the technology. Some space will now be given to considering the major issues surrounding the implantation of transponders into humans. These issues are broken down into three areas: personal privacy, data security, and ethical considerations.

8.1 Personal Privacy

Given its contactless nature and non-line-of-sight (nLoS) capability, RFID has the ability to automatically collect a great deal of data about an individual in a covert and unobtrusive way. Hypothetically, a transponder implanted within a human can communicate with any number of readers it may pass in any given day. In addition to the implant, Electronic Product Code (EPC) item-level tagging will mean that apparel or peripheral items carried by an individual may also be available for data collection. This opens up a plethora of possibilities, including the ability to link data based on a unique identifier (i.e. the chip implant), to locate and track an individual over time, and to look at individual patterns of behaviour whether they be transaction-oriented or based on communities-of-interest (CoI). The severity of violations to personal privacy increase as data collected for one purpose is linked with completely separate datasets gathered for another purpose. For instance, consider matching the number and type of transactions carried out by an individual, with related location and recipient information, and one finds themselves conducting a type of social network analysis [70] synonymous with criminal investigations [71].

At a more basic level, consider the use of an implant that deducts programmed payment for road tolls as you drive through sensor-based stations. Imagine this same data originally gathered for traffic management now being used to detect speeding and traffic infringements, resulting in the automatic issue of a fine. Real cases with respect to GPS and fleet management have already been documented. Kumagi and Cherry [72] describe how one family was billed an “out-of-state penalty” by their rental company based on GPS data that was gathered for a completely different reason. Stanford [73] menacingly calls this a type of data use “scope creep” while Papasliotis [74] more pleasantly deems it “knowledge discovery”. Whether this cross-correlation is a positive or negative use of data can depend on one’s immediate perspective, however, at a banal level, consider the following questions posed by Juels et al. [75] regarding the actual collection of information: “[w]hat woman wants her dress size to be publicly readable by any nearby scanner? Who wants the medications and other contents of a purse to be scannable? Who wants the amount of money in a wallet to be easily determinable by a scanner? Who wants his or her location to be tracked and recorded based on the unique ID number in shoes or other clothing?”

These notions of ‘every-day’ information gathering, where an implantee must submit to information gathering practices in return for access to services, offends the absolutist view of privacy and “an individual [having] the right to control the use of his information in all circumstances.” [75] Indeed, given they are implanted beneath the skin, the very nature of humancentric transponders negates the individual’s ability to ‘control’ the device and what flows from it. Not only do the majority of consumers lack the technical ability to either embed or remove implants but they naturally lack the ability to know when their device is emitting data and when it is not. There is also a limited understanding of what information ‘systems’ are actually gathering in terms of details. For service providers like VeriChip who may be looking to establish a presence in

Europe, intellectual property directives may hamper their promise to consumers to keep their data private. According to Papasliotis [74] "…the proposed EU Intellectual Property (IP) Enforcement Directive includes a measure that would make it illegal for European citizens to de-activate the chips in RFID tags, on the ground that the owner of the tag has an intellectual property right in the chip. De-activating the tag could arguably be treated as an infringement of that right." In addition, laws in different jurisdictions provide little restraint on the data mining of commercial databases by commercial entities. In this instance, there would be little to stop RFID service providers from mining data collected from their subscribers and on-selling it to other organisations.

8.2 Data Security

Relevant approaches to RFID tag or transponder security in relation to inanimate objects have been discussed in the literature. Gao [76] summarises these methods as "killing tags at the checkout, applying a rewritable memory, physical tag memory separation, hash encryption, random access hash, and hash chains." Transponders that are embedded within the body pose a different type of data security requirement though. They are not in the body so they can be 'killed' or turned off, this being a circumvention of the original purpose of implantation. Instead, they are required to provide a persistent and unique identifier. In the U.S. however, also thwarting an original purpose, a study has shown that some RFID transponders are capable of being cloned, meaning the possibility of payment fraud or other forms of theft may still exist [77]. One possibility, as proposed by Perakslis and Wolk [27], is the added security of saving an individual's feature vector onboard the RFID chip. This assumes the use of an active transponder which has the additional storage capacity and functionality to execute dynamic commands. Biometrics too, however, is fraught with its own legal problems [78]. Despite some moves in criminal justice systems, it is still controversial to say that one's fingerprint or facial image should be held on a public or private database.

Regardless of how security is applied, the threats to data can be categorized as follows: corporate espionage threat, competitive marketing threat, infrastructure threat, and trust perimeter threat [77]. The main risk for consumers though, seems to underpin the concern that third parties might potentially gain access to data about them and their movements without prior notice. To this end, gaining and maintaining the trust of consumers is essential to the success of the technology. Mature trust models need to be architected and implemented, but more importantly they need to be understood outside of an academic context. Though it is important that trust continues to grow as an area of study within the e-commerce arena, it will be the practical operation of companies like VeriSign in these early days of global information gathering which will allow consumers to create their own standards and opinions.

Stemming from the significance of trust, service providers now have great power and great responsibility in deciding who will be granted access to the systems that house personal information and with what intent the information will be used at any given point [25]. The main temptation will be in the value of the data and how it can be used not only to sell value-added services but separate service-sets that rely on location information. Unfortunately, researchers like Stanford believe that it is a "virtual certainty" that the tags and their respective systems "will be abused" [73]. Even more unfortunate, data security in embedded systems does not stop with access-based issues. To consider an extreme, we can envisage the potential for underground implant rackets that specialize in the kidnapping of individuals to steal transponders or the development of cloning technology which allows for the duplication of existing implants. If this cyber crime results, and an individual is implanted with multiple transponders, which implant would be considered the true implant? In short, one would be able to falsify their location by impersonation. Considering more immediate feasible concerns, this leads to the question of where the implant will most likely be located in the human body? For now live services place the implant in the left or right arm but the problems with designating such a zone surround the possibility of exclusion. For example, what if the consumer is an amputee or has prosthetic limbs? What if other medical devices like a cochlear implant or heart pacemaker are already implanted? Surely the limited space of the human body means that certain things are possible, while others are not. Thus, recognizing the limitations of the human body, will service providers brand transponders and allow multifunctional tags for different niche services? Which party then owns the transponder? The largest service provider, the government acting as an issuer, or the individual? Who is liable for errors in location precision, abuse and misuse of information provided by the subscriber and gathered by the service provider? And more importantly, who is liable for break-downs in communication when services are unavailable or unmanageable and disastrous incidents result?

8.3 Ethical Considerations

Molnar and Wagner [79] ask the definitive question “[i]s the cost of privacy and security “worth it”?” Stajano [80] answers by reminding us that, “[t]he benefits for consumers remain largely hypothetical, while the privacy-invading threats are real.” Indeed, when we add to privacy concerns the unknown health impacts, the potential changes to cultural and social interaction, the circumvention of religious and philosophical ideals, and a potential mandatory deployment, then the disadvantages of the technology seem almost burdensome. For the present, proponents of emerging humancentric RFID rebuke any negatives “under the aegis of personal and national security, enhanced working standards, reduced medical risks, protection of personal assets, and overall ease-of-living.” [27] Unless there are stringent ethical safeguards however, there is a potential for enhanced national security to come at the cost of freedom, or for enhanced working standards to devalue the importance of employee satisfaction. For example, does the state have the right to order citizens to be implanted for national identification? Do employers have the right to dismiss an employee who has not accepted to be tagged for access control purposes? [81] Can overprotective parents impose implants on their teenage children or a husband on his wife? [82] Do medical personnel have the right to remotely stimulate an individual’s nerves for therapeutic reasons? The innovative nature of the technology should not be cause to excuse it from the same “judicial or procedural constraints which limit the extent to which traditional surveillance technologies are permitted to infringe privacy” [74]. This need for monitoring is not limited purely to humancentric applications of RFID. As Stajano [80] highlights, even if tags are only affixed to objects rather than to people, one need only consider the results of correlating the RFID serial numbers in your eyeglasses, your watch and your home keys before the capabilities of data-mining become obtrusive.

Garfinkel et al. [77] provide a thorough discussion on the key privacy, security, and ethical considerations in their paper. Though their main focus is on users of RFID systems and purchasers of products containing RFID tags, the conclusions drawn are also relevant to the greater sphere of humancentric RFID. Firstly, Garfinkel et al. begin by stipulating that a user has the right to know if the product they have purchased contains an RFID tag. In the current climate of human transponder implant acceptance, it is safe to assume that an individual who has requested implantation knows of their implant and its location. But, does the guardian of an Alzheimer's patient or adult schizophrenic, have the right to impose an implant on behalf of the sufferer for monitoring or medical purposes [83]?

Secondly, the user has the right to have embedded RFID tags "removed, deactivated, or destroyed" [77] when a product is purchased. Applied to the human transponder implant scenario, this second point poses a number of difficulties. While the user has every freedom to request that an implant be removed, deactivated or destroyed, they cannot remove the implant themselves without some harm to their body, they have no real way of finding out whether a remaining implant has in fact been 'deactivated', and destroying an implant without its removal from the human body implies some form of amputation. Garfinkel et al.'s third ethical consideration is that an individual should have alternatives to RFID, allowing them to opt-out of RFID altogether. In the embedded scenario the user has voluntarily opted-in. Taking the idea further, users should then have the ability to opt-in to new services and opt-out of their current service set as they see fit.

Given the remote and wireless nature of RFID however, there is little to indicate the success or failure of a stipulated user requested change, save for a receipt message that may be sent to a web client from the server. Quite possibly the user may not be aware that they have failed to opt-out of a service until they receive their next billing statement.

The fourth notion involves the right to know what information is stored on the RFID transponder and whether or not this information is correct. In this regard, there is a difference between passive and active tags. Passive transponders are limited in their size, storage space and reading range. They often only contain a serial number or unique identifier which links the host to a remote, ‘real-world’ database. Thus, considerations of database access and administration are primary concerns. Active transponders on the other hand can be read from greater distances and are more likely to be used to transmit location-based, ‘here I am’ type information to the subscribed service. In this instance, it is more important that the information on the transponder correctly identifies you, as opposed to information about you. The fifth and final point is “the right to know when, where and why a RFID tag is being read” [77]. This is quite difficult to exercise, especially where unobtrusiveness is considered a goal of the RFID system. In the resultant struggle between privacy, convenience, streamlining and bureaucracy, the number of times RFID transponders are triggered in certain applications may mean that the end-user is bombarded with a very long statement of transactions. Some of these transactions may well be fee-free, while some will come at a price.

8.4 The Privacy Fear and the Threat of Totalitarianism?

Mark Weiser, the founding father of ubiquitous computing, once said that the problem surrounding the introduction of new technologies is “often couched in terms of privacy, [but] is really one of control.” [70] Indeed, given that humans do not by nature trust others to safeguard their own individual privacy, in controlling technology we feel we can also control access to any social implications stemming from it. At its simplest, this highlights the different focus between the end result of using technology and the administration of its use. It becomes the choice between the idea that I am given privacy and the idea that I control how much privacy I have. Looking at this from the perspective of biometrics provides an interesting digression. Sweeping legislative changes in the United States have meant that visitors must now have their biometric registered before they are allowed to enter the country. Even despite a dim general acceptance of biometrics in recent years, the new border-entry scheme (stipulated in the Enhanced Border Security and Visa Entry Reform Act) has not stopped the majority of travellers from visiting the U.S. This is perhaps because there is a bargain of exchange - I’ll give you what you want if you let me do what I want. Privacy is traded for access.

While this border security scheme does provide a certain level of social control to the end-user (there is always the option not to travel to the U.S. at all), what some civil libertarians fear beyond privacy is a government-driven mandatory introduction of invasive technologies based on the premise of national security. While the safety and security argument has obviously paved the way for some new technologies in response to the new environment of terrorism and identity fraud, [27] there is now a concern that further advancements will begin to infringe on the freedoms that security paradigms were originally designed to protect. For invasive technology like humancentric RFID, the concerns are multiplied as the automated nature of information gathering means that proximity to a reader, and not personal choice, may often be the only factor in deciding whether or not a transponder will be triggered. Though most believe that government-imposed mandatory implantation is a highly unlikely outcome of advancements in humancentric RFID, it should be recognised that a voluntary implantation scheme offers negligible benefits to a government body given the incompleteness of the associated data set. This is equally true of private enterprises that mandate the use of transponders in employees, inmates or other distinct population groups. Indeed, in any humancentric scenario where information is not used for the direct benefit of the host of the technology, we can assume that control has been removed from the implantee.

Where the usability context of control then becomes the realm of government organizations and private enterprise, RFID regulation is increasingly important [76]. Not only is regulation necessary for ensuring legitimacy in control-type applications, it is also needed to prevent the perversion of convenience and care-related uses. For example, many of those implanted with RFID transponders today might consider them to be life-saving devices and the service-oriented nature of these applications means they must clearly remain voluntary (Table 5). If the data collected by the device was also to be used for law enforcement or government surveillance purposes however, users may think twice about employing the technology. These “unintended consequences” [72] are those that may well have the greatest impact on end-users. In regulating them we do not want to allow unrestricted deployment and unparalleled capabilities for commercial data mining, but nor should we allow a doomsday scenario where all citizens are monitored in a techno-totalitarian state [83]. Pottie [84] echoes these sentiments by stating that without appropriate architecture and regulatory controls democratic values are at risk of being subverted, claiming that “[i]nformation technology is not in fact neutral in its values” and that “we must be intentional about design for democracy.”

Any scope for such design of regulations must further be considered in light of the illustrated privacy / security trade-off (Figure 2). Taking any two vertices of the government – service provider – consumer triangle, privacy or security (which can often be equated with ‘control’) will always be traded in relation to the third vertex. For example, where we combine government and service providers in terms of security regulations and the protection of national interests, the consumer is guaranteed to forgo certain amounts of privacy. Similarly, where we combine government and the consumer as a means of ensuring privacy for the individual, the service provider becomes limited in the control it holds over information gathered (if indeed it is still allowed to gather information).

9 Conclusion

In the current state of humancentric development, stand-alone applications exist for control, convenience and care purposes, but as control is the dominant context its effects can be seen in other application areas. Applications are also influenced by power and processing confines, and as such, many functions have simple bases in identification or monitoring. Application usage is made more complex however, as a need for peripherals (including readers, information storage systems and, in some cases, GPS) is coupled with a lack of industry standards for interoperability. Though the technology has been deemed feasible in both research and commercially approved contexts, the market for humancentric applications of RFID is still evolving. Initial adoption of the technology has met with some success but, as research continues into humancentric applications of RFID, the market is still too niche for truly low-cost, high-quality application services. Any real assessment of the industry is further prejudiced by the commercial monopoly of the VeriChip Corporation and the limited social acceptance of the product at present. Feasibility is also constrained by limited research into long-term effects on humans and, where use in herd animals has seen the transponders dislodged or attacked as a foreign body by the immune system; this presents a negative view of humancentric RFID. Coupled with security and privacy concerns then, the long-term commercial viability for humancentric applications of RFID is questionable. In the short- to medium-term, adoption of humancentric RFID technology and use of related applications will be hindered by a lack of infrastructure, a lack of standards, not only as to interoperability but also as to support for service and transponder placement, and the lack of response from developers and regulators to mounting ethical dilemmas.

References

[1] S. Witt, Professor Warwick Chips In, Computerworld, 33(2) January 11 (1999) 89-90.
[2] K. Michael and M.G. Michael, The Social, Cultural, Religious and Ethical Implications of Automatic Identification, Proceedings of the Seventh International Conference on Electronic Commerce Research, Texas US (2004) 432-450.
[3] D. Icke, Has The Old ID Card Had Its Chips? Soldier Magazine, April (2001).
[4] Applied Digital Solutions, Applied Digital Solutions Announces Working Prototype of Subdermal GPS Personal Location Device, Press Release, April 13 2003.
[5] P. Eng, I Chip? ABC News.com, March 1 (2002).
[6] J. Wakefield, Chips To Fight Kidnapping, BBC News Online, March 24 (2002).
[7] C. Murray, Injectable Chip Opens Door To Human Bar Code, EETimes, January 7 2002. Available from: <http://www.eetimes.com/story/OEG20020104S0044>.
[8] J. Scheeres, New Body Art: Chip Implants, Wired News, March 11 2002. Available from: <http://www.wired.com/news/culture/0,1284,50769,00.html>.

[9] J. Wilson, Girl To Get Tracker Implant To Ease Parents' Fears, The Guardian, Available from: <http://www.guardian.co.uk/Print/0,3858,4493297,00.html>.
[10] Anonymous, GP Creates Cyberman In Surgery, Pulse [Online], September 5 1998. Available from: ProQuest.
[11] J. Sanchez-Klein, And Now For Something Completely Different, PC World Online, August 27 1998. Available from: ProQuest.
[12] K. Warwick, Cyborg 1.0, Wired Magazine 8.02, February 2000. Available from: <http://www.wired.com/wired/ archive/8.02/warwick.html>.
[13] R. Woolnaugh, A Man With A Chip In His Shoulder, Computer Weekly [Online], June 29 2000. Available from: Expanded Academic Index.
[14] C. Holden, Hello Mr Chip, Science [Online], March 23 2001. Available from: ProQuest.
[15] G. Vogel, Part Man, Part Computer, Science [Online], 295(5557), February 8 2002, p. 1020. Available from: Expanded Academic Index.
[16] R. Kobetic et al., Implanted Functional Electrical Simulation System For Mobility in Paraplegia: A Follow-up Case Report, IEEE Transactions on Rehabilitation Engineering [Online], December 1999. Available from: ProQuest.
[17] C. Murray, Prodigy Seeks Out High-tech Frontiers, Electronic Engineering Times [Online], February 25 2002. Available from: ProQuest.
[18] J. Black, Roll Up Your Sleeve- For A Chip Implant, Business Week Magazine [Online], March 21 2002. Available from: <http://www.businessweek.com/bwdaily/dnflash/mar2002/nf20020321_1025.htm>.
[19] L. Grossman, Meet The Chipsons, Time New York, 159(10) (2002) 56-57.
[20] D. Streitfeld, Chips To Be Implanted In Humans, Los Angeles Times [Online], May 10 2002. Available from: LexisNexis.
[21] B. Gengler, Chip Implants Become Part Of You, The Australian, September 10 2002.
[22] K. Michael, The technological trajectory of the automatic identification industry, PhD Thesis, School of Information Technology and Computer Science, University of Wollongong, Australia, 2003.
[23] A. Masters, Humancentric applications of RFID, BInfoTech (Hons) Thesis, School of Information Technology and Computer Science, University of Wollongong, Australia, 2003.
[24] K. Michael and M.G. Michael, Microchipping People: The Rise Of The Electrophorus, Quadrant 414 March (2005) 22-33.
[25] L. Perusco and K. Michael, Humancentric Applications of Precise Location-Based Services, IEEE Conference on e-Business Engineering, IEEE Computer Society, Washington, (2005), 409-418.
[26] K. Johnston, RFID transponder implants: a content analysis and survey, BInfoTech (Hons) Thesis, School of Information Technology and Computer Science, University of Wollongong, Australia, 2005.
[27] C. Perakslis and R. Wolk, Social Acceptance Of RFID As A Biometric Security Method, Proceedings of the IEEE Symposium on Technology and Society, (2005) 79-87.
[28] J. Gerdeman, Radio Frequency Identification Application 2000, North Carolina, USA, 1995.
[29] K. Finkinzeller, RFID Handbook: Radio-Frequency Identification Fundamentals and Applications, England, 2001.
[30] R. Geers et al., Electronic Identification, Monitoring and Tracking of Animals, United Kingdom, 1997.
[31] R. Yin, The Case Study Method As A Tool For Doing Evaluation, Current Sociology 40(1) (1998) 123.
[32] C. Thomas and N. Bevan, Usability Context Analysis: A Practical Guide, Middlesex, U.K., 1996.
[33] K. Michael, Location-based services: a vehicle for IT&T convergence, in: K. Cheng et al., Advances in E-engineering & Digital Enterprise Technology, UK Professional Engineering Publishing, 2004, 467-477.
[34] WherifyWireless, Corporate Home, Wherify Wireless Location Services, 2003. Available from: <http://www.wherifywireless.com/corp_home.htm>.
[35] K. Hall, Students Tagged In Bid To Keep Them Safe, The Japan Times, 2004. Available from: <http://search.japantimes.co.jp/print/news/nn10-2004/nn20041014f2.htm>.
[36] M. Wood, RFID: Bring It On, CNET.com, 2005. Available from: <http://www.cnet.com/4520-6033_1-6223038.html>.
[37] Vxceed Technologies, RFID Technology, 2003. Available from: <http://www.vxceed.com/developers/rfid.asp>.
[38] Automatic ID News, Radio Frequency Identification (RF/ID), 1998. Available from: <http://www.autoidenews.com/technologies/concepts/rfdcintro.htm>.

[39] M. Hawthorne, Refugees Meeting Hears Proposal To Register Every Human In The World, Sydney Morning Herald [Online], 2001. Available from: <http://www.iahf.com/other/20011219.html>.
[40] P. Hewkin, Smart Tags- The Distributed-Memory Revolution, IEE Review 35(6) (1989) 203-206.
[41] M. Mechanic, Beastly Implants, MetroActive, 1996. Available from: <http://www.metroactive.com/papers/metro/12.12.96/implants-9650.html>.
[42] W. Wells, The Chips Are Coming, Biotech Applied 2001. Available from: <http://www.accessexcellence.com/AB/BA/biochip.html>.
[43] D.B. Kitsz, Promises and Problems of RF Identification, in: R. Ames, Ed., Perspectives on Radio Frequency Identification: What is it, Where is it going, Should I be Involved? Van Nostrand Reinhold, New York, 1-19- 1-27.
[44] R. Want et al., The Active Badge Location System, ACM Transactions on Information Systems 10(1) (1992) 91-102.
[45] P. Puchner, Badges Can Track Staffing Needs, Pacific Computer Weekly, July 8 (1994), 26.
[46] W. Saletan, Call My Cell, Slate Magazine, May 2005. Available from: <http://slate.msn.com/id/2118117/>.
[47] B. Goldsmith, Homing In On Electronic Jail, The Australian, October 9 (1996) 32.
[48] J. Scheeres, Politician Wants To Get Chipped, Wired News, February 15 2002. Available from: <http://www.wired.com/news/print/0,1294,50435,00.html>.
[49] Applied Digital Solutions, Protected by VeriChip™- Awareness Campaign Continues- VeriChip To Exhibit At Airport Security Expo in Las Vegas, Press Release, July 2 2002.
[50] K. Michael and A. Masters, Realized applications of positioning technologies in defense intelligence, in: H. Abbass, D. Essam, Eds., Applications of Information Systems to Homeland Security and Defense, IDG Press, 167-195.
[51] L. Nadile, Call Waiting: A Cell Phone ATM, Wired News. Available from: <http://www.wired.com/news/business/0,1367,41023,00.html>.
[52] J.C. Ramo, The Big Bank Theory and What It Says About the Future of Money, Time, April 27 (1998), 46-55.
[53] S. Dennis, UK Professor Implants Chip, Turns Himself Into Cyborg, Newsbytes, 1998. Available from: <http://www.newsbytes.com/pubNews/110782.html>.
[54] Texas Instruments, Loyally Yours, TIRIS News, 1997. Available from: <http://www.ti.com/ tiris/docs/manuals/RFIDNews/Tiris_NL17>.
[55] K. Warwick, Project Cyborg 2.0. Available from: <http://www.rdg.ac.uk/KevinWarwick/html/project_ cyborg_2_0.html>.
[56] W. Underhill, Merging Man and Machine, Newsweek [Online], October 14 2002. Available from: Expanded Academic Index.
[57] K. Coughlin, The Melding of Man and Machine, New Jersey, April 1 2000. Available from: <http: //www.cochrane.org.uk/opinion/interviews/01-04-2000.htm>.
[58] T. Seneadza, Biosensors- A Nearly Invisible Sentinel, Technically Speaking, July 21 2003. Available from: <http://tonytalkstech.com/archives/000231.php>.
[59] P.L. Harrison, The Body Binary, Popular Science, October, 1994. Available from: <http://www.newciv.org/nanomius/tech/implants>.
[60] M-Biotech.: Biosensor Technology. M-Biotech Salt Lake City, 2003. Available from: <http://www.m-biotech.com/technology1. html>.
[61] IEEE. Biomimetic Systems: Implantable, Sophisticated, and Effective. IEEE Engineering in Medicine and Biology 24(5) Sept/Oct (2005).
[62] Cochlear, Nucleus 24 Cochlear Implant, 1999. Available from: <http://www.Cochlear.com/euro/nucleussystems/ci24m.html>.
[63] Sun-Sentinel, The Smart Pill, Sun-Sentinel News: The Edge, 2003. Available from: <http://www.sun-sentinel. com/graphics/news/smartpill>.
[64] J. Rizzo and J. Wyatt, Prospects For A Visual Prosthesis, The Neuroscientist 3(4) 1997. Available from: <http://rleweb.mit.edu/retina/a2.page1.html>.
[65] G.T.A. Kovacs, The Nerve Chip: Technology Development For A Chronic Neural Interface, Stanford University, 1997. Available from: <http://guide.stanford.edu/publications/dev4.html>.
[66] K. Mieszkowski, Put That Silicon Where The Sun Don't Shine, Salon.com, 2000. Available from: <http://www. salon.com/tech/feature/2000/09/07/chips/>.

[67] K. Michael and A. Masters, Applications Of Human Transponder Implants In Mobile Commerce, Proceedings of the Eighth World Multiconference on Systemics, Cybernetics and Informatics, Florida 5 (2004) 505-512.
[68] Applied Digital Solutions, Press Release VeriChip™ Subdermal Personal Verification Microchip To Be Featured At IDTechex Smart Tagging In Healthcare, Conference In London, April 28-29 (2003).
[69] RFID News, International Standards Organization Returns RFID Standard For Animal Use To Working Group For Major Revisions, RFID News, 2002. Available from: <http://www.rfidnews.com/returns.html>.
[70] O. Günther and S. Spiekermann, Tagging The World: RFID and the Perception of Control, Communications of the ACM 48(9) 2005 74.
[71] K. Michael and A. Masters, The advancement of positioning technologies in defense intelligence, in: H. Abbass, D. Essam, Eds., Applications of Information Systems to Homeland Security and Defense, IDG Press, ch. 8, 196-220.
[72] J. Kumagi and S. Cherry, Sensors and Sensibility, IEEE Spectrum 41(7) (2004) 22-26, 28.
[73] V. Stanford, Pervasive Computing Goes That Last Hundred Feet With RFID Systems, IEEE Pervasive Computing 2(2) (2003) 9-14.
[74] I-E. Papasliotis, Information Technology: Mining For Data And Personal Privacy: Reflections On An Impasse, Proceedings of the 4th International Symposium on Information and Communication Technologies, (2004), 53.
[75] A. Juels, R.L. Rivest and M. Szydlo, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, Proceedings of the 10th ACM Conference on Computer and Communications Security, (2003), 104.
[76] X. Gao et al., An Approach To Security And Privacy Of RFID System For Supply Chain, IEEE International Ecommerce Technology for Dynamic e-Business, (2004), 164-168.
[77] S.L. Garfinkel, A. Juels, R. Pappu, RFID Privacy: An Overview of Problem and Proposed Solutions, IEEE Security and Privacy Magazine 3(3) (2005) 38-43.
[78] J.D. Woodward, Biometrics: Privacy's Foe Or Privacy's Friend?, Proceedings of the IEEE 85(9) (1997) 1480-1492.
[79] D. Molnar and D. Wagner, Privacy: Privacy And Security In Library RFID: Issues, Practices, and Architectures, Proceedings of the 11th ACM Conference on Computer and Communications Security (2004) 218.
[80] F. Stajano, Viewpoint: RFID Is X-ray Vision, Communications of the ACM 48(9) (2005) 31.
[81] Accenture, Silent Commerce Chips Away At Star City Casino Wardrobe Worries. Available from: <http://www.accenture.com/xdoc/en/services/technology/vision/Star_City_Casino_Final.pdf>.
[82] S.N. Roberts, Tracking Your Children With GPS: Do You Have The Right? Wireless Business and Technology 3(12) (2003) 20.
[83] J.E. Dobson and P.F. Fisher, Geoslavery, IEEE Technology and Society Magazine 22(1) 2003 47.
[84] G.J. Pottie, Viewpoint: Privacy in the Global e-Village, Communications of the ACM 47(2) (2004) 21.

	Intended Users	**Specific Uses**	**Constraints**
Security	Mass market, persons likely to be involved in high-risk situations, the elderly, children	Personal identification, location based services	Lack of widespread infrastructure, need for reader proximity to RFID tags, data correlation, external GPS integration
Management	Employees, visitors to restricted locations	Access control, monitoring	Employee consent, need for reader proximity to tags, external GPS integration
Social	Military personnel, police officers, inmates, parolees	Monitoring, crime prevention	Possible involuntary use of application, external GPS integration

Table 1 Control Usability Sub-Contexts.

	Intended Users	**Specific Uses**	**Constraints**
Assistance	Mass market, travelers, athletes, car owners	Identification of objects, location based services, roadside assistance, emergency services	RF interference, need for an appropriate placement of the transponder to facilitate accurate reading, external GPS integration, GPS will not work indoors
Finance	Mass market	Credit or debit facilities, identification of transaction owner.	Lack of widespread infrastructure, cannot eliminate all human interaction
Interactivity	Mass market, home owners, office dwellers, car owners	Interactive buildings, keyless entry systems, remote control of devices	Need for advanced infrastructure, close proximity between readers and RFID tags

Table 2 Convenience Usability Sub-Contexts.

	Intended Users	Specific Uses	Constraints
Medical	Mass market, persons with allergies, persons with chronic medical conditions	Storage and portability of medical records, patient identification	Lack of widespread infrastructure, external GPS integration
Biomedical	Sufferers of chronic disease, trauma victims, those taking regular medication, in-patients	Monitoring of biological parameters for medical and health-related care purposes	Implant attacked or rejected by the human host, implant dislodgement, lack of widespread infrastructure, limited development and human testing
Therapeutic	Those with previously implanted therapeutic devices, those in need of remedial care, disabled persons	Monitoring of implanted devices, physiotherapy	System complexity, material constraints, computational ability, power, robustness and fault tolerance, scalability and continuous operation

Table 3 Care Usability Sub-Contexts.

	Humancentric Applications	Humancentric RFID Devices
Benefit	Improved control, enhanced security, increased convenience, improved care, accurate identification, theft-proof, counterfeit-proof, access control, resource monitoring, location tracking and emergency alert (with GPS), interactive locations and devices, biosensing, streamlined processes, data portability, time savings, economic benefits, implant is hidden, tag cannot be forgotten or ‘lost’	Secured within the body, reduced theft and loss of components, serial numbers and passwords on the transponder are imperceptible to the naked eye
Cost	Lack of widespread reading infrastructure, need for data correlation, need for a standardized placement of the transponder to facilitate accurate reading, possible involuntary use of application, crude success in human-to-human communications	Material constraints, computational ability, low power, wireless interference, system complexity, fault tolerance, need for continuous operation, robustness, implant attacked or rejected by the human host, dislodgement, close proximity between reader & tag, external GPS integration

Table 4 High Level Benefits and Costs for Humancentric RFID.

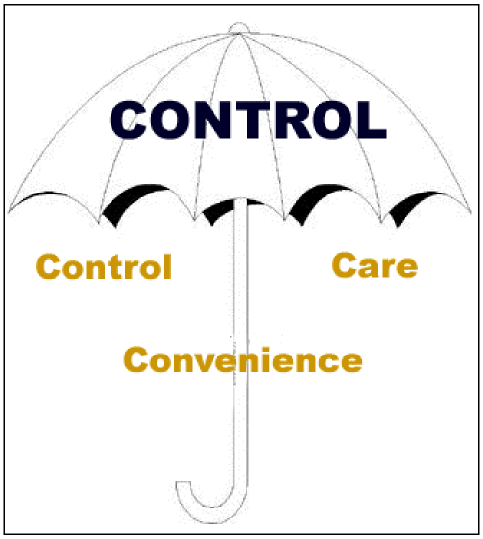

Figure 1 The Pervading Nature of Control.

Usability Contexts	**Stakeholder Driving Innovation**	**Setting**	**Major Function**
Control	Government/ Private Enterprise	Mandatory	ID, Track
Conveni-ence and Care	Service Provider/ Consumer	Voluntary	Trace & Monitor

Table 5 Mapping Contexts to the Environment.

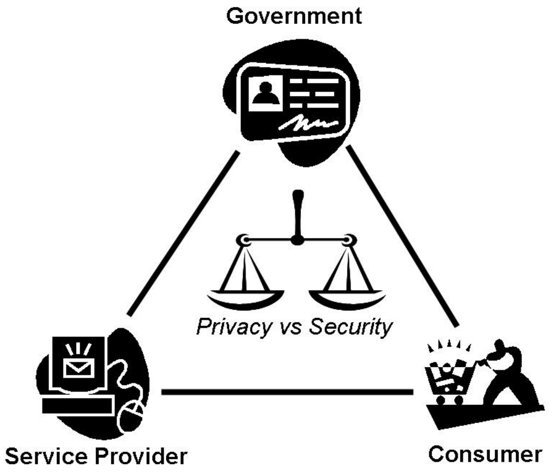

Figure 2 The Privacy-Security Trade-Off.