Available online at www.sciencedirect.com
ScienceDirect
Electronic Commerce Research and Applications 6 (2007) 29–39
Electronic Commerce Research and Applications
www.elsevier.com/locate/ecra

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, Wollongong, NSW 2522, Australia

Received 15 December 2005; received in revised form 15 February 2006; accepted 24 April 2006
Available online 12 June 2006

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. 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,

* Corresponding author. Tel.: +61 2 4221 3937; fax: +61 2 4221 4170.
E-mail address: katina@uow.edu.au (K. Michael).

1567-4223/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.elerap.2006.04.008

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 [1] for example lack the evidentiary support needed to assuage doubts. Further, many articles highlight the technological obstacles besieging humancentric RFID systems. These include GPS hardware miniaturization [2] 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 [3], for example, predicts that tags will be melded into children to advise parents of their location.

Despite concerns and conjecture, actual implementations of humancentric control applications of RFID have been identified. Both Murray [4] 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. Wilson [5] 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.

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. Sanchez-Klein [6] and Witt [7] both 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 [8].

Woolnaugh [9], Holden [10], and Vogel [11] 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. 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 [7]. 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 [12]. 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 [13], Black [14], Grossman [15] and Gengler [16] all document medical reasons behind the implantation of four subjects. Supplemented by press releases however, all reports of the trials were journalistic, rather than research-based. In contrast, non-trivial research is found in the work of Michael [17]. 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 [18], Michael and Michael [19], Perusco and Michael [20], Johnston [21], and Perakslis and Wolk [22]. 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 [23], Finkinzeller [24] and Geers [25] all use case studies to investigate non-humancentric RFID and hence our methodological precedent is set here. The bulk of the remaining literature is newstype in nature and the absence of research frameworks is evident. The few exceptions to this include Woolnaugh [9] who conducted an interview and Murray [13] and Eng [3] who provide small case studies. In further criticism the news articles do not demonstrate technological trajectories but speculate on utopian implementations unlikely to be achieved by incremental development in the short to medium-term. Thus, any real value in these news articles can only be found in the documentation of events.

3. Research methodology

Several modes of academic inquiry were used in this study, though usability context analyses were the focal means of research. 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" [26]. 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" [27]. 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 defining the research framework, the primary question to be answered – '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. The usability context analyses are also 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. Usability context analysis: control

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

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.

Numerous applications have been proposed to assist individuals who depend solely on carers for support. This group consists of newly-born babies, sufferers of mental illness, persons with disabilities and the elderly. One 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. Further, when connected to security sensors and alarms, the technology can alert staff to the "unauthorized removal of children" [28]. The South Tyneside Healthcare Trust Trial in the UK 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 trial was so successful that the hospital was considering expanding the system to include the children's ward. [29] Notably, a number of other institutions have already begun targeting RFID applications toward adolescents. 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 [30]. A similar practice is being conducted in California where children are being asked to "wear" RFID tags around their necks when on school grounds [31].

Commentators are using this lack of objection to external electronic tagging for minors 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 travellers. Smet [32] 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."

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 are similarly 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 [33]. In this regard, Olivetti's "active badge" was ahead of its time when it was first launched [34].

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.

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 trials are taking place in the UK, US, Netherlands and Canada. In 2002, 27 American states had tested or were using some form of satellite surveillance to monitor parolees [14]. In 2005 there were an estimated 120,000 tracked parolees in the United States alone [35]. Whilst tagging low-risk offenders is not popular in many countries it is far more economical than the conventional jail. 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 marketed toward victims of crime rather than offenders. They are seen as a way "to identify kidnapping victims who are drugged, unconscious or dead" [36].

5. Usability context analysis: convenience

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

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" [37]. 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 [38]. This includes "find me", "find a friend", "where am I" and "guide me to" solutions. Integrating RFID and GPS technologies with a geographic information systems (GIS) portal such as the Internet-based mapquest.com would also allow users to find destinations based on their current GPS location. The nature of this application 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 acknowledged the rise of the cashless society. In recent years though, alongside traditional contact cards, we have seen the emergence of alternate payment processes. In 2001, Nokia tested the use of RFID in its 5100-series phone covers, allowing the device to be used as a bank facility. RFID readers were placed at McDonalds drive-through restaurants in New York and the consumer could 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. Wired News noted the convenience stating, "there is no dialing, no ATM, no fumbling for a wallet or dropped coins" [39]. 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" [40]. 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 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 questioned. This has similar benefits for automatic teller machines. When such intermediary transaction devices are fitted with RFID readers, RFID transponders have the ability to replace debit and credit cards. This is in line with Warwick's prediction that implanted chips "could be used for money transfers, medical records, passports, driving licenses, and loyalty cards" [41].

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 already exist) [42].

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" [43]. 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 [44]. Movement sensations were therefore effectively, though primitively, transmitted.

6. Usability context analysis: care

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

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" [16]. 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" [45]. It combines biological and electronic components to produce quantitative measurements of biological parameters, or qualitative alerts for biological change. 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 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 [25]. 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 such a microchip implanted in their body to monitor and perhaps even control blood pressure, their heart rate, and cholesterol levels.[46] Though Cambou's predictions did not come to timely fruition, the multitude of potential applications are still feasible 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 [47]. 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 [48]. 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 [49] and smart pills aside [50]. 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 [51] 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 [52]. Arguably the technology for the applications already exists. 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. 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 [53].

Alongside the contextual themes encapsulating the usability contexts are the corresponding benefits and costs in each area (Table 1). When taking a narrow view 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.

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. This indicates 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 an incompatible, 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. Without a common site for implantation 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.

Table 1
High level benefits and costs for humancentric RFID

	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 and tag, external GPS integration

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 service 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.

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. 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 [54], 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 [55]. Not only did the standards not require unique identification codes, they violated the patent policy of the International Standards Organization. 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, moves have now 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 [18].

8. Discussion

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. 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. The severity of violations to personal privacy increase as data collected for one purpose is linked with completely separate datasets gathered for another purpose. 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 [56] 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 [57] menacingly calls this a type of data use "scope creep" while Papasliotis [58] more pleasantly deems it "knowledge discovery".

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" [59]. Indeed, given their implantation 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. This becomes a greater danger when we note that 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.

Moreover, even where ethical data usage is not questioned, intellectual property directives in Europe may hamper the promise of some service providers to keep consumer data private. According to Papasliotis [58] "... 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".

8.2. Data security

Relevant approaches to RFID security in relation to inanimate objects have been discussed in the literature. Gao [60] 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 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 US however, also thwarting an original purpose, a study has shown that some RFID transponders are capable of being cloned, meaning the prospect of fraud or theft may still exist [61]. One possibility, as proposed by Perakslis and Wolk [22], is the added security of saving an individual's feature vector onboard the RFID chip. Biometrics too, however, is fraught with its own problems [62]. 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.

Unfortunately, whatever the security, researchers like Stanford believe it is a "virtual certainty" that tags and their respective systems "will be abused" by some providers [57]. Here, the main risk for consumers involves third parties gaining access to personal data 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 oversight companies like VeriSign in these early days of global information gathering which will allow consumers to create their own standards and opinions.

Outside of clear ethical concerns regarding third-party interests in information, another temptation for service providers surrounds the use of data to target individual consumer sales in value-added services and service-sets relying on location information. Though not an extreme concern in itself, we note that any such sales will face the more immediate concern of deciding on a secure and standard location for implants. 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. What if the consumer is an amputee or has prosthetic limbs? 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 or agency acting as an issuer, or the individual? Who is responsible for accuracy and liable for errors? And more importantly, who is liable for break-downs in communication when services are unavailable and disaster results?

8.3. Ethical considerations

Molnar and Wagner [63] ask the definitive question "[i]s the cost of privacy and security "worth it"?" Stajano [64] 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" [22]. 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. 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" [58].

Garfinkel et al. [61] provide a thorough discussion on key 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 [65]?

Secondly, the user has the right to have embedded RFID tags "removed, deactivated, or destroyed" [61] at or after purchase. Applied to humancentric implantation, this point poses a number of difficulties. The user cannot remove the implant themselves without some physical harm, 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 body implies some form of amputation. Garfinkel et al.'s third ethical consideration is that an individual should have alternatives to RFID. In the embedded scenario users should then also have to ability to opt-in to new services and opt-out of their current service set as they see fit. Given the 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, while the fifth point is "the right to know when, where and why a RFID tag is being read" [61]. 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.

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" [59]. Indeed, given that humans do not by nature trust others to safeguard our 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. In this regard, privacy is traded for service.

What some civil libertarians fear beyond privacy exchange though 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 technologies in response to the new environment of terrorism and identity fraud [38], 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.

Where the usability context of control then becomes the realm of government organizations and private enterprise, RFID regulation is increasingly important. 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 2). 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. In regulating then we do not want to allow unrestricted deployment and unparalleled capabilities for commercial data mining, but nor

Table 2
Mapping contexts to the environment

Usability contexts	Stakeholder driving innovation	Setting	Major function
Control	Government/private enterprise	Mandatory	ID, track
Convenience and care	Service provider/ consumer	Voluntary	Trace and Monitor

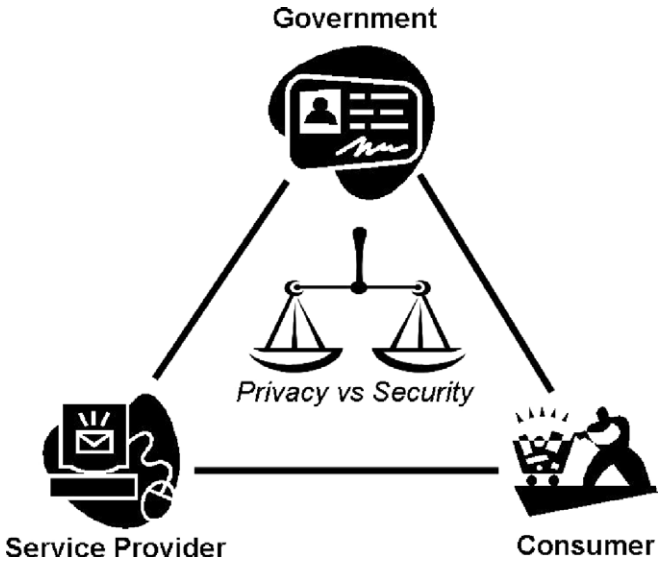

Fig. 1. The privacy-security trade-off.

should we allow a doomsday scenario where all citizens are monitored in a techno-totalitarian state [61]. Any scope for such design of regulations must be considered in light of the illustrated privacy/security trade-off (Fig. 1). 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 and information storage systems) is restrained by 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 commercial monopoly and limited research into the long-term effects of use. 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] D. Icke, Has the old ID card had its chips? Soldier Magazine (2001).
[2] Applied Digital Solutions, Applied Digital Solutions Announces Working Prototype of Subdermal GPS Personal Location Device, Press Release, April 13, 2003.
[3] P. Eng, I Chip? ABC News.com, March 1, 2002.
[4] C. Murray, Injectable chip opens door to human bar code, EETimes, January 7, 2002. Available from: <http://www.eetimes.com/story/OEG20020104S0044>.
[5] 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>.
[6] J. Sanchez-Klein, And Now For Something Completely Different, PC World Online, August 27, 1998. Available from: ProQuest.
[7] S. Witt, Professor Warwick Chips In, Computerworld 33 (2) (1999) 89–90.
[8] K. Warwick, Cyborg 1.0, Wired Magazine 8.02, February 2000. Available from: <http://www.wired.com/wired/archive/8.02/warwick.html>.
[9] R. Woolnaugh, A man with a chip in his shoulder, Computer Weekly [Online], June 29, 2000. Available from: Expanded Academic Index.
[10] C. Holden, Hello Mr Chip, Science [Online], March 23. 2001. Available from: ProQuest.
[11] G. Vogel, Part Man, Part Computer, Science [Online], 295 (5557), February 8, 2002, p. 1020. Available from: Expanded Academic Index.
[12] 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.
[13] C. Murray, Prodigy seeks out high-tech frontiers, Electronic Engineering Times [Online], February 25, 2002. Available from: ProQuest.
[14] 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>.
[15] L. Grossman, Meet The Chipsons, Time New York 159 (10) (2002) 56–57.
[16] B. Gengler, Chip implants become part of you, The Australian, September 10, 2002.
[17] K. Michael, The technological trajectory of the automatic identification industry, Ph.D. Thesis, School of Information Technology and Computer Science, University of Wollongong, Australia, 2003.

[18] A. Masters, Humancentric applications of RFID, BInfoTech (Hons) Thesis, School of Information Technology and Computer Science, University of Wollongong, Australia, 2003.
[19] K. Michael, M.G. Michael, Microchipping people: the rise of the electrophorus, Quadrant 414 (2005) 22–33.
[20] L. Perusco, K. Michael, Humancentric Applications of Precise Location-Based Services, IEEE Conference on e-Business Engineering, IEEE Computer Society, Washington, 2005, pp. 409–418.
[21] 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.
[22] C. Perakslis, R. Wolk, Social acceptance of RFID as a biometric security method, in: Proceedings of the IEEE Symposium on Technology and Society, 2005, pp. 79–87.
[23] J. Gerdeman, Radio frequency identification application 2000, North Carolina, USA, 1995.
[24] K. Finkinzeller, RFID Handbook: Radio-Frequency Identification Fundamentals and Applications, England, 2001.
[25] R. Geers et al., Electronic Identification, Monitoring and Tracking of Animals, United Kingdom, 1997.
[26] R. Yin, The case study method as a tool for doing evaluation, Current Sociology 40 (1) (1998) 123.
[27] C. Thomas, N. Bevan, Usability Context Analysis: A Practical Guide, Middlesex, UK, 1996.
[28] Vxceed Technologies, RFID Technology, 2003. Available from: <http://www.vxceed.com/developers/rfid.asp>.
[29] Automatic ID News, Radio Frequency Identification (RF/ID), 1998. Available from: <http://www.autoidenews.com/technologies/concepts/rfdcintro.htm>.
[30] 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>.
[31] M. Wood, RFID: Bring It On, CNET.com, 2005. Available from: <http://www.cnet.com/4520-6033_1-6223038.html>.
[32] 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>.
[33] 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, pp. 1-19–1-27.
[34] R. Want et al., The Active Badge Location System, ACM Transactions on Information Systems 10 (1) (1992) 91–102.
[35] W. Saletan, Call my cell, Slate Magazine, May, 2005. Available from: http://slate.msn.com/id/2118117.
[36] 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>.
[37] Applied Digital Solutions, Protected by VeriChip™ – Awareness Campaign Continues – VeriChip To Exhibit At Airport Security Expo in Las Vegas, Press Release, July 2, 2002.
[38] K. Michael, A. Masters, Realised applications of positioning technologies in defense intelligence, in: H. Abbass, D. Essam (Eds.), Applications of Information Systems to Homeland Security and Defense, IDG Press, pp. 167–195.
[39] L. Nadile, Call Waiting: A Cell Phone ATM, Wired News. Available from: <http://www.wired.com/news/business/0,1367,41023,00.html>.
[40] J.C. Ramo, The Big Bank Theory and what it says about the future of money, Time, April 27, 1998, pp. 46–55.
[41] S. Dennis, UK Professor Implants Chip, Turns Himself Into Cyborg, Newsbytes, 1998. Available from: <http://www.newsbytes.com/pubNews/110782.html>.
[42] Texas Instruments, Loyally Yours, TIRIS News, 1997. Available from: <http://www.ti.com/tiris/docs/manuals/RFIDNews/Tiris_NL17>.
[43] K. Warwick, Project Cyborg 2.0. Available from: <http://www.rdg.ac.uk/KevinWarwick/html/project_ cyborg_2_0.html>.
[44] W. Underhill, Merging Man and Machine, Newsweek [Online], October 14, 2002. Available from: Expanded Academic Index.
[45] T. Seneadza, Biosensors – A Nearly Invisible Sentinel, Technically Speaking, July 21, 2003. Available from: <http://tonytalkstech.com/archives/000231.php>.
[46] P.L. Harrison, The Body Binary, Popular Science, October, 1994. Available from: <http://www.newciv.org/nanomius/tech/implants>.
[47] M-Biotech: Biosensor Technology. M-Biotech Salt Lake City, 2003. Available from: <http://www.m-biotech.com/technology1.html>.
[48] IEEE, Biomimetic Systems: Implantable, Sophisticated, and Effective. IEEE Engineering in Medicine and Biology 24(5) Sept/Oct (2005).
[49] Cochlear, Nucleus 24 Cochlear Implant, 1999. Available from: <http://www.Cochlear.com/euro/nucleussystems/ci24m.html>.
[50] Sun-Sentinel, The Smart Pill, Sun-Sentinel News: The Edge, 2003. Available from: <http://www.sun-sentinel.com/graphics/news/smartpill>.
[51] J. Rizzo, J. Wyatt, Prospects for a visual prosthesis, The Neuroscientist 3 (4) (1997). Available from: http://rleweb.mit.edu/retina/a2.page1.html .
[52] 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>.
[53] K. Michael, A. Masters, Applications of human transponder implants in mobile commerce, in: Proceedings of the Eighth World Multiconference on Systemics, Cybernetics and Informatics, Florida, vol. 5, 2004, pp. 505–512.
[54] 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.
[55] 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>.
[56] J. Kumagi, S. Cherry, Sensors and sensibility, IEEE Spectrum 41 (7) (2004) 22–26, 28.
[57] V. Stanford, Pervasive computing goes that last hundred feet with RFID Systems, IEEE Pervasive Computing 2 (2) (2003) 9–14.
[58] I.-E. Papasliotis, Information technology: mining for data and personal privacy: reflections on an impasse, in: Proceedings of the 4th International Symposium on Information and Communication Technologies, 2004, pp. 50–56.
[59] O. Günther, S. Spiekermann, Tagging the world: RFID and the perception of control, Communications of the ACM 48 (9) (2005) 74.
[60] 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.
[61] 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.
[62] J.D. Woodward, Biometrics: privacy's foe or privacy's friend? Proceedings of the IEEE 85 (9) (1997) 1480–1492.
[63] D. Molnar, D. Wagner, Privacy: privacy and security in library RFID: issues, practices, and architectures, in: Proceedings of the 11th ACM Conference on Computer and Communications Security, 2004, p. 218.
[64] F. Stajano, Viewpoint: RFID is X-ray vision, Communications of the ACM 48 (9) (2005) 31.
[65] J.E. Dobson, P.F. Fisher, Geoslavery, IEEE Technology and Society Magazine 22 (1) (2003) 47.