FIDIS

Future of Identity in the Information Society

Title:	"D12.6: A Study on ICT Implants"
Author:	WP12
Editors:	Eleni Kosta (ICRI - K.U. Leuven, Belgium)
	Mark Gasson (University of Reading, UK)
Reviewers:	Hans Hedbom (Karlstad University, Sweden)
	Vassiliki Andronikou (ICCS, Greece)
Identifier:	D12.6
Type:	[Deliverable]
Version:	1.0
Date:	Tuesday, 30 September 2008
Status:	[Final]
Class:	[Public]
File:	FIDIS_D12.6_v1.0.doc

Summary

The increasing commercialisation and growing potential of human ICT implants has generated debate over the ethical, legal and social aspects of the technology, its products and application. Despite stakeholders calling for greater policy and legal certainty within this area, gaps have already begun to emerge between the commercial reality of human ICT implants and the current legal frameworks designed to regulate these products.

This study will detail and discuss the security and privacy implications of human ICT implants that are used both in a medical context and for authentication and identification purposes, that can hold or transmit personal data, and which could ultimately be used for human enhancement. Here, we will not only focus on the latest technological developments, but also the legal, social and ethical implications of the use and further application of these technologies.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant

[2] Legal name: Ministerie Van Justitie

[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	13-09-07	• Initial release
0.2	17-11-07	• Initial draft structure of the deliverable
0.3	17-03-08	• First compilation of contributions
0.4	12-04-08	• Editorial changes
0.5	24-04-08	• Editorial changes
0.6	01-05-08	• Revision of socio-ethical chapter and overall structure
0.7	02-07-08	• Revision of technical chapter
0.8	09-07-08	• Revision of legal chapter
0.9	10-07-08	• Release for internal review
1.0	30-09-08	• Final release

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Executive Summary**)**	Editors
2 (Introduction**)**	Editors & VUB
3 (ICT Implants: From Restoration to Enhancement**)**	Reading
4 (Application cases of ICT implants**)**	Reading, IPTS, VIP, COSIC
5 (A legal analysis of ICT implants **)**	TILT, ICRI
6 (Socio-ethical considerations on ICT implants**)**	VIP, IPTS, VUB
7 (Regulatory challenges of human ICT implants**)**	Diana Bowman (Monash University)
8 (Conclusion**)**	Editors

Table of Contents

1 Executive Summary

While considered by many to be within the realm of science fiction, human ICT implants have actually been developed for many years in a medical context. Notable examples of such devices are cardiac defibrillators and pacemakers used to restore heart rhythm, and deep brain stimulators which are used to treat the symptoms of conditions like Parkinson's disease. Keeping in step with developments of other fundamental technologies, these types of active devices are becoming increasingly complex, and their functionality continues to grow. Data logging and wireless, real-time communications with external computing devices are now well within their capabilities and becoming standard features. However, because these devices have not been designed with security and privacy in mind, we are already seeing virtually all commercially available devices produced without even the simplest of access control which has series implications.

In a rather different application area, simple passive technologies such as RFID tags are being routinely implanted in healthy humans. Whilst the numbers of people with such devices are still small, the commercialisation of this technology specifically for this area will mean that they could become commonplace. The security and privacy implications of RFID for a variety of applications have been well explored, but the use of them inside the body serves to further aggravate some of the known issues.

While development in the area of human ICT implants has been slow, the convergence of fields such as nanotechnology, biotechnology, information technology, cognitive science, robotics, and artificial intelligence is likely to increase the application and prevalence of such ICT implant devices. Indeed, the next step of forming direct bi-directional links between human and machine is moving inexorably closer, and the likelihood of technology being developed for medical use finding application for human enhancement cannot and should not be discounted.

Current applications alone introduce challenging questions. Indeed the increasing commercialisation of human ICT implants has generated debate over the ethical, legal and social aspects of the technology and its products. Here we aim to introduce the current state-of-the-art of this technology, demonstrate how it may be used in the near future, and investigate some of the pertinent identity related issues from technical, legal, social and ethical viewpoints.

To aid the discussion, in Chapter 2 we classify the devices by function. We specifically distinguish between implants used to *restore* or repair human capabilities, those designed for the *diagnosis* of a biological state, those that *identify* a person and whose primary function is to *enhance* the human. In order to strike a balance between needing an understanding of implantable ICT devices before presenting case studies, and yet achieving understanding through the application studies themselves, Chapter 3 discusses the potential evolution of current day restorative devices, to more futuristic enhancement devices. This is intended to serve as an introduction to the state-of-the-art in human implantable ICT devices. Using the categorisation described, Chapter 4 will introduce some specific examples of human ICT implants, and will analyse the privacy and security concerns from a technical perspective. Chapter 5 will follow up on this technical analysis with the legal perspective on implantable devices and the implications they have on bodily integrity and privacy, before Chapter 6 discusses the social and ethical implications and Chapter 7 the regulatory challenges such technology brings.

2 Introduction

It is clear that not all visions of the future will be accurate, and this goes for those debated by scientists as much as anyone else. Indeed many of the great revolutionary technologies prophesised by scientists have to date evidently failed to materialise. However, in a shift in approach, 'Emerging Technologies' is a new way of thinking which considers the convergence of fields such as nanotechnology, biotechnology, information technology, cognitive science, robotics, and artificial intelligence. It is considered that the next wave of disruptive technologies will actually be a result of this domain fusion rather than from any one field in isolation.

The relatively new trend for low-tech human implants has recently risen in the public consciousness, although less publicised developments of high-tech implants in the medical domain have been progressing for several decades. Indeed, a significant drive behind the development of so called Information Communicating Technology (ICT) implant devices is medical – i.e. restoring deficient human abilities. It is clear that this application area is one which can be greatly enhanced through the new emerging technology phenomenon, and it is not clear where this may ultimately take us. The ability to form direct, bi-directional links with the human brain will open up the potential for many new application areas. Scientists predict that within the next thirty years neural interfaces will be designed that will not only increase the dynamic range of senses, but will also enhance memory and enable "cyberthink" - invisible communication with others and technology (McGee & Maguire, 2007). But are these claims realistic, and should they be taken seriously?

In this deliverable we discuss the current state-of-the-art of human implantable devices, consider the security and privacy issues that these already bring, and further debate the legal and ethical ramifications of the current and potential application of this technology.

2.1 Terminology and crucial distinctions

For a proper understanding of the wide scope of human implants we will briefly discuss the different types of implants and their different functions. Technological implants are often used to restore bodily functions, as in the case of cardiovascular pacemakers or deep brain stimulation (see Chapter 4). Moreover, entirely different uses can be envisioned, like monitoring of biological functions to enable real time diagnostics or the identification of clients or patients in order to grant them a right of access or to streamline the information system of healthcare institutions. The most imaginative usage of human implants is human enhancement or the creation of human-machine hybrids that challenge our notion of what it is to be human and raise the issue of who is in control: software programs, the individual human mind of whoever 'has' or 'is' the implant, or the data controller who holds the remote control.

Due to the different affordances of distinct types of implants in the human body, and the different consequences they may have, we will discriminate between:

1. Implants that aim to *restore* or *repair* human capabilities
2. Implants designed for the *diagnosis* of a biological state

3. Implants that *identify* a person in order to e.g. provide access to certain locations, information or knowledge, or to automatically pay/bill for services rendered
4. Implants that aim to *enhance* human memory, vision, auditory perception, alertness or other human capabilities

Technically, we will discriminate between:

1. *Active* implantable devices which can function using an internal power source, and *Passive* implantable devices which depend on power supplied to it remotely
2. *Online* ICT implants that rely for their operation on an online connection to an external computer and *Offline* or stand alone ICT implants that can operate independently of external devices

Using this categorisation, Chapter 4 will introduce some specific examples of ICT implants, and will analyse the privacy and security concerns from a technical perspective. Chapter 5 will follow up on this technical analysis with the legal perspective on implantable devices and the implications they have on bodily integrity and privacy, before Chapter 6 discusses the social and ethical implications and Chapter 7 the regulatory challenges. In order to strike a balance between needing an understanding of implantable ICT devices before presenting case studies, and yet achieving understanding through the application studies themselves, the following chapter will present a road map of the evolution of current day restorative devices, to somewhat futuristic enhancement devices. This is intended to serve as an introduction to the state-of-the-art in human implantable ICT devices.

3 ICT Implants: From Restoration to Enhancement

Technology suitable for implantation has been actively developed for some years with specific application to restore aspects of the human body's normal function. While these devices, through the evolution of component technologies driven by other market areas, have become gradually more complex and capable, they have not raised significant ethical or social issues. More recently, the implantation of simple technologies in people with no medical need has started to generate some concern, and the discussion is turning to where this may ultimately lead us in the future. Here, we consider the evolution of this trend by extrapolating from its roots in restorative devices, through the current state-of-the-art, to the potential use of technology developed in a medical context in healthy humans for enhancement.

3.1 ICT implants for Restorative application

There is a fair range of 'restorative' devices already in clinical use, although many, such as artificial joints, could not through their function alone be considered ICT devices. Others, such as the artificial heart pacemaker, have actually become notably sophisticated in recent years with integrated movement sensors to adjust heart rate based on estimated demand, internal logging of biological data, and RF communication with the outside world. Of greater interest is the development of technologies which are able to interact with us on a neural level. The most ubiquitous sensory neural prosthesis is by far the cochlear implant (Zeng, 2004). Where destruction of cochlea hair cells and the related degeneration of auditory nerve fibres has resulted in sensorineural hearing loss, the prostheses is designed to elicit patterns of nerve activity via a linear array of electrodes implanted in the deaf patient's cochlea that mimics those of a normal ear for a range of frequencies. Current devices enable around 20 percent of those implanted to communicate without lip reading and the vast majority to communicate fluently when the sound is combined with lip reading. Its modest success is related to the ratio of stimulation channels to active sensor channels in a fully functional ear, with recent devices having up to 24 channels, while the human ear utilises upwards of 30,000 fibres on the auditory nerve. With the limitations of the cochlear implant in mind, the artificial visual prosthesis (Hossain *et al.*, 2005) is certainly substantially more ambitious. While degenerative processes such as retinitis pigmentosa selectively affect the photodetectors of the retina, the fibres of the optic nerve remain functional, so with direct stimulation of the nerve it has been possible for the recipient to perceive simple shapes and letters. However, the difficulties with restoring full sight are several orders of magnitude greater than those of the cochlear implant simply because the retina contains millions of photodetectors that need to be artificially replicated, and so this technology remains in development.

While both cochlear implants and retina stimulators operate by artificially manipulating the peripheral nervous system, less research has been conducted on direct electrical interaction with the human central nervous system, and in particular the brain. Work on animals (Olds and Milner, 1954), (Talwar *et al.*, 2002) has demonstrated how direct brain stimulation can be used to guide rats through a maze problem, essentially by reinforcement, by evoking stimuli to the cortical whisker areas to suggest the presence of an object, and stimulation of the medial forebrain bundle (thought to be responsible for both the sense of motivation and the sense of reward) when the rat moves accordingly. Early work to translate this research to humans demonstrated radical (and occasionally dubiously interpreted) changes in mood and personalities when such 'pleasure centres' were stimulated (Moan and Heath, 1972), (Delgado, 1977). This period saw some seventy patients implanted with permanent micro-

stimulators to treat a variety of disorders with reportedly good success, although the indiscriminate use of the procedure and significant failure rate saw it largely condemned. This may have been in part because the disorders targeted were psychiatric rather than neurologic, and it was not until the 1980s, when French scientists discovered that the symptoms of Parkinson's disease (PD), with better understood anatomical pathology, were treatable using Deep Brain Stimulation (DBS), that research again picked up pace. However, difficulties in accurately targeting structures deep in the brain, lack of safe durable electrodes, problems of miniaturising electronics and power supply limitations meant that such therapy was not readily available for several more years.

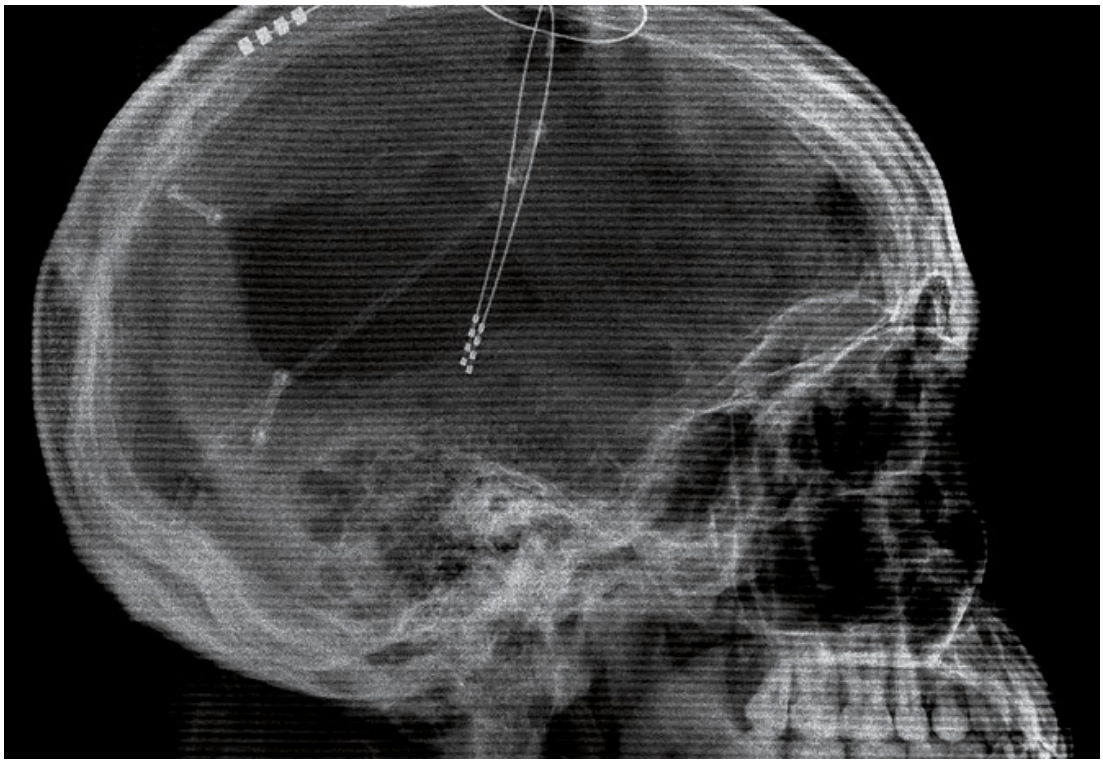

Figure 1: A lateral X-Ray of the head of a 38-year-old showing two Deep Brain Stimulation leads implanted in the sub-cortical thalamus area

Recently there has been a resurgence of interest in the surgical treatment of movement disorders such as PD. This is because of the disabling side effects of long term treatment with L-dopa, a chemical precursor to dopamine which can cross the blood-brain barrier and metabolise in the brain to address insufficient dopamine levels, thought to be a primary cause of PD. Also many movement disorders, such as multiple system atrophy or dystonia, do not respond to dopaminergic treatment at all. A limited range of DBS systems have been made commercially available and are now in clinical use despite their significant cumulative costs. Deep brain electrodes are routinely implanted into the thalamus, pallidum or sub-thalamic nucleus to alleviate the symptoms of Parkinson's disease, tremors of multiple sclerosis and dystonia. In pain patients, electrodes are implanted into the sensory thalamus or periventricular / periaqueductal grey area (see e.g. Figure 1). The depth electrodes are externalised for a week to ascertain effect prior to internalisation. A control unit and battery is

implanted in the chest cavity and the electrode connections internalised after this time if good symptom relief is realised, at a cost of around £12,000.

At present DBS is used to stimulate deep brain structures continuously at high frequencies (typically 100-180Hz for movement disorders and 5-50Hz for pain). Such high frequency DBS is probably effective because it takes command of the local networks and prevents them from relapsing into the slow synchronous cycles that may cause the symptoms of the disorder. The corollary of this is that when entrained to continuous deep brain stimulation the basal ganglia neurons are probably unable to perform their normal functions. However, the success of DBS as a treatment for the symptoms of movement disorders, combined with an improved understanding of the pathophysiologic basis of neuropsychiatric disorders has now seen renewed interest in the application of DBS for these conditions (Wichmann and DeLong, 2006).

The ability of electrical neural stimulation to drive behaviour and modify brain function without the recipient's cognitive intervention is evident from this type of device. Further, it has been demonstrated how electrical stimulation can be used to replace the natural percept, for example the work by Romo *et al.* (Romo *et al.*, 2000). However, in all cases these devices operate in a unidirectional fashion - the ability to form direct bi-directional links with the human nervous system certainly opens up the potential for many new application areas. Nevertheless, bi-directional neural implants are very much experimental. Whilst they have much potential in the areas of prosthetics, major developments have been slow in coming. Recent research in the area of DBS has shown that by recording brain activity via the implanted electrodes it is possible to detect characteristic signal changes in the target nuclei prior to the event of tremor, and so stimulation based on a prediction of what the brain will do is possible (Gasson *et al.*, 2005). The development of such technologies, which are able to decode the brain's function, are clearly of great value.

3.2 Application of ICT implants for Enhancement

On Monday, August 24th, 1998, a groundbreaking experiment was conducted by Prof. Warwick's group at the University of Reading in the UK (see Figure 2). At the heart of this work were the sub-dermal implantation of a Radio Frequency IDentification (RFID) tag[4] and the augmentation of the infrastructure at the university's Department of Cybernetics with RF nodes such that the system was able to track him, via the tag, as he roamed the building. The possibilities using this technology were, even at that time, not greatly limited, however the system was restricted to simple profiling of his behaviour. From this automated customisation of his environment was possible, such as unlocking doors, turning on lights and brewing his coffee on arrival.

While the public response to this work was varied, from suggestions that this was the work of the devil,[5] to awe of the technological possibilities, acknowledgement of the prophetic merit

[4] In brief, RFID tags wirelessly communicate data to reader devices from which typically the power is supplied wirelessly to the tag. The data, in the simplest devices, is a unique code which identifies the tag, and thus the object, if known, to which it is attached – see section 4.1.

[5] Revelation 13:16-18 "He [the beast] also forced everyone, small and great, rich and poor, free and slave, to receive a mark on his right hand or on his forehead, so that no one could buy or sell unless he had the mark, which is the name of the beast or the number of his name". Such scaremongering is in keeping with the flawed

largely mirrored that of academic musings on the scientific value. Few could appreciate the idea that people may actually be open to having such devices implanted if there was some net benefit in doing so. Equally, few entertained the realisation that, at that time, RFID technology was on the cusp of becoming cost effective enough to essentially become ubiquitous.

Figure 2: A 2cm long RFID tag (shown right) is invasively implanted into a healthy volunteer during a research program conducted in 1998.

Some six years later, implantable identifying RFID tags were commercialised by 'VeriChip' and approved by the FDA in the USA for human use. It was proposed that these devices could essentially replace 'medic alert' bracelets and be used to relay medical details when linked with an online medical database. Such devices have subsequently been used to allow access to secure areas in building complexes, for example the Mexican Attorney General's office implanted 18 of its staff members in 2004 to control access to a secure data room, and nightclubs in Barcelona, Spain and The Netherlands use a similar implantable chip to allow entry to their VIP customers, and enable automated payments.

By 2007, reports of people implanting themselves with commercially available RFID tags for a variety of applications have become a familiar occurrence (see e.g. Figure 3). The broad discussion on security and privacy issues regarding mass RFID deployment has picked up pace, and security experts are now specifically warning of the inherent risks associated with using RFID for the authentication of people[6]. Whilst the idea that RFID can be used to

logic which demonstrates that the common barcode contains a hidden '666', e.g. as described by Relfe in her 1982 book "The New Money System: 666".

[6] RFID technology is still in its infancy and resource-constraints in both power and computational capabilities make it hard to apply well understood privacy protection techniques that normally rely heavily on cryptography (see section 4.1.4 for more information). For instance a 'man-in-the-middle' attack would make it possible for an

covertly track an individual 24-7 betrays a fundamental misunderstanding of the limitations of the technology, there are genuine concerns to address. The use of implanted RFID tags in this scenario is especially thwart with issues because being implanted forms a clear, permanent link with the individual and makes compromised tags hard to revoke.

Figure 3: An individual with two RFID implants: His left hand contains a 3mm by 13mm EM4102 glass RFID tag that was implanted by a cosmetic surgeon, his right hand contains a 2mm by 12mm Philips HITAG 2048S tag with crypto-security features, implanted by a GP using an animal injector kit (Graafstra, 2007)

Concerns for those who have decided to have an RFID tag implanted are valid, although an assumption is that such procedures will never become compulsory and so most people will remain unaffected. However, while mass deployment of RFID technologies is well documented, especially in the context of commerce, it should be noted that, through non-nefarious means, it is possible that people could become implanted with RFID unknowingly. This is mostly related to safety issues regarding passive medical devices such as hip replacements and breast implants whereby being able to determine the exact manufacturing details non-invasively could be advantageous. This is especially valuable when manufacturing faults are subsequently discovered and devices of unknown provenance have been used. Thus embedding an RFID enabled device before it is surgically utilised would enable this function, but result in the wider issues of having RFID implanted. Further, following the polemic on

attacker to steal the identity of a person (i.e. tag identifier), while widely published techniques for RFID tag cloning make utilising this information technically feasible.

silicone-gel breast implants (Kessler, 1992), a device based around RFID technology, designed to be located inside the breast, which detects rupture has been developed, and many are investigating the benefits of being able to non-invasively monitor the condition of a medical device, such as a heart valve, using this type of technology.

Exact numbers of those who have received this type of low-tech implantable technology are not known, but it is clear that the figure is rising, and, with familiarity, public acceptance will surely grow. Because we largely dismissed such uses of the technology as improbable some ten years ago, a lack of timely debate on the wider implications means that we are now faced with the prospect of addressing them whilst the technology gets a foot-hold. Not least of all, this certainly leaves some open identity management questions which technologists must now address. It is not hard to imagine that dealing with technical and wider issues retrospectively will be immensely more difficult.

Having seen the applications which RFID has found despite earlier pessimism, we should consider the application of the more advanced medically orientated technologies on healthy individuals, i.e. enhancement rather than restoration, as a distinct probability. Reports of this pioneering step are rare, although in a notable echo of 1998, the University of Reading in the UK has been active in this area. On March 14th, 2002, an array of one hundred individual needle electrodes was surgically implanted into the median nerve fibres of the left arm of Prof. Warwick, a healthy volunteer (Gasson *et al.*, 2005), (Warwick *et al.*, 2003). This study demonstrated, in a rudimentary fashion, a range of applications, from nervous system to nervous system communication, feedback control of robotic devices and augmented sensory capabilities.

To date there are no well reported studies involving implantation in the central nervous system of healthy volunteers. There is, however, some largely anecdotal evidence of the occasional positive side effect that DBS in patients has had. In one such case, a graphic designer, who received DBS surgery for a severe Tourettes disorder, found that stimulation through one specific electrode could actually make her more creative. Indeed, when this electrode was used, her employer noted an improvement in colour and layout in her graphic design work (Cosgrove, 2004). The application of this type of effect in the long term clearly cannot be discounted, and so nor can the translation of medical devices to this area.

To further the discussion the following chapter selects some of the implantable devices currently used in a variety of contexts, and analyses them and their security and privacy implications in more depth from a technical perspective.

4 Application cases of ICT implants

Having first looked at how the technology being developed in a medical context could in fact ultimately be applied to human enhancement, here we will examine in more detail the technicalities of a selection of specific case studies. These cases studies are drawn from the variety of commercially available devices currently in use, and will be described in line with the terminology stated in section 2.1. Note that it is not the intention that this chapter exhaustively covers the variety of categories previously defined, rather it aims to investigate identity related issues which are already manifesting in state-of-the-art devices and not those devices which are still largely theoretical.

4.1 Passive implants for identification

RFID technology was originally developed for automatic identification of physical objects. An RFID tag, a small device attached to the object, emits identification data through radio waves in response to a query by an RFID reader. This information is captured by the reader and then further processed. RFID technology is already employed as barcode replacement offering a number of advantages. It is increasingly used in production and the logistics chain of enterprises and is starting to penetrate the medical and healthcare sector, defence, agriculture and other domains. Both industry and governments are promoters of RFID technology. All EU Member States, the US and many other countries are gradually deploying electronic passports. These passports contain RFID tags that store personal data, including the owners' biometrics. This allows for semi-automatic authentication of people at borders. Credit-card-sized contactless smart cards, based on RFID technology[7] are also becoming increasingly popular for access control. While some RFID-enhanced smart cards contain only identification numbers, others include additional cryptographic security features to protect the data during transmission. More sophisticated RFID-based devices not only identify, but can also be used to track people's location and activities (Smith *et al.*, 2005). RFID implants are RFID tags that are introduced into the human body. These devices are already commercialised and are specifically designed to facilitate the identification and authentication process.

RFID implants for identification and authentication of people provide some potential advantages compared to more established methods. The identification process is fully automatic and is thus more convenient. The user is not required to take any action, and there is no need to type or confirm any information or to remember to carry a token. The user does not have to have clean hands, as she would when using a fingerprint scanner, or to stand still without blinking, as she would have to when having her iris image captured. Identification and authentication with an RFID implant is practically immediate, whereas with other technologies time is required for typing passwords, for acquiring and matching of biometrics or for taking a smart card out of a wallet. Implants are a reliable method of identification, especially when compared to biometrics, which due to the statistical nature of their matching process cannot guarantee error-free results[8]. Implants are more durable than tokens and many types of biometrics, which usually change during a person's lifetime. Unlike tokens, implants

[7] For example see Mifare, www.mifare.net

[8] See for more detail FIDIS deliverable D6.1 'Forensic Implications of Identity Management Systems' and D3.10 'Biometrics in identity management'.

cannot be lost or stolen (unless an attacker physically assaults a user to extract the implant). RFID implants can be used by everyone without exception, including people with cognitive impairment. The user will always be identifiable, even if she is unconscious or not carrying any identity documents.

RFID implants are passive tags, i.e. they do not require batteries to operate but make use of the energy emitted by the external RFID reader. As a result, and since they have no moving parts and are largely biocompatible, once implanted under the skin they can be operational for many years (typically at least 10 years, although some manufactures claim over 40 years). Their extremely small size and lack of any internal power source limit the devices' performance in terms of memory, processing power and communication range. The hardware limitations make it difficult to design RFID implants with advanced authentication methods. They also have limited communication range. However, this can be seen as an advantage from a security and privacy point of view.

4.1.1 Application I: Access to VIP areas in a night club in Barcelona

Probably the most cited example of human implanted passive identifiers centres around a night club in Barcelona, Spain,[9] which proposes to its 'most valued' customers the use of an ICT implant to gain several benefits while they are in the club. The device implantation, using a syringe type delivery system, is made onsite by a trained employee of the night club. The implant not only grants the customer access to VIP areas, but can also be used as a payment method. Every waiter and waitress is equipped with a scanner which, during the payment procedure, registers the identity of the customer and charges her account (e.g. a credit card) with the cost of the drinks ordered.

While this system has been successfully utilised for some time now with apparently little or no expansion of the system's core purpose, the possible use of information which can be generated through further 'silent' capture and processing of the tag's, and thus person's, location warrants discussion. Using such a system, one may infer with enough precision the habits of a customer and thus it is, in principle, possible to establish a profile of each user – or each group of users – which for example might indicate:[10]

- The frequency of the visit of each customer
- The times of the year that the customer is in the region
- The usual time when the customer visits the night club (beginning of the evening or end of the night) and the duration of these visits (even if the customers are not scanned when they go, using the time of their last order, one can estimate when they left).
- The type of drink she has ordered and their quantity. This information is contained within the bills that the customer has paid. One may even deduce if the customer has an inclination to alcoholism (but one should remember that typically in a night club there are not many people drinking juice).

9 See: http://www.baja-beachclub.com/bajaes/asp/zonavip2.aspx
10 Note that the points hereafter are speculation on what *could* be done with the data.

- Based on the number of drinks the customer has paid within some time slot (when she pays for a round of drinks for example), one could estimate how many people she is with. A customer who regularly invites many people may be considered a "prescriber", may have a higher influence on other people, and is of interest to the club. On the other hand, a customer who is always alone may be of less interest.

- Considering the events organised by the club at the time the customer was present, one can deduce the kind of activities she likes (musical preferences, the shows she likes, etc). This parameter is even more important if the customer is a "prescriber". This could be used to determine the kind of advertisements she should receive.

If one goes some steps further, one can imagine the building augmented with several scanners which could be used to characterise the person based on their movements around the club, and their proximity to other tagged individuals. There are other examples along similar lines, see for example (Eudes, 2006).

4.1.2 Application II: From identifying animals to tracking people

For some time the implantation of domesticated animals with passive identifiers has been obligatory in some EU countries. In these cases, the implant is typically placed by a veterinarian in the scruff of the neck of the animal. However, the rationale of using such a passive identifier device is varied depending on the context, e.g. farm animals versus pets. For domesticated pets, by having an implant which cannot be removed, if the animal is lost or stolen and subsequently found, the owner can be identified. Furthermore, because it is more difficult to "erase" or falsify than e.g. a tattoo, it is considered to be more reliable. In Switzerland, for example, this kind of implant is mandatory for every dog born after the 1st of January 2006 and it is likely that the law will be extended to cover other animals such as cats.[11] Being a simple RFID passive identifier, the data held by the device is limited. Essentially it contains a unique identifier which, in the case of Switzerland, can be used as an access key to a centralised database of dog owners called ANIS[12]. All subsequent data is stored in the database and not on the chip itself.

Identification tags are also used for livestock management. A typical application is the automatic detection of which cow is being milked at a given milking bay, in order to collate data on e.g. volume of milk and notable elements of the composition in a database. Such data may in turn be used to automatically formulate an appropriate food mix for each cow depending on deficiencies in its milk. It could also potentially automatically administer medication via the food mix to a specific animal, based on an automatically detected or previously determined disease. In the agricultural sector, many applications of this kind are being developed and used.

Whilst having been applied for the management of animals in several instances, the drift towards application areas for humans has become well established. In October 2004, the first

[11] See the official communication of the Swiss federal veterinarian office (in French) http://www.gstsvs.ch/files/presse/FAQHundechip_f.pdf

[12] ANIS is hosted at http://www.anis.ch and stands for Animal Identification Service AG, a non-profit organisation supported by several associations like the Swiss association of veterinarians, etc.

RFID implant for human use – the so-called VeriChip[13] – obtained approval from the US Food and Drug Administration. The VeriChip implant, essentially an RFID tag similar, but smaller to that described in section 3.2, stores a unique identification number, and can be read from a distance of up to 10-15 cm.[14] The ID number is long enough to be able to create enough devices to uniquely identify everybody in the world. Other data related to the owner are not stored on the implant itself, but, again, in a centralised database. The first commercial application, known as VeriMed, is designed to identify patients in a healthcare context. An authorised user, e.g. a doctor, can access a patient's medical data (although note only the data held on the VeriMed database which is unlikely to be their entire medical record) through a password-protected website, using the patient's implant ID number, detected by an RFID reader, as the database key.

The application drift of this technology is likely to continue. In the healthcare context, it has been proposed that for a person suffering from a disease such as epilepsy or Alzheimer's, it could be preferable for them to be tracked around their environment. In these cases it would be possible to, e.g., detect if a person had left their 'safe' environment, determine if mediation had been taken, or if a person had fallen. It should be noted that implantation is not necessary for such applications, but exactly like the animal scenarios, it is preferable if the device simply cannot be removed or lost. In a further application area, the use of RFID implants as replacements for externally attached devices used to localise or register the movements of prisoners are being discussed.[15, 16]As mentioned in section 3.2, an RFID tag, implanted or not, cannot be utilised as a global tracking device without a substantial infrastructure being put in place at prohibitive cost. However, future implant technology may incorporate transmitter modules (using e.g. ultra-wideband) for applications such as tracking children or prisoners.[17]

4.1.3 A summary of RFID implant application areas

The automation of the identification and authentication process is probably the major driver for RFID implant deployment. It could make existing services faster and more convenient and will allow for further services and applications. Indeed, the feature of fully-automated identification and potentially continuous detection of person's presence is valuable. Given the inherent limitations of the functionality of the passive RFID devices, the main potential areas of application for RFID implants can be grouped into:

---

[13] See :www.verimedinfo.com

[14] The VeriChip has been designed to operate at a distance of about 10cm with a handheld reader and 50cm with a door reader but cannot operate over very large distances. Simulations (see e.g. Z. Kfir and A. Wool "Picking virtual pockets using relay attacks on contactless smartcard systems.") and practical experiments (see G. Hancke "A Practical Relay Attack on ISO 14443 Proximity Cards.") show that a standard distance can be increased several times (up to 0.5m for ISO 14443), but with further increase the signal disappears in the environment noise.

[15] "UK jails considering RFID implants for prisoners" http://www.engadget.com/2008/01/14/uk-jails-considering-rfid-implants-for-prisoners/

[16] "Proposal for UK Prisoners to be Given RFID Implants" http://yro.slashdot.org/article.pl?sid=08/01/13/1324217&from=rss

[17] For further examples and general discussion on using RFIDs for identifying living organisms see also http://www.caslon.com.au/rfidprofile3.htm

1. Applications not requiring strong security

There are applications which require the identification of users but strong measures against identity theft are not necessary. Here, RFID implants may replace other technologies simply because they are more convenient, as identification through the implant is immediate, does not require any action from the user and the implant cannot be forgotten, lost or accidentally destroyed. Examples include the Baja Beach Club in Barcelona, described above. The use of RFID implants for such applications should be seriously debated, since the advantages may not outweigh the ethical, privacy and health concerns that the use of RFID implants entail. The question here is: Is it worth being chipped in order to avoid e.g. queuing for a drink? The choice lies of course with each one of us, but it should not be a mandatory solution for such environments.

2. Identification and authentication in secure environments

In closed environments, such as restricted workplaces, the identity of employees is verified at the entrance and strong authentication of people who are already inside is usually not necessary. In such situations, RFID implants can help prevent authorised people from supplying their credentials to unauthorised users. In highly protected environments where security concerns prevail over privacy (e.g. nuclear power stations) implant-based systems could also facilitate continuous monitoring of the location of workers. For instance, employees' movements from one room to another could be tracked by placing RFID readers in all doorways, so in the case of an accident, the location of every worker is known. RFID implants may also be used in secure, but more open environments like hospitals. They would help to prevent access by unauthorised people to certain instruments, restricted places, or to patients' medical files. In such environments, RFID implants facilitate the identification of a person. Where strong authentication is required, RFID implants can be complemented with other identification and authentication technologies, like PINs/passwords, tokens and/or biometrics. It should be noted that many RFID devices, including the commercialised VeriChip device, have been shown to be susceptible to cloning – i.e. the duplication of the 'unique' identifier in another device (Halamka *et al.*, 2006). As such it has been proposed that implanted RFID tags are only ever used for identification, and not authentication. Despite this, in 2004, more than 100 employees in the organised-crime division of the Mexican Attorney-General's offices received implants giving them access to restricted areas.[18] In 2006, an Ohio-based company had chips implanted into some of its employees.[19] CityWatcher.com, a private video surveillance company, uses the technology for controlling access to a room where it holds security video footage for government agencies and the police.

3. Identification and authentication in non-secure environments

RFID implants in combination with established identification and authentication technologies can provide additional security. They could protect systems from accepting PINs/passwords obtained by theft, or which have been cracked or disclosed without authorisation. Similarly, the RFID implants may reduce the risk of false authentication with a stolen token or with one which has been loaned by an authorised person to a third party, either willingly or as a result

---

[18] *Implantable Chips Get Under Skin of Security Experts*. Available at: http://www.adsx.com/newsarticles/01.htm

[19] *US group implants electronic tags in workers* Financial Times, 12 February 2006 available at http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html

of blackmail. Prominent application fields are those where people are less willing to delegate their rights, e.g. withdrawing cash at an automatic teller machine.

Identification number read from an RFID implant may also be used to speed-up the process of biometric identification. To identify a person, his/her biometric sample must be compared with each sample in a database. The RFID implant could contribute to speeding-up the process by yielding an immediate and reliable identification (1:N), while biometrics would offer a strong authentication (comparing the user's sample with only one database entry, indicated by the RFID implant).

Finally, it is possible to deploy an RFID implant which would incorporate some biometric information (Perakslis and Wolk, 2006), so the user and implant authenticate each other mutually. It would be secure against a coercive attack as an implant extracted from a victim's body could not be used by another person (who has different biometric features). However, it would still be possible for an attacker to duplicate the identification number and modify biometric features.

4. Access control for mobile devices and services

Mobile devices, like portable computers, PDAs or mobile phones, store a growing amount of confidential information about their owners, and people are motivated to secure them. In existing devices, people are usually identified when they switch on the device. When a user leaves, the device still retains the authentication for a certain time period, during which an unauthorised person could get access. Here, an RFID implant can help. An RFID-based system can detect continuously the presence of the authorised person and demand a re-authentication when this person leaves the area covered by the reader. Thus, the additional security feature arises from the permanent identification through the proximity of the RFID implant. For high-security applications, the mobile device would identify a person by reading her RFID implant, and then the owner would authenticate to the device via a PIN/password or biometrics.

A 'smart weapon' is another example where the application of RFID implants could increase the security of a mobile artefact. On 14th April 2004, VeriChip, announced a partnership with gun maker FN Manufacturing to produce a police gun with an RFID reader embedded, so that the gun cannot be fired should it fall into the wrong hands. A digital signal unlocks the trigger when the scanning device inside a handgun identifies the authorised police officer, otherwise the gun is useless.[20]

5. Identification in healthcare

In the healthcare sector RFID implants might offer advantages for both medical personnel and patients. Vital information can easily and immediately be retrieved everywhere, even in cases where patients are unconscious and previously unknown.

The first commercial application, VeriMed – a system for patient identification and heath-care flow management described above – is apparently enjoying rapid adoption by a number of hospitals (620 in July 2007[21]). The system is especially recommended for people who suffer from cognitive impairment, such as Alzheimer's, or chronic diseases which put them at high

[20] "*No Chip in Arm, No Shot from Gun"*. Wired Associated Press, 14 April 2004, available at www.wired.com/science/discoveries/news/2004/04/63066

[21] According to their own website: www.verimedinfo.com

risk and instant identification of unconscious patients is crucial. On 7th August 2006, the first known life-saving incident involving a VeriChip was reported. Policeman W. Koretsky, a VeriChip subscriber, was rushed to a medical centre with head trauma following a crash during a high-speed police pursuit. In this case doctors were able to access his medical records in the VeriMed database, using the ID number retrieved from his VeriChip implant.

6. Smart environments

The Ambient Intelligence (AmI) vision assumes that people will be surrounded by intelligent interfaces that are embedded in a range of objects. These smart environments will be capable of recognising and responding to the presence of different individuals in a seamless, unobtrusive and often invisible way.[22] RFID implants could provide the interface between people and the smart environments. Let us take the example of the car. The car's RFID reader would read a person's ID, recognise that she has permission to drive the car, open the door, adapt the seat height and position the mirrors. Similar applications could also be thought of for other smart environments, like homes. Some people have already volunteered to have RFID tags implanted to experience ambient intelligence environments as discussed in section 3.2.

7. Other potential long-term applications

Up to now, the main purpose of wireless-based networks was communications, but recently the network data is increasingly used to provide location-based services (LBS). Examples of location-based services include emergency services (location of emergency calls by the fire brigade, medical rescue, etc) or local information services (finding the nearest restaurant, ATM, petrol station, etc.). Combining RFID implants with location-based systems may deliver new personalised services for people on the move. The communication range of RFID implants is limited to about 0.5 m (10-15 cm with a hand reader), but an intermediate device, e.g. a mobile phone equipped with an RFID reader, could provide a connection between the RFID implant and the network. The user would activate the interface device, e.g. a phone, to request a service via the wireless network and the RFID implant would provide the user's identification. In the long term, if a dense network of RFID readers were available, no 'bridging device' would be necessary.

The security issues relating to RFID in general have been well documented, especially those concerning cloning (Halamka *et al.*, 2006). However, the permanent and physical link between an RFID tag and a person makes RFID implants more susceptible to privacy risks than any other kind of contactless tokens (Rotter, 2008). These will be investigated in the next section.

4.1.4 Privacy threats and possible solutions for human implants

Many publications (Juels, 2006), (Garfinkel *et al.*, 2005) bring up the privacy issues regarding the use of RFID in several scenarios. The first part of this section aims to summarise their contributions and the second to discuss its applicability to human ICT implants. It should be noted that these issues are further elaborated in FIDIS deliverable D12.3 'A holistic privacy

[22] ISTAG Reports Grand challenges and Visions for the information society technologies is available at http://cordis.europa.eu/ist/istag.htm

framework for RFID applications', to which the interested reader is directed. Following this summary, we give an overview of the proposed solutions and how, if possible, they could be applied in an implant scenario.

4.1.4.1 Privacy issues in common RFID applications

Despite the advantages that the use RFID technology entails, privacy concerns stemming from its massive deployment causes concern in society and the academic community. In the last few years, the internet has been flooded with over 80 million pages related to RFID, from which 68% mention privacy concerns (Langereich, 2007). One of the main reasons why RFID tags pose special privacy concerns is the fact that they usually respond to any reader that interrogates them. This behaviour, combined with the fact that humans cannot sense the transmission used to perform the reading, makes RFID tags an ideal target for imperceptible eavesdropping. Besides, tags do not maintain a history of readings, thus they cannot be detected at a later time, reinforcing the undetectability of these transmissions. This promiscuity, together with the limited computational, storage and communication abilities of the tags, raises privacy concerns unique to the use of RFID technologies.

Secondly, most RFID tags responses include a *unique identifier*. Thus, even if any extra data a tag transmits is cryptographically protected, and no information can be extracted from it, the device (or person) carrying the tag can still be tracked. We note that even if this identifier is encrypted and resembles a random number to the eavesdropper, she could link repeated occurrences of the same tag, as the tag would always transmit the same random value. Besides, it is not uncommon that a person carries more than one tag. This creates a constellation of identifiers that can be linked amongst themselves and to the carrier. This situation worsens the risks associated with traceability by making it easier to do and more accurate.

RFID tags and RFID constellations pose a big threat for what is commonly known as location privacy. Here, the main goal is to prevent other parties from learning the current location and further movements of a person. By placing covert RFID readers in strategic places it is possible to monitor these movements. For instance, a company could place these readers inside its buildings, allowing the tracking of its employees, and use this information to make inferences about their productivity rates. As mentioned previously, it is not necessary to make these readers secret as RFID cards are often used to enforce access control to restricted areas. The information provided by these readers could already be used to extract information about employees' behaviour.

Moreover, when personal information and RFID tags can be linked, a person may be exposed not only to the danger of being tracked, but to further privacy invasions. For instance, when a payment with credit card is carried out next to an RFID reader the identity of the payer and the constellation of tags she carries can be directly linked. It may be the case that these tags reveal information about the products they are attached to, such as the type of product: clothes, mobile phone, medicaments, etc., or even more detailed information: aspirin, syrup, etc. These data can be used to infer personal information about the carrier (e.g., illnesses or preferences). The surveillance of a tag (or a group of tags) associated to an individual cannot only leak personal information but can also reveal the behaviour or intentions of that person. In a shop, the fact that a customer stops for long time in front of a shelf may reveal her

purchase intentions. Readers can be placed to detect this behaviour and the information can be exploited by shop assistants to increase the sales or to perform customer profiling.

It is important to realise that this association of identities and tags made in shops, companies, and so on is inexact, as they only take into account the "association" (i.e. a person is related to a tag) but not the opposite operation where a person breaks this association (loosing, throwing away, selling... the tagged item). This "eternal" association in databases may become a threat if the item is used afterwards for any malicious activity, for which the original owner may be incriminated.

Up to this point we have only considered commonly denominated *personal privacy threats.* However, RFID tags attached to goods also involve corporate *data security threats*, where the risk is shifted from the leakage of personal information to business sensitive information (espionage, marketing, etc.). As explained before, RFID tags are hailed as the future of product and merchandise identification. The fact that RFID technology does not require close physical proximity between reader and scanned objects, nor a line-of-sight between them, makes it ideal for inventory management. However, these characteristics might be a double-edge sword, by allowing third parties to spy on a business at different steps in the production. The threats stemming from RFID use in the production of goods are not limited to information theft and misuse. Finally, using RFID as core technology in the supply chain makes it susceptible to denial of service attacks, as radio frequency signals can be easily jammed to stop or at least complicate the full production process.

4.1.4.2 Specific privacy issues of RFID implants

The privacy risks affecting people with RFID implants slightly differ from the risks stemming from the use of other contactless tokens. To start with, none of the so-called *corporate data security threats* apply anymore because implants are not part of massive production processes. However, the aforementioned threats to personal privacy still concern implant users. Moreover, the fact that RFID implants are *permanently* linked to a person make them especially susceptible to privacy invasions and, in some cases, this persistent connection may even worsen the situation, exposing the RFID users to physical danger.

When talking about RFID implants, the undiscriminating behaviour of RFID tags with respect to any reader becomes crucial. Such implants answer any reader's request - usually with a message containing its unique identifier (we recall that encryption is not a solution for this problem). This identifier can, in this case, be linked with absolute certainty to a physical person, contrary to other tokens where this association cannot be ensured. For instance, people may share access cards, car keys, etc. which helps 'hide' the actual owner of the token. However, when the token is implanted, the anonymity set of possible owners is reduced to one, facilitating traceability.

Permanent identifiers associated to people make constellations of RFID tags more dangerous to privacy. As in the previous case, the fact that RFID tokens can be exchanged prevents inferences about identifiers appearing in two or more constellations. On the contrary, if the identifier of an implanted tag is part of two constellations, it can be used as evidence that in both cases the same physical person was detected.

These drawbacks are also very important when speaking about location privacy, or further inferences about private information that can be derived from a tag constellation (e.g., use of a

product/medicine). Again, the fact that a tag is uniquely related to a person makes it easier to extract information and use it afterwards. Nevertheless, the permanent association of tag/user may become an advantage in scenarios where users need to prove their presence in some place, or to avoid false incriminations stemming from the misuse of contactless tokens. However, in such scenarios, one has to consider that these tags can be cloned, and as such this may not be of any benefit.

Finally, the use of implants for authentication purposes, for instance in an access control environment, may result in physical damage to the user. An attacker may want to extract the implant from the body, or even tear it apart if necessary (Kent, 2005). It has been argued that the solution to this problem lays in either allowing easy cloning of the devices (Halamka *et al.*, 2006) or limiting its use to identification.

4.1.4.3 Proposed Solutions

Privacy advocates and researchers have extensively studied the threats to privacy that RFID introduces. Although many solutions have been proposed, none of them seems to fulfil their expectations.

As a first measure, RFID tags can be 'killed', i.e. the ability to communicate with a reader can be permanently disabled (Garfinkel *et al.*, 2005). However, when this killing operation should take place is not clear. When RFID tags are used as Electronic Product Codes (EPC), they could be disabled at point-of-sale. This would solve most of the privacy-related problems, yet, would also hinder further applications of these tags, e.g. smart refrigerators, destroying any possible post-purchasing benefits for the consumer. In the case of implants, this solution makes little sense as having a 'dead' implant is equivalent to not having it at all.

A second option is to 'sleep' the tag rather than completely disabling it. When applying this solution, one has to take care to introduce a mechanism to ensure that only authorised readers can wake up the tag. This could be achieved by means of a PIN, or more complex methods (Stajano & Anderson, 1999). Sleeping strategies could be applied to ICT implants, but implant bearers would need to take care of the PIN. Note that if PINs are not secretly stored, the method is not effective anymore, and to some degree this additional level of user interaction defeats some of the purpose of the device.

Juels *et al.* proposed the Blocker tag in (Juels *et al.*, 2003). In this scheme, tags contain what is called a modifiable 'privacy bit'. If this bit is set to '0', the tag behaves normally, thus responding to any reader that interrogates it. If the bit is set to '1', the tag is considered as private. Once tags are categorised, a "blocker tag" will prevent private tags from being scanned. Again, this solution could be applied to ICT implants, however, its security is not completely assessed and blockers cannot guarantee full protection (Rieback, 2005).

Finally, privacy could be protected through policies (Juels & Brainard, 2004), (Garfinkel, 2002), that do not prevent undesired scan of the tags but make the detection of these scans easier. However, these techniques rely on the good will of providers and customers and cannot be seen as an ultimate solution for privacy invasions derived from the use of RFID tags.

4.1.5 Medical concerns of RFID implants

Potential medical risks of implanted RFID tags have been analysed by the US Food and Drug Administration (FDA). The FDA saw no major risk and gave clearance for the commercialisation of the VeriChip RFID implants, although it points to some potential medical issues: "adverse tissue reaction; migration of the implanted transponder (…), failure of implanted transponder; failure of inserter; failure of electronic scanner; electromagnetic interference; electrical hazards; magnetic resonance imaging incompatibility; and needle stick".[23]

On 8th September 2007, an article "Chip Implants Linked to Animal Tumors" published by the Associated Press reported on several studies, dating to the mid 1990s, which indicated cases of cancer in laboratory rodents that were injected with RFID implants. The quoted percentage of rodents which developed tumours differs from report to report, from 1 to even 10%.[24] Curiously, the head of the Department of Health and Human Services, which oversees the FDA, became a member of the VeriChip board after the approval, raising questions whether the approval was objective. The FDA would not reveal which studies were reviewed before they took a decision to approve the implant, or whether the abovementioned reports were taken into consideration. VeriChip claimed that the company was not aware of them.

It is argued (Wustenberg, 2007) that observations presented in the cited studies do not imply any risks for people implanted by RFID. The main arguments are that tumours among laboratory rodents can often be caused by just the injection itself. During the past 15 years millions of dogs and cats have been injected with RFID implants and only one case of cancer at the site of the implant was reported, although it seems probable that many were not examined in this way, or reported. It is also argued that, so far, no health problems related to implants were found among 2000 people injected by VeriChip.

A recent review by the consumer privacy protection organisation CASPIAN found conflicting results in the literature.[25] However, as the probability of causing cancer appears to be very small, they recommend leaving the implant in injected pets. For people already implanted, they leave the decision to remove it to the individual. Given the risk / benefit trade-off of having an RFID implant, clearly more research in this area is needed.

4.2 Active implants for restoring function

Implantable Medical Devices (IMDs), such as pacemakers, have been used for years as lifesaving devices. They have become increasingly sophisticated and multifunctional. The operation of such devices is not necessarily based on a routine that is periodically repeated - some actions are performed automatically as a result of a continuous monitoring of the

[23] "Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information." U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, December 10, 2004, http://www.fda.gov/cdrh/ode/guidance/1541.pdf

[24] Studies on larger population indicated lower percentage (1% among over 4200 mice, while 10% among 177 mice).

[25] Albrecht, K. Ed. "Microchip-Induced Tumors in Laboratory Rodents and Dogs: A Review of the Literature 1990–2006". Available at: http://www.antichips.com/cancer

patient's body with sensors embedded in the IMD. With such devices, there is usually a need for two-way communication between IMDs and the external world. In this sense these are devices which, by the terminology outlined in section 2.1, are *offline* implants which are capable of, but not dependent on, communicating with other remote devices.

Data can be sent to the implanted device in order to program its parameters or to trigger a specific action on demand. The device may in turn send data, for example the history of any measured characteristics or a log of device actions, which can be externally analysed. The most effective way of such communication is through wireless, radio transmission. However, such communication can raise concerns about privacy and security.

The main communication functions of IMDs are (see Figure 4):

- Communicating the presence and type of device to medical staff
- Deactivation of the device on demand, e.g. before an operation
- Sending collected measured medical data (e.g. EKG, body temperature) and data on the history of the device operation to help in the diagnostic process[26] and the auditing of the device's operational history
- Configuration of the device
- Manual control over the device
- Upgrade of the software included in the device

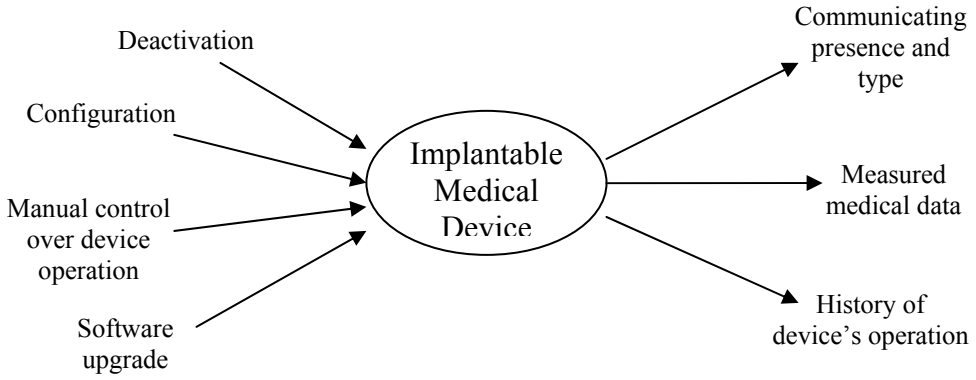

Figure 4: Communication of a generic IMD with the external world, showing the directional flow of information

4.2.1 Application 1: Pacemakers and Cardiac defibrillators

While both pacemakers and cardiac defibrillators, pager sized devices implanted in the chest, are used to treat abnormal heart conditions, they have notably different applications. The primary purpose of a pacemaker is to maintain an adequate heart rate, either because the heart's native pacemaker is not fast enough, or because the electrical system controlling the heart has failed. The pacemaker continually monitors the heart activity, and so when an

[26] Some modern IMDs offer the possibility of on-line home monitoring: data received wirelessly from the IMD by the base station are passed through a website to a doctor.

abnormal heartbeat pattern occurs, it can stimulate the ventricle of the heart via an implanted electrode lead with a short electrical pulse. An implanted cardiac defibrillator (ICD), on the other hand, is used in patients who are at risk of sudden cardiac death due to ventricular fibrillation. By detecting cardiac arrhythmia, it can revert both atrial and ventricular arrhythmias as well as perform biventricular pacing by delivering electrical stimulation. Some devices combine a pacemaker and cardiac defibrillator in a single implantable unit.

Pacemakers and cardiac defibrillators typically consist of a sealed, battery powered, sensor-laden pulse generator, several steroid-tipped wire electrodes that connect the generator to the heart muscle, and a custom ultralow-power microprocessor, typically with about 128 Kbytes of RAM for telemetry storage (Israel & Barold, 2001). The device's primary function is to sense cardiac events, execute therapies, and store measurements such as the history of the device's operation. Modern devices communicate wirelessly and are programmable to allow the cardiologist to select optimum parameters for individual patients post-implantation. Device manufacturers also produce at-home monitors that collect data from the implanted devices through the wireless channel and relay it to a central repository, accessible to doctors via an SSL-protected website.

4.2.2 Application 2: Deep brain stimulators

In the neurotechnology field, deep brain stimulation (DBS) is a surgical treatment involving the implantation of a medical device which sends electrical impulses to specific parts of the brain. DBS in select brain regions has provided remarkable therapeutic benefits for otherwise treatment-resistant movement and affective disorders such as chronic pain, Parkinson's disease, tremor and dystonia. Typical DBS systems consists of: the electrode implanted in the brain with its tip positioned within the targeted area, an insulated wire extension which is passed under the skin of the head, neck and shoulder and connects the electrode with the neurostimulator, also containing the battery, which is implanted under the skin near the collarbone. Once the stimulator is fully connected it delivers a continuous electrical pulse to the targeted brain area via the electrode. The general therapeutic stimulation parameters of the pulse have been derived primarily through trial and error. This has been possible in disorders such as Parkinson's disease as the effects of DBS on symptom alleviation manifest quickly – in contrast to other disorders (McIntyre, 2004). However, despite the increasing successful clinical use of DBS, its mechanisms of operation are still unclear. Further to this, continuous electrical stimulation does not allow the targeted brain area to engage in normal function. In addition, patient quality of life is adversely affected by repeat operations (every ~3 years) to replace stimulator batteries as a direct result of continuous stimulation. This is costly in terms of time and money and currently severely limits the number of people able to undergo this highly successful treatment. Because of this, neurophysiologists, bioengineers and signal analysts, are currently collaborating to develop a device that is able to utilise predictive brain activity to trigger the stimulator. Such devices, in a similar but more complex way to cardiac defibrillators, will monitor the brain activity through the electrodes, and respond to abnormal patterns of activity with electrical stimulation to abort it. It is likely that the additional complexities involved with detecting such events will see computationally more complex devices being utilised verses current cardiac devices.

The ability to optimise stimulation parameters based on the changing pathophysiology of the disorder targeted is vital for the application of DBS technology. As such, the devices utilise

wireless communication channels in an almost identical fashion to those of the pacemakers and cardiac defibrillators.

4.2.3 Privacy and Security concerns

There are several substantial differences between RFID implants described in section 4.1 and Implantable Medical Devices:

- IMDs are not optional – usually the patient has no choice. On the other hand, identification implants (RFID tags) are implanted mostly for convenience or even for fun. Although it has been argued that RFID implants are lifesaving devices, clearly alternative solutions for identification exist such as wearable tokens (these need not necessarily be electronic).
- Insecure implementation of IMDs may provoke much more serious threats than in the case of identification implants implementation. Any malicious attack on IMDs if successful may directly threaten the life of the patient by for example changing the implant's parameters or triggering the device, e.g. causing defibrillation.
- The device itself, as well as communication with it, is much more complex than in the case of RFID implants.

Privacy and security risks related to RFID implants are analysed in Chapter 4.1.4. Below we present privacy and security risks related to the use of implantable medical devices. All risks listed below are related to radio communication between the IMD and external world.

Potential risks to the *privacy* of an individual include:

- Unauthorised scanning of people in order to detect the presence and type of medical implant
- Unauthorised reading of the device ID number, which can then be used for tracking of people
- Unauthorised reading of the patient's personal data, which are often saved in the device's memory.
- Unauthorised reading of medical data collected by the device, which gives insight into patient's health state.

Apart from privacy, there are several risks related to *security* including:

- Malicious modification of firmware or data stored in a device's memory
- Malicious modification of the device's configuration parameters
- Stopping the device from operating. This can be achieved by sending the instruction code which stops the device, or by a denial-of-service attack.
- Triggering a device into action which may threaten a patient's health and life, for instance by triggering defibrillation.

The risks to privacy and security are context-dependent. In every particular case only some items from the list above are relevant and specific analysis of risks should be performed for every individual application.

4.2.4 Security / accessibility trade-off

There is a trade-off between security and accessibility of the device, which needs to be seriously considered. For the sake of functionality, which can be crucial for a patient's life, especially in emergency situations, the communication with the device should be easy and free of limitations. For example, if an unconscious patient is brought to an emergency department in a foreign country, it is likely that the personnel will not be able to follow advanced authorisation procedures to obtain control over the device (Halperin *et al.*, 2008). On the other hand, requirements for privacy and security cannot be disregarded. The possibility of unauthorised access to the device, reading of the data and manipulation of the device by an unauthorised person is a serious risk to a patient's safety and privacy. Therefore there is a need to find a compromise between security measures and accessibility requirements.

4.2.5 Means of protection for IMDs

Basic means of protection against unauthorised access to IMDs are:

- Access control: Authorisation of specific people (patient, patient's doctor) or entities (ambulance staff) to perform specified operations on the device. Different operations may require different levels of authorisation, for example manual control over the device (including entering testing mode) is the most potentially dangerous.
- Requirement of authorisation via a secondary channel, for example by using near field communication to initialise the data transmission.
- A set of measures against denial-of-service attack, in particular against the overflow of the device memory, the draining of the battery power and the blocking communications.

Also some other measures can be applied for IMDs, as proposed in (Halperin *et al.*, 2008):

- Notification to the patient when the device exchanges data with an external reader through a secondary channel (e.g. vibration)
- Using an intermediate device for communication, which could be embedded e.g. in a smart phone, watch or belt. Then short-range communication between the IMD and the intermediate device could use light-weight encryption and authentication, while strong security could be applied for the exchange of data between intermediate device and external devices.

While such solutions would not be technically difficult to implement, it is currently the case that commercial products lack even basic access control, and so are significantly vulnerable to attack. Security through obscurity may work in the very short term, but other mechanisms need to be implemented.

It is clear from the case studies presented in this chapter that a range of human ICT implants are being developed and utilised, and they are bringing with them their own security and privacy implications. This is in the main because these devices are being developed without due consideration to these important aspects, in many case without even basic access control being implemented. However, in light of the personal data which can be contained within, and the possibilities for identification and utilisation by unauthorised people, it is clear that consideration needs to be made to these areas. This is clearly better addressed while the technology is still relatively immature.

5 A legal analysis of ICT implants

ICT devices can be implanted into the human body for a variety of reasons. As detailed in section 2.1, we can discriminate between implants that aim to *restore* or *repair* human capabilities, those designed for the *diagnosis* of a biological state, ones that *identify* a person in order to e.g. provide access to certain locations, information or knowledge, or to automatically pay/bill for services rendered and finally implants that aim to *enhance* human memory, vision, auditory perception, alertness or other capabilities. All these types of ICT implants may have significant differences from a technical point of view, but they all put some core human rights of the individuals at stake. The use of such devices implies an actual interference with the body of an individual that creates questions regarding her right to bodily integrity. These considerations will be analysed in section 5.1.

The use of ICT implants in the health sector seems to be more socially acceptable, than when the technology is used to enhance the existing normal functioning (Warwick, 2002). In the advent of the era of electronic health records, implants can serve various roles and can be potentially useful in cases of medical emergencies (Gadzheva, 2007). Notwithstanding the fact that being able to get real-time information about the medical condition of patients with serious medical problems can prove helpful when the person is in crisis, there are several arguments raised by the opponents of human implants. An implant will allow an at-all-times *data*veillance[27] of the person (Clarke, 1997), while the same benefits can be achieved by the use of an electronic bracelet that can be easily removed, according to the wishes of the person[28].

As already discussed in Chapter 4, human implants impose a number of personal privacy threats. The fact that ICT implants are *permanently* linked to a person makes them especially susceptible to privacy invasions and allows the constant tracking and tracing of the individuals that carry them. RFID tags, in particular, usually respond to any reader that interrogates them, thus putting in danger location privacy (4.1.4.1). The systematic reading of an ICT implant can allow inferring with enough precision the habits of an individual and thus it is, in principle, possible to establish her profile, as already illustrated in 4.1.1. These privacy and mainly data protection issues that arise via the use of ICT implants will be presented and discussed in section 5.2.

5.1 Implants and human rights, in particular bodily integrity

The deployment of human implants has induced various implications for human rights. One of the most crucial rights at issue is the right to bodily integrity, and so, this contribution largely centres on this specific right, which has a twofold character. On the one hand it implies the right to prevent one's body from being harmed by others, while on the other hand it constitutes a right to do with one's body whatever one wants; a right to self-determination. Even though the right has only been included in Constitutions fairly recently,[29] it may already

[27] According to Clarke: "Data Surveillance (or Dataveillance) is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons".

[28] See for instance the King County's Project Lifesaver program, at http://www.kingcountyprojectlifesaver.org/

[29] See for example, Art. 2 para. 2 of the German Constitution and Art. 11 of the Dutch Constitution; cf. also Ch. 2, Art. 6 of the Swedish Instrument of Government (a part of the Swedish constitution).

be influenced by unforeseen developments in the field of technology. Biotechnology, nanotechnology, and RFID have become part of society and are gradually influencing our daily lives. These technologies can also be connected to or implanted in the human body. The purposes of implants can vary from strictly medical purposes, via aesthetic purposes, to human enhancement.

The development towards combining human beings with technological implants can have a great impact on social life and the concept of certain values, such as human dignity and privacy. The main research question at this point is how the constitutional right of the integrity of the human body is influenced by new technologies such as nanotechnology, RFID or biotechnology. The hypothesis is that the concept of this right or the idea of the human body might be subject to slight changes when artificial parts become implanted into it. Examples are RFID implants or nanocomputers. These can still be considered as separate parts, which are implanted, but not part of the body itself. But what if a human organ is replaced by an artificial organ made with biotechnology? In that case it is not a supplement *to* the body but a replacement in the body, so it might in fact even be considered as a part *of* the body.

If we accept this development, which has already started, does this mean that all this messing around with the body is not violating the right of bodily integrity? And if it appears that bodily integrity is not considered to be violated by implants, does this mean that the concept of this right is changing or has already changed? With regard to brain implants which can e.g. help reduce the tremors in Parkinson's disease, the European Group on Ethics (EGE) expressed the opinion that "[t]hey show that ICT implants may influence the nervous system and particularly the brain and thus human identity as a species as well as individual subjectivity and autonomy" (Rodotà & Capurro, 2005). This remark makes the link with dignity and bodily integrity very clear.

With respect to bodily integrity, another question comes to mind, next to the question of which part of the body should be protected with integrity. As the functioning of the body can be expanded with external devices, the boundaries of the body may become unclear. The persons involved in experiments with implants and connections to external devices can experience the connected devices also as parts of their body. For example, after an RFID implant experiment, Kevin Warwick stated: "The biggest surprise for me during the experiment was that I very quickly regarded the implant as being 'part of my body', a feeling shared with most people who have a cochlea implant or a heart pacemaker. In my case though, there was a computer linked to my implant and because the computer was making things happen, I very quickly became attached to it as well." (Warwick, 2002). Even though the computer or other external device is clearly not a physical part of the body it is performing personal activities. The person considers it as part of the body, because the link is as direct as possible. The question is whether this implies that an infringement on the device also infringes the right to bodily integrity, based on the restrictions brought to the linked person. So here is another criterion which can be used to determine whether the right to bodily integrity is under tension because of technological implants: what exactly does the person consider to be part of her body?

When using this criterion problems may occur when people are connected to networks. Via networks, people also become connected to each other. An implication is that different people may try to steer or use an external device at the same moment. If these people do not have the same goal, their communications with the device conflict. If the involved persons do consider

the external device to be a part of their body because they are directly connected to it, the conflicting action of the other person(s) might be considered as a violation of bodily integrity. People find themselves restricted in doing with their body whatever they want. It becomes even more critical when there is not only a restriction, but when there is also harm or damage brought to another person, e.g. when programmed applications are erased or modified.

In order to identify to what extent and in which circumstances the right to bodily integrity is affected by these new technologies, we will first give a brief explanation of the right and its international context. This is best explained by using a specific national example of the right, for which we have chosen the Netherlands, since the Dutch Constitution has a complete, separate article (Art. 11) dedicated to bodily integrity. Then, the right will be discussed in relation to technological implants. Subsequently, there will be a focus on information carriers, such as RFID, and the influence of readable information on the right to bodily integrity.

5.1.1 The right to bodily integrity

The right to bodily integrity in the Netherlands has a brief history. It was implemented in the Dutch Constitution (*Grondwet*) in 1983 after a discussion that had started in 1976, when the first proposal for a provision containing this right was drawn.[30] The Dutch government was of the opinion that the right to privacy, as laid down in Article 10 of the Dutch Constitution, was sufficient enough to include the specific protection of the human body. However, the parliament did not agree and unanimously asked for a modification of the Constitution. The government submitted a proposal, in conformity with the request of the parliament, which was accepted without much discussion (Koops & Van Schooten, 2004, p.117). Since then, Article 11 of the Dutch Constitution reads as follows:

> "*Everyone shall have the right to inviolability of his body, without prejudice to restrictions laid down by or pursuant to Act of Parliament.*" (Koops & Groothuis, 2007, p.172)

The scope of the constitutional right is considered to be very wide. The government and the parliament explicitly wanted to cover the right to prevent others from harming your body (defensive right), as well as the right to do whatever you want with your body (right of self-determination) (Koops *et al.*, 2004, p.124). The government has a duty to make the positive right possible to be executed. There is a duty of care to ensure that a climate arises in which the constitutional right to inviolability of the human body indeed comes to expression (Zoontjens, 2000, p.180).

It appears that in practice the right is particularly related to criminal law and health law. However, the right also applies to horizontal relationships, i.e. relations between citizens and not only in relations between the government and citizens. The right is meant to provide a protection of the human body, thus to prevent others from making infringements to the body. Nevertheless, a claim to let other persons perform certain treatments (like euthanasia) cannot be derived from Article 11 (Koops *et al.*, 2004, p.125), as the right is a so-called negative one,

[30] *Kamerstukken II* 1976/77, 13 872, nr. 17.

which facilitates complaining after harm is done. This is in contrast with positive rights which offer a claim towards others to perform certain actions. Negative rights are mostly related to the classical fundamental rights, whereas positive rights are usually socio-economic rights.

As mentioned above, there has been discussion concerning whether a specific right related to bodily integrity was necessary to be contained in the Constitution, as the right might be covered by other provisions concerning privacy rights. The fact that adding a specific provision is not that self-evident also becomes clear when looking at other countries. Germany has a similar right in Article 2(2) of its *Grundgesetz*.[31] Also Canada and Sweden provide for a constitutional protection of bodily integrity (De Hert *et al.*, 2007, p.275). However, in most countries the right is not separated, but reference is made to other constitutional rights such as the right to privacy, the right to life and, even more often, to human dignity.[32] The relation between bodily integrity and human dignity becomes very clear in cases like, for example, xenotransplantation, where organs of animals are implanted to replace a human organ.

The reason to treat the body with dignity or integrity can be based on the person as being an instance of human life or of the human species. "A being that is human possesses, to the extent that it is human, an essential dignity and identity, because it is *human*." (Reuter, 2003, p.57). This implies that for example xenotransplantation results in a human that should be treated with dignity, except for the animal part. Fukuyama, however, states that "[t]he kind of moral autonomy that has traditionally been said to give us dignity is the freedom to accept or reject moral rules that come from sources higher than ourselves, and not the freedom to make up those rules in the first place" (Fukuyama, 2002, p. 124). And "[h]uman beings are free to shape their own behaviour because they are cultural animals capable of self-modification" ((Fukuyama, 2002, p. 128). If xenotransplantation should imply rejecting a moral rule, namely that animals and humans should not be combined, Fukuyama's argument defends that because of this rejection of dignity exists. In contrast with the first argument then, the human being as a whole, including the transplanted organ, would be treated with dignity. From this discussion the difficulty of human dignity as part of bodily integrity, or maybe even as an overarching concept, under which bodily integrity exists, becomes clear. The concept is closely related to moral considerations, whereas the right to bodily integrity is meant to be a concretisation of morality. When discussing bodily integrity by using dignity, it appears to be difficult to exclude moral arguments. Dignity is a basic moral concept, so discussions where dignity is at stake will almost automatically focus on moral arguments. Morality is inextricably bound up with reasoning people and can therefore not be excluded. These ethical challenges to the acceptability of implants are the result of a natural technology development, diffusion and acceptance process (Marshall, 1999).

In this chapter, the focus is on voluntary implants, which, basically, implies that criminal law is excluded from the scope of this chapter. Health law can still be applicable, because implants often imply a medical interference. In the following sections we will, for the sake of clarity, use the term "right to bodily integrity", to include "human dignity" and "privacy", when these rights are interconnected or are similar in meaning. The crucial point of discussion

---

[31] **Article 2 [Personal freedoms]** (2) Every person shall have the right to life and physical integrity. Freedom of the person shall be inviolable. These rights may be interfered with only pursuant to a law. Text (official translation) available at: http://www.bundestag.de/htdocs_e/parliament/function/legal/germanbasiclaw.pdf

[32] Idem, p. 275.

concerning the scope of the right to bodily integrity may appear at the border when treatment and enhancement cannot be categorically separated.

5.1.2 Biotechnological implants

While this deliverable is focusing on ICT implants, the legal discussion around enhancement and bodily integrity has to date predominantly centred on 'biotechnological' implants, i.e. human organs, genes or cells that can be implanted or injected. Clearly much of this discussion is relevant and transferable to the area of ICT implants, and so this section gives an overview of biotechnological implants in relation to bodily integrity.

Biotechnological implants can violate bodily integrity. According to the legal interpretation of constitutional rights as applied by Canadian courts, the closer something can be tied to the individual, the higher the expectation of privacy and the protection of the body (Marshall, 1999). Implantation and transplantation are often considered as the most invasive to bodily integrity of the individual. Implanting something is the closest one can get to the individual. Because it is considered to be so invasive, consent of the patient, as a requirement for (certain) medical treatments, shall be very well explained in a legal sense. Without clarity on the scope of the term 'consent' it is impossible to judge whether this consent was given in a particular case. Basically, most biotechnological implants have a medical function. For instance, kidney transplants and heart transplants are quite common as treatments and offer patients good opportunities to live longer. Since these treatments require, as mentioned, the consent of the patient, the infringement of the right to bodily integrity is covered by law; personal decision-making about bodily integrity must be respected (Hartman, 2007, p.69). However, the exact requirement is *informed* consent. On the scope of this term, discussion is possible. It appears to be difficult to define 'informed consent' properly, in particular when patients have to agree on a certain treatment which is technologically not understandable for a layman. This discussion is, however, out of the scope of this section and will be further analysed under section 5.2 in the context of the processing of personal data.

With respect to bodily integrity, more problematic is what happens if biotechnological implants are not implanted because of a medical treatment, but because someone wants to have another organ, or when someone wants to have cells or genes of another person injected into her body.[33] In this situation the medical purpose is absent, but the aim is to change or alter the body or to enhance certain properties of a person. In these cases there is consent of the person who asks for the implant. However, since there is no medical purpose, even though an implant operation in itself certainly is a medical treatment, the applicability of medical law provisions might become unclear.[34] To make it easier for the argument, only the open norm of Article 11 of the Dutch Constitution (the right to bodily integrity) will be discussed here. When there is consent, it might be argued that there is no violation of the right. However, as already discussed in section 5.1.1, the right does not cover a claim to let other persons perform a certain treatment. Even though there is consent and the right to bodily integrity seems not be harmed, a tension towards the right comes to being. If persons can just change their body with implants or gene injections, questions arise with regard to the value of the

[33] This situation is future theoretical. However, there are cases where this has already happened, even though the treatments are prohibited by law.
[34] Basically, these laws do apply, but most treatments like those mentioned are not allowed to be performed, so they take place in secret.

right and the boundaries of the human body which is protected by the right to bodily integrity. Responses to these questions will mainly be determined by moral arguments.

As mentioned earlier in section 5.1.1, the difficulty is where to draw the line between therapeutic interventions in the body and enhancement. "What may be therapeutic in one circumstance may be considered an enhancement when used by healthy individuals and adapted for other purposes" (Hogle, 2005). The distinction can be made between replacements (filling in the missing part) and designs for specialised or enhanced functions (Hogle, 2005). However, the impact of an artificial organ or a xenotransplant goes much further than just the replacement. "[L]ike all technological objects the replacement is not a neutral adjunct to the body; rather, depending on the context in which it is used, a new subjectivity may be created for the user, and new meanings of embodiment may be created." (Hogle, 2005). Here, the tension towards the right to bodily integrity becomes clear. The way in which a person experiences her body might be changing. The question is whether this affects the integrity of the body. Is the body, when experienced in a new way, still the body one had before the biotechnological implant was inserted? And if not, does this mean that bodily integrity does not exist anymore for this person or only partly? Absence of bodily integrity as a result of an implant appears to be very strange and will, likely, not be the case. But still, there seems to be a difference with other changes to the body. This is because the bodily perception is at stake in contrast with other cases where the body can be seen as an object. A more instrumentalistic view will lead to different outcomes to the questions and more or less reject the moral issues that arise. However, it is questionable to what extent an instrumentalistic view can be upheld in a biotechnological debate.

Changes to the human body are certainly not new. For centuries, tattoos and piercings have been commonly accepted as permanent alterations. What then exactly is the difference, between a tattoo and an implant that makes bodily integrity be at stake with implants, but not with tattoos? Or does the same concern count for tattoos, but we are less aware of that? The most obvious distinction between tattoos and technological implants is that implants become part of the inner body, whereas tattoos are put onto the skin outside the body. The question is whether this really makes a difference. What, for instance, if someone wants to have an extra limb? It would be an adaptation of the body, visible at the outside. The aim, beauty or belief, can be the same for this person as the aim of a tattoo.

It is very difficult to identify exactly what makes biotechnological implants, when used for purposes other than medical, different and why they put the right to bodily integrity under a certain tension. One thing that certainly makes biotechnological implants special is that the implants have a 'living interaction' with the rest of the body. The value of the right might be at stake when there are no limits to alter the body with parts that are also alive and become dependent of the connection to your body to continue existence. On the contrary, it can be argued that the right becomes even more valuable, since parts that are added to the body also need to be treated with bodily integrity. A violation of an added part will likely cause serious damage to the 'original' body because of the direct connection. The tissue of the biotechnological implant and the body will attach to each other, implying that it becomes more difficult to remove the implant after a while.

Here, reference is made to today's liberal society. Indeed, society and social values are subject to change, but not everything will be accepted. However, given the idea that social and moral values are slightly changing over time and that with these changes step by step more practices become accepted, at some point in time the situation will occur that the right to bodily

integrity is valueless since it does not protect any dignity anymore, at least not in the sense that it does nowadays. It can protect dignity in the sense that individuals have the right to modify or enhance their body because they are human beings with moral autonomy (Fukuyama, 2002, p. 124). The body, as a living matter can be changed or enhanced as much as the individual wants, implying that there no longer exists an unequivocal notion of what the human body exactly is. Without this common concept, the right as it is applied nowadays cannot be made concrete in practice. The uniform explanation on which everybody would agree that this should be protected with bodily integrity is lacking.

Even when there should remain an unequivocal notion of what the human body is, also when it is mutilated or enhanced, the approach towards the way the body should be treated is changing. Treatments or surgeries that unarguably violate the integrity of the human body, albeit with consent of the patient, become commonly accepted. This can be elucidated from two different perspectives. One is that absence of a medical need for a treatment in combination with the patient's consent does not imply a violation of the right to bodily integrity. In essence, the violation is 'repaired' by the voluntary character of the treatment. In this approach the right to bodily integrity still exists, but the focus for the application of the right lies on consent. The other perspective to explain the general acceptance of treatments and surgeries is related to the notion of what the body exactly is. From this perspective, the body is the natural body including all possible alterations, mutilations or additions. Because of the fact that all supplementary parts are considered to be part of the body, and therefore are considered to be protected by the right to bodily integrity, the treatments needed for changing the body should also be respected.

To conclude, with regard to biotechnological implants it can be argued that these implants are usually seen as real body parts. Because of the nature of these implants this is more often the case than with other implants, (see below). When taking the connection and living interaction with the body into account, the right to bodily integrity can be subject to change in several ways. Either the right is loosing its value, since there is no common notion remaining of what the body exactly is and what exactly should be protected with the right, or the right is extending its value by also protecting the implants. Another approach towards the right to bodily integrity is to differentiate between a focus on the patient's consent and a focus on the notion of the body when examining the applicability of the right.

5.1.3 Nanotechnological implants

This section deals with nanotechnological implants. While the term 'nanotechnology' has been increasingly used by governments, industry, the media and others, a universal definition has yet to be agreed upon. A functional starting point is however the National Nanotechnology Initiative (2007) definition of nanotechnology, that being '…the understanding and control of matter at dimensions of roughly 1-100 nanometers, where unique phenomena enable novel applications. Encompassing nanoscale science, engineering and technology, nanotechnology involves imaging, measuring, modelling, and manipulating matter at this length scale'. A single nanometer is the equivalent of one billionth of a meter (10^{-9}), while nanoparticles are particles with one or more dimensions within the 1-100nm size range.

The small size of nanoparticles makes them very suitable for making products that can be implanted or injected. The fast development – in particular miniaturisation – in the field of

computer chips gives input for spectacular speculations, for example mind transplants, and gives perspectives on a broad range of practical applications (Van Est *et al.*, 2004, p.39). In contrast with the biotechnological implants of the previous section, nanotech implants are not living. These implants can, however, also interact with the body. One such example is the (hypothetical) curing of diabetes by injecting many nanobots into the patient's bloodstream. These nanobots would be able to synthesize insulin, and to secrete it according to the level of glucose they would sense.

In the case of nanotechnological implants there are only two possible justifications: a medical purpose or enhancement. At first glance, the aesthetic purpose cannot be the case, since the implants are not visible on the outside of the body, apart from the question whether they would be visible without a microscope anyway. However, indirectly the purpose can be aesthetic in cases where beauty mechanisms are influenced by the implants. For instance, certain functionalities can be considered as aesthetic.

In the context of this chapter, it is important to make a distinction between monitored and modified bodies. Monitoring bodies with the help of (nano) technological devices usually has a medical care purpose. It can enable regulated secretion of medicines, as mentioned above, in combination with monitoring by specialists at a distance. However, this distanced monitoring implies data transfer to external devices. The next section will deal with information carriers and communication in more detail. In this section the focus lies on modification for enhancement. This focus does not necessarily mean that there is no communication with other devices, but it excludes devices which carry personal data.

As an example of enhancement with nanotechnological implants, one can think of brain-machine interfaces (BMI), which translate neuronal activity into command signals for artificial actuators (Lebedy & Nicolelis, 2006).[35] The translation is based on algorithms. In the future BMI can help people to steer devices at a distance by thinking. One specific application of the technology is to let disabled people drive their wheelchair without requiring the user to perform any physical action (Millán, 2004). As mentioned above, nanotechnology enables the development of devices on a small scale, which are more suitable for implanting. However, the use of nanotechnology is not necessarily required for BMI. In this respect, see also section 4.2 where IMDs are discussed.

A completely different issue that comes to mind when discussing nanotechnological implants is the possible risk these implants bring. There are fears over the possible dangers of some nanotechnologies, i.e. some free engineered nanoparticles, such as carbon nanotubes. "[S]tudies examining the toxicity of engineered nanomaterials in cell cultures and animals have shown that size, surface area, surface chemistry, solubility and possible shape all play a role in determining the potential for engineered nanomaterials to cause harm." (Maynard, 2006). The question is whether the risk and uncertainty of what exactly will happen is acceptable, or whether humans should not be exposed to these risks. At least it is known that nanomaterials can possibly penetrate intact skin, implying that controlling the movement of these particles is difficult (Rousse *et al.*, 2007). There is, however, a debate going on whether

[35] A more technical description of the technology can be found in (Wolpaw *et al.* 2002).

skin penetration by nanoparticles is really possible. At least, there seem to be some conditions which can be of help, but there is no certainty at this current moment.[36]

The exposure of the body to risks and uncertainties with regard to health can also be considered as an infringement of the right to bodily integrity. Posing risks and accepting possible harm is closely related to human dignity. When using Fukuyama's description of why humans have dignity (see section 5.1.1), unpredictable risks can violate dignity, since the objective choice to change or modify the body is absent. A person who wants to have nanocomputers injected or implanted into her body only states that she wants that, but the desired change or modification cannot be defined exactly. It seems that current concerns over potential risks focus on free nanoparticles as opposed to those that are fixed in a matrix (Maynard, 2006).

5.1.4 Information carriers

This section deals with implants which are not only able to communicate with external devices, but which are also capable of transferring personal data to these devices, the implications of which will be analysed in section 5.2. Such transferring is to be considered in a broad sense; so not only 'real' transfer is involved, but also implants which can be read by an external device, without needing to touch the physical body, like for instance RFID[37], which can be read at a distance. When these devices contain personal data, this implies that these data can be read from a distance without the person, whom they concern, necessarily being aware of that.

The extent to which this 'data reading' is an infringement of the right to bodily integrity depends on the explanation of the right to bodily integrity. Is the essence of the right related to physical violation of the body, or is the focus more on the protection of information about the body? (Koops *et al.*, 2004, p.182). When physical violation of the body is considered to be a necessary factor, data reading does not imply an infringement to the right, because the body is not affected. However, the right to privacy, which is closely related to the right to bodily integrity, can be harmed, in particular when the person involved has no knowledge of her data being read. In this respect, human dignity is of importance, since this concept usually covers bodily integrity as well as privacy rights. In the case that bodily integrity is considered to protect information about the body, data reading means an infringement of the right. In this case, privacy, or more specific the protection of personal data, can be seen as part of bodily integrity.

From a privacy perspective, the majority of European citizens and other RFID technology stakeholders ask for serious considerations with regard to the use of RFID technologies (EC, Consultation on RFID, 2007, p.18). Privacy considerations are mostly connected to registration of goods and tracking and tracing possibilities, which lead to extensive profiling. Obviously, tracking and tracing becomes ultimately personal when the tracked device is implanted into an individual and not attached to a product which can be left behind or passed on to another person. When the traceability is connected to personal information which is

[36] For an overview of research on this aspect, see for example: Australian Government, Department of Health and Ageing Therapeutic Goods Administration, 'A Review of the Scientific Literature on the Safety of Nanoparticulate Titanium Dioxide or Zinc Oxide in Sunscreens', 16 January 2006.

[37] RFID stands for Radio Frequency IDentification, as discussed in section 4.1.

carried by the RFID device and can be read by external devices, the tension towards privacy rights becomes critical. Moreover the use of such technologies can increase the danger for identity theft and endanger consumer anonymity.

Even though there certainly is a tension in relation to privacy rights, it can be questioned whether there are specific concerns for bodily integrity. As discussed above, privacy can be seen as a part of bodily integrity when data that can be read from RFID devices are personal data or contain information about the body. However, the fact that these data are carried on implanted devices does not necessarily make a difference in comparison to situations where the data are read from a chip card or passport. The mere fact that personal data are read secretly is an infringement of privacy rights. The only difference might be that it is impossible to remove the implanted RFID devices, while a passport can be left at home. The voluntary implantation of an RFID devices or other information carrier requires informed consent. This informed consent then should include proper knowledge about the impossibility to shield your personal data that are on the devices from being read.

5.1.5 Other implications of ICT implants, with legal effects

The use of ICT implants can have other implications, next to possible infringements on the right to bodily integrity, such as various cultural effects. In this respect, it is striking that these effects can be the result of different ideas. On the one hand, general acceptance and use of implants can influence legal concepts, as mentioned above. However, on the other hand there is a risk in not participating in technological developments related to ICT implants. For instance, deafness is sometimes considered as a characteristic of a person and not as a handicap. People in the "deaf-pride community [consider] deafness a cultural identity, not a disability to be cured" (Sandel, 2007). Not everyone will agree on this. As a result, different opinions may have negative consequences, related to discrimination, stigmatisation, and exclusion.

Discrimination may occur if people do not participate in implant technologies. They may become relatively inferior to others, because they are not enhanced. In this sense, choosing to stay as a human being naturally leads to discrimination. The other way round, discrimination may occur towards people with implants, if they remain a minority.

A generalising effect of discrimination can result in stigmatisation of the subject group of people and then (social) exclusion. This exclusion may even go further towards exclusion from certain public services or health care, since people have chosen to change their body with implants or since they have chosen not to have implants.

It remains difficult to have a clear vision on the implications of ICT implants and which side will become reality, if one. Although the implications can certainly have legal effects, they will be described more thoroughly in Chapter 6.

5.2 Data protection issues

The general right to bodily integrity covers a broad area relating to any kind of intervention on the human body. However, an implant itself may in various instances contain information about the individual. As already discussed in section 2.1, human implants can be used for different purposes, like restoration or enhancement of human capabilities, diagnosis of the

biological state or identification of a person. In some of these cases the implant functions as an information carrier, bearing for instance information about the health condition of the person (Halperin *et al.* 2008). In other applications, the implant contains only a unique number that can be linked to concrete information about an individual, which is for instance stored in a database.

When information of any kind can be linked directly or indirectly to an individual it qualifies as personal data, as will be further discussed under section 5.2.1, and the relevant legal provisions on data protection shall apply during its processing. In the case of human implants, which cannot be disconnected from the human body, the implications against the privacy of the individual are imminent. In the future Ambient Environments[38], readers will be present at various places, being able to monitor information continuously. The building up of profiles will become an everyday practice and all the movements and actions of every individual will be monitored.

The European Group on Ethics in science and new technologies to the European Commission in its research on various topics regarding information and communication technologies has identified some key ethical values, which can be usefully mentioned in relation to ICT implants as well. The first one is the respect for the privacy and right to protection of their personal data, "respecting the people's right to maintain boundaries and also to preserve privacy, autonomy and confidentiality" (Rodotà & Capurro, 2005, p.27). The second value is the empowerment of individuals "against the introduction of systems likely to reduce their freedom and autonomy […] or likely to increase people's dependency on selection and decision mechanisms which are not transparent or understandable (Rodotà & Capurro, 2005, p.27). Although the autonomy of the individual seems to be an important right of the individual, she is not always completely free to do everything she wishes with her body, as it is illustrated, albeit indirectly, in Article 8(2)(a) of the data protection directive[39]. According to this article, Member States are allowed to regulate that the explicit consent of the data subject is not enough to justify the processing of her sensitive personal data, such as health data (see section 5.2.3.3).

5.2.1 Defining personal data in the context of ICT implants

The European legislation on data protection applies to ICT implants when they entail processing of personal data, irrespective of the technology used. According to Article 2(a) of the data protection directive, personal data shall mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to her physical, physiological, mental, economic, cultural or social identity". Therefore we need to assess firstly if the processed data relate to a natural person and secondly whether the data relate to an individual who is identified or identifiable (Pitkänen and Niemelä, 2007).

---

[38] See FIDIS deliverable D7.7: 'RFID, Profiling, and AmI' for more detail

[39] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, L 281, p. 31-50 (23.11.1995).

When information about an individual, such as her name, age, medical condition etc., is directly stored on the implant, it is beyond doubt that this information qualifies as personal data. More attention is to be paid to cases where the information can not be directly linked to a natural person, i.e. when the person is eventually "identifiable". The information can for instance be reasonably associated to an individual by linking the number of the implant to a back-end database, which contains information about the medical condition of the individual. In this case, the information will be considered as personal data and the data protection legislation will apply. Recital 26 of the data protection directive stipulates that "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person" in order to conclude if we are talking about an identifiable natural person. However, the European Member States have not interpreted "identifiability" in the same way. The data protection laws of France, Belgium and Sweden for instance have adopted a broad interpretation of the concept of personal data, rendering any information as personal data if an individual can be identified, regardless of the technical or legal difficulties in determining the identity of the individual.

In view of the need for clarification of the notion of "personal data" in various contexts, the Article 29 Working Party[40] adopted an opinion on the concept of personal data (Article 29 Working Party, WP136, 2007). The Working Party considers that the technological state of the art at the time of the processing, as well as the future technological possibilities during the period for which the data will be processed, have to be considered. More specifically the Article 29 Working Party stated that "if [the data] are intended to be kept for 10 years, the controller should consider the possibility of identification that may occur also in the ninth year of their lifetime, and which make them personal data at that moment" (Article 29 Working Party, WP136, 2007, p.15). Since technology is developing with great speed, in many cases it will not be possible for the controller to "guess" the means that might be used within some years. Trying to foresee the possibility for identification after 10 years can be extremely difficult for a controller too and therefore the question arises whether we shall apply the data protection legislation in all relevant applications, following a "just-in-case" model (see Fischer-Hübner and Hedbom, 2007, where RFID is used as an example).

5.2.1.1 Health data[41]

The data protection directive has instituted several separate restrictions and requirements for the processing of special categories of personal data, commonly known as "sensitive data". These include personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (Art. 8(1) data protection directive). According to the same Article, the processing of such data is, as a rule, prohibited. The reason for this general prohibition is that this sort of information is so closely related to the private life of individuals that the processing of such

[40] Under Article 29 of the Data Protection Directive, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data is established, made up of the Data Protection Commissioners from the Member States together with a representative of the European Commission. The Working Party is independent and acts in an advisory capacity. The Working Party seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics.

[41] This part is based on the Brendan Van Alsenoy, "Task HE 2.1.1. Legal requirements analysis" (Internal deliverable), Interactive Mobile Medical Monitoring Project (IM3), 31 May 2007

information creates a far greater risk for the privacy of the individuals concerned (De Bot, 2001). In the context of ICT implants, an important category of sensitive data that should be analysed are health data, as a great number of human implants are intended for health and medical applications.

The definition of health data as personal data concerning health is very broad and it could be assumed that it covers all personal data pertaining to the past, present or future physical or psychological health condition of the data subjects involved (De Bot, 2001). The European Court of Justice has taken the position that the expression "data concerning health [must be given a] wide interpretation, so as to include information concerning all aspects of the data subjects, both physical and mental, of the health of an individual" (ECJ, Lindquist Case). Moreover the Article 29 Working Party has recently stated that "all data contained in medical documentation, in electronic health records (EHR) and in EHR systems should be considered to be 'sensitive personal data'" (Article 29 WP, Opinion on EHR, p.7). Health data cover all personal data that have a clear and close link with the description of the health status of a person, such as genetic data or data relating to the consumption of medicinal products, alcohol or drugs. In the same opinion the Article 29 Working Party considered that even "any other data – e.g. administrative data (social security number, date of admission to hospital, etc.) – contained in the medical documentation of the treatment of a patient will have to be considered as being sensitive" (Article 29 WP, Opinion on EHR, p.7).

5.2.2 Applicability of the ePrivacy Directive

The European legislation for the protection of personal data consists not only of the data protection directive, but also of the ePrivacy directive[42], which regulates specific issues regarding the processing of personal data in the electronic communications sector. The directive aims at protecting the personal data and the privacy of the users of publicly available electronic communications services that are offered via public communications networks. Therefore, in order to decide upon the applicability of the ePrivacy directive in the context of ICT implants, three main issues shall be examined:

i) whether there is an *electronic communications service*,

ii) whether this service is offered in a *communications network* and

iii) whether the aforementioned service and network are *public*.

The aim of the ePrivacy directive is to protect the users of publicly available electronic communications services that are offered via public communications networks regardless of the technologies used, having as its ultimate goal the achievement of technology neutrality (Rec. 4 ePrivacy Dir.). However, questions arise regarding the applicability of the ePrivacy directive to several emerging technologies (Cuijpers *et al.*, 2007). It shall be clarified that when processing of personal data takes place in applications or systems, the users still enjoy

[42] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), Official Journal L 201, pp. 37-47 (12.07.2002).

the protection of the general data protection directive. It remains to be examined whether the specific provisions of the ePrivacy directive that regulate issues, such as security, confidentiality, traffic and location data, apply as well.

According to Article 2(d) of the Framework directive[43] "*public communications network* means an electronic communications network[44] used wholly or mainly for the provision of publicly available electronic communications services[45]". The term '*communication*' is defined in Article 2(d) ePrivacy directive as "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information". The need for further clarification of these quite complicated definitions has already been recognised by the Article 29 Working Party: "The Working Party notes that both definitions 'electronic communications services', and 'to provide an electronic communications network' are still not very clear and both terms should be explained in more details in order to allow for a clear and unambiguous interpretation by data controllers and users alike" (Article 29 Working Party, WP126, 2006).

Besides the unclear definitions of electronic communications services and electronic communications networks, an additional question arises with regard to the applicability of the ePrivacy directive to emerging technologies. When are the aforementioned services and networks public? No definition of the term 'public' is included in the current regulatory framework on electronic communications and the term can be subject to various interpretations. (Cuijpers *et al.*, 2007) mention some of the criteria regarding the question whether or not a network or service should be considered public: "is it the provider's intention to offer the service to anyone who requests this service?; standardisation, which suggest an intention of uniform and public accessibility; whether the network or service is oriented at a limited geographical area; and whether the network or service is specifically aimed or designed for a specific group of people".

The European Commission presented on the 13th of November 2007 a "Proposal for a Directive amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation". The proposal explicitly refers to RFID technology (and not to all emerging technologies) in recital 28 stating that "[w]hen [RFID] devices are connected to publicly available electronic communications

---

[43] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive), Official Journal L 108 , pp. 33-50 (24.04 2002).

[44] '*Electronic communications network* means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed' (Art. 2 (a) Framework Directive).

[45] '*Electronic communications service* means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks' (Art. 2 (c) Framework directive).

networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC, including those on security, traffic and location data and on confidentiality, should apply". However, as the European Data Protection Supervisor has also pointed out "RFID-applications might not be covered because of the limitation of this (i.e. the ePrivacy) directive to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks" (EDPS, 2007). The issue regarding the definition of networks or services as "public" still remains and the questions regarding the application of the ePrivacy directive on services offered via networks that are not clearly "public", such as ones used for ICT implants, are still open.

5.2.3 Processing of Personal Data with regard to ICT implants

5.2.3.1 Defining the controller and the processor in an ICT implant system

The European data protection legislation distinguishes between the data controller and the data processor. The controller is defined as a person (natural or legal) which alone or jointly with others "determines the purposes and means of the processing of personal data" (Art. 2(d) data protection directive), while the processor is a third party who simply processes personal data on behalf of the data controller without controlling the contents or use of the data (Art. 2(e) data protection directive). This distinction is of great importance in the processing of personal data that are directly stored in ICT implants or can be indirectly linked to an individual. The data controller (and not the data processor) is the one who will carry the obligations described in the data protection directive and is the one to define the details of the data processing. When personal data are stored on an ICT implant for instance, the controller will be the one who has chosen that the implant will be used as a medium to store personal data and has decided which data will be stored on the tag (see Zwenne & Schermer, 2005, where they applied the same reasoning to RFID tags). As a rule of thumb, it can be said that the data controller is liable for violations of the data protection legislation, while the role of the data processor is reduced (Kuner, 2007). In some cases there may be multiple controllers for the same data set or multiple processors (Kuner, 2007). It is however the entity which has the final decision making power with regard to the processing at issue (the type of information being processed, access to the information, transmission of data, …) that should be labelled the controller (Verhenneman, 2008). Once an entity becomes sufficiently involved in the determination of the purposes and means of the processing, it will be considered a (joint) controller (Kuner, 2007).

5.2.3.2 Legitimate data processing

ICT implants enable the processing of personal data in two ways. Either personal data are directly stored on the implant (e.g. information about the medical condition of the patient) or by combining information that is available on the implant, like a unique identifier, with data that are stored somewhere else, such as in a database (Zwenne & Schermer, 2005). However in the ubiquitous networked societies of the future, ICT implants will be used as the means to easily identify an individual and will enable their tracking and tracing at all times. The processing of personal data is allowed only under the grounds mentioned in Article 7 data protection directive - or Article 8 when processing of sensitive data takes place - and shall be

respected when the processing of personal data is taking place in any form. This means that for each processing of personal data - collection, recording, storage, adaptation, alteration, retrieval, consultation, disclosure, dissemination, etc. - the controller has to verify if the processing falls under one of the criteria for making data processing legitimate.

The first case in which processing of personal data can be considered as legitimate is when the data subject has unambiguously given her consent. The 'data subject's consent' is defined as any freely given specific and informed indication by which the data subject signifies her agreement to personal data relating to her being processed (Art. 2(h) data protection directive). The processing is equally legitimate when it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject for entering into a contract. The processing is in the third place authorised when it is necessary for compliance with an obligation to which the controller is subject. In the fourth place, processing of personal data is legitimate when necessary to protect the vital interest of the data subject. Finally, processing personal data is legitimate when it is necessary for purposes of the legitimate interests pursued by the controller or by a third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (Buchta *et al.*, 2005). The processing of personal data in relation to ICT implants has to be based on one of the aforementioned grounds and compliant with the principles that are set out in Article 6 of the data protection directive.

One basic principle for the processing of personal data is that the data shall be processed fairly and lawfully (Art. 6(1)(a) data protection directive). It is crucial that the data are collected for "specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes" (Art. 6(1)(b) data protection directive). In the context of medical ICT implants for instance, "the Convention on Human Rights and Biomedicine[46] provides that test predictive of genetic diseases 'may be performed only for health purposes or for scientific research linked to health purposes'" (EGE, 2005). Furthermore the data controller shall ensure that the collected data are "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Art. 6(1)(c) data protection directive). The procedure followed for the collection of data shall be transparent for the additional reason that in this way the criteria used for choosing the specific data as appropriate can be easily checked. The data shall be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (Art. 6(1)(e) data protection directive). The data shall also be "accurate and, where necessary, kept up to date" (Art. 6(1)(d) data protection directive).

5.2.3.3 Processing of health data in the context of ICT implants

Article 8 of the data protection directive contains exceptions to the general rule of prohibiting processing of sensitive data, several of which are relevant in the context of ICT implants. These exceptions can serve as the legal basis for the processing of health data.

[46] Council of Europe, No 164

- The data subject has given her *explicit* consent to the processing of those data. As defined in Article 2(h) data protection directive, the consent must be freely given, specific and informed indication of the wishes by which the data subject signifies her agreement to personal data relating to her being processed. The explicit consent of the data subject may not be sufficient for the processing of health data, when the laws of a Member State provide that the prohibition may not be lifted by the data subject's giving her consent (Art. 8(2)(a) data protection directive). This exception is most likely to be used as the legal basis for the processing of health data with regard to ICT implants.
- The processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law insofar as it is authorised by national law providing for adequate safeguards (Art. 8(2)(b) data protection directive). This exception may serve as the basis for the processing of data included in ICT implants in the context of companies that ask their employees to accept an implant for authentication or security purposes.
- The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving her consent (Art. 8(2)(c) data protection directive). If ICT implants are embedded in patients that are not able to give their consent, the processing of data that relates to such cases can be based on this provision.
- The processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy (Art. 8(3) data protection directive). This provision has a broad application in the context of ICT implants.

5.2.4 Privacy Rights of the Individuals

However, ICT implants enable the unnoticed collection of personal data and therefore, questions arise as to how the users can be informed about the identity of the data controller in order to exercise their rights. When data are collected directly from the data subject, the data controller must provide her with some information relating to the processing of her personal data. Such information includes the identity of the controller and of her representative, if any, and the purposes of processing. Additional information may be also necessary, such as the recipients or categories of recipients of the data, whether replies to the questions of the data subject regarding the processing of her data are obligatory or voluntary, as well as the possible consequences of failure to reply. Furthermore the controller should inform the data subject about the existence of the right of access to and the right to rectify the data, insofar as such information is necessary (Art. 10 data protection directive). As a rule of thumb, it shall be noted that the controller shall provide the data subject with all the aforementioned information before the implantation takes place.

The European data protection legislation grants the data subject some rights that have to be safeguarded by the data controller. The data subject has the right to be informed whether her personal data are being processed. In positive cases she has the right to know the purposes of

the processing, the categories of data concerned and the recipients to whom the data are disclosed. The information shall be given to her in an intelligible way. Moreover, in cases of automatic processing of the data, the data subject is entitled to know the logic involved in this (Art. 12(a) data protection directive). Article 12 further grants the data subject a right to ask for the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the directive, in particular because of the incomplete or inaccurate nature of the data. Finally, according to Article 14 of the directive, Member States should grant the data subject the right to object, on compelling legitimate grounds relating to her particular situation, to the processing of data relating to her.

5.2.5 Legal requirement for security of ICT implants

Article 17(1) data protection directive addresses the issue of data security, requiring data controllers to take 'appropriate technical and organisational measures' against unauthorised or unlawful processing, and accidental loss, destruction or damage to the data. To the extent that this principle covers the security requirements and robustness of the network itself, this principle overlaps with the security and confidentiality requirements laid down in articles 4 and 5 of the ePrivacy directive, when there is processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. Taken as a whole, this principle imposes a statutory obligation on data controllers to ensure that personal data are processed in a secure environment. This means that the data controllers must consider the state of technological development and the cost of the implementation of any security measures. Bearing in mind these factors, the security measures that are adopted by the data controllers must ensure a level of security that is appropriate to both the nature of data to be protected and the likely harm that would result from a breach of this principle (Carey, 2002). It follows that, the more sensitive the data, the more adverse the consequences of a security breach would be for the data subject, and therefore more stringent security requirements should be put in place. This is especially the case as regards the processing of health-related data. In any case, the data controllers should implement appropriate security measures to ensure that non-authorised personnel are not able to gain access to personal data. Some specific measures are already discussed under section 4.1.4.3 for RFID technology and under 4.2.5 for Implantable Medical Devices in general.

6 Socio-ethical considerations on ICT implants

Ethical implications can be assessed from different philosophical perspectives.[47] Mainstream approaches to ethics are either utilitarian, deontological or based on virtue ethics. From a utilitarian position one would try to calculate to what extent the consequences of human implants satisfy the prevalent preferences of individual citizens, aggregated in order to calculate which usage would achieve the highest (average) good (defined in terms of individual preferences). From a deontological position one would test to what extent human implants violate moral rules or principles, such as human dignity, bodily integrity, autonomy and self-determination or non-discrimination. These two approaches are mostly involved in what is called 'applied ethics', which a preference for rationalist analysis, often based on methodological individualism.[48] Virtue ethics would investigate to what extent human implants contribute to or obstruct human flourishing in terms of virtues like justice, courage, honesty, prudence, etc. One could see ethics like Nissenbaum's 'value sensitive design' and Brey's 'computer disclosure ethics' in that light, as they seem to advocate a less one-sided rationalist exploration of the way computer design affects human interaction.[49]

Though it may be an interesting exercise to chart the ethical implications from these different positions, which each build on distinct assumptions about what is important in human interaction, we will take a different and more practical approach. In tracing the ethical implications we will focus on the extent to which the usage of specific types of implants affects core tenets of constitutional democracy.[50] So, while avoiding a *utilitarian* consequentionalist position we will follow a *pragmatic* consequentialist approach, apt to assess potential effects on individual freedom, personal identity and democratic participation. The difference between utilitarian and pragmatic consequentialism is that the first assumes that means and ends can be neatly separated, which – together with methodological individualism – allows the calculation of which means are best in achieving a specific goal. Pragmatic consequentialism, however, acknowledges that means and ends are often intertwined, meaning that technologies are never neutral in terms of the objective they are supposed to further. This allows for a more precise understanding of the implications of human implants for democracy and rule of law. In terms of democracy and rule of law the focus would be on freedom from unjustified constraints (liberty), on the freedom to participate in democratic processes and public debate, on the freedom to participate on an

---

[47] Ethics is a sub-discipline of philosophy. For an excellent overview of approaches in the field of Computer Ethics, see Bynum, Terrell, "Computer Ethics: Basic Concepts and Historical Overview", The Stanford Encyclopaedia of Philosophy (Winter 2001 Edition), Edward N. Zalta (ed.), see: http://plato.stanford.edu/archives/win2001/entries/ethics-computer/

[48] The rationalist perspective derives from Kant's ethical position, which is termed deontological. This implies adherence to moral rules that apply even if the consequences of their application are problematic. The moral imperative overrules other considerations. This perspective is focused on individual choice. Methodological individualism inspires the consequentialist ethics derived from Bentham's utilitarian position, meaning that choices are based on a calculation of costs and benefits. Rational choice theory could be said to combine rational calculation with normative preferences.

[49] Brey, Philip (2001) "Disclosive Computer Ethics." In R. A. Spinello and H. T. Tavani, eds., Readings in CyberEthics, Jones and Bartlett; Friedman, Batya, ed. (1997) Human Values and the Design of Computer Technology, Cambridge University Press and Nissenbaum, Helen (1999) "The Meaning of Anonymity in an Information Age," The Information Society, Vol. 15, 141-144.

[50] Cf. e.g. Nissenbaum, Helen (2004), Privacy as Contextual Integrity, 79 Washington Law Journal, at 101-140.

equal footing in the economic market (non-discrimination, distributive justice), on due process, privacy and identity (legal subjectivity). Applied to the specific implications of artificial human implants we will translate this focus into e.g. ethical issues around donation and transplantation of human organs, end of life decisions, the need for involuntary interventions, distributive issues, cultural effects, discrimination and segmentation, the borderline between repair and enhancement, privacy and potential personality change (in the end raising questions of what it is to be human).

We assume that different types of human implants may have different ethical implications, meaning that the analysis will require an acute awareness of both the specific affordances of the technology under discussion and the context in which it is used. After a first assessment of relevant ethical issues in section 6.1, we will look into Opinion 20 of the European Ethics Group (published in 2005) in section 6.2, already mentioned under section 5.2, and follow up with a more systematic analysis in section 6.3. We will finish with a brief discussion on human implants as an enabling technology for (group) profiling.

6.1 Assessment of ethical implications

> "When I hear the phrase ''human-implantable electronics,'' I must confess that I feel a bit queasy. It conjures up a more extreme image of pervasive computing than is usually justified. However, my perspective is that of a relatively healthy person in his 40s, without any physical handicaps. If my hearing was impaired or my heartbeat arrhythmic, I might be keen to find a remedy - and, at this time, an electronic implant would probably be the way to go. Putting my emotional reaction aside, when I think about the possibilities of implantable technology, it actually begins to sound pretty cool." (Want, 2008)

This statement clearly shows different aspects which might be problematic in the context of ICT implants in general: On one hand there is the person without physical handicaps which may – at a first glance – be rather opposed to such implants "augmenting" his own capabilities, perhaps not only restricted to physical ones.[51] On the other hand when it comes to physical handicaps, quite a lot of people agree with "replacing" some parts by ICT implants. Here, we consider the term implants in its probably quite general form of any ICT enhanced item stably connected to the human body, hence we begin with tiny items or small RFID tag within the arm (as in the Baja beach club example of section 4.1), continue to larger items (but indivisible) like hip replacement containing some ICT components for – say – measuring physical data with respect to pressures executed on the hip replacement, and end with major parts of the body (like arms or legs) being replaced or enhanced by artefacts containing ICT components.[52] In this sense, the statement above also extends the – sometimes

[51] A first problem here is to define what really *is* considered as "augmented". How should standard human abilities be defined? Consider the case of vision: What *is* standard human vision capability? A myopic person might answer quite differently to that question than a hyperopic person or even a blind one. Should and can we define an average vision possibility?

[52] We do not restrict the analysis to "standard" ICT implants which are typically considered of being small or even tiny size. Because it is, in our opinion, quite difficult to restrict the term ICT implants to tiny things; what *is* tiny in this context anyway? For example, we do not exclude nano-sized ICT items from this discussion at all.

quite restricted – view on ICT implants as small things (like RFID tags, pacemakers, etc.) to larger items (cf. also the discriminations with respect to their type, respectively discussed in section 2.1) but eventually also very tiny things. Hence the subject discussed here extends heavily the concepts discussion in the context of RFID tags, for example in FIDIS deliverable D12.3 "*A Holistic Privacy Framework for RFID Applications*" (Fischer-Hübner, 2007).[53]

A major difference in treating ICT implants and RFID tags within this context is that we consider implants here as typically being not easily detachable from the person while (standard) RFID tags usually can be localised and detached if they are – typically – not implanted. Let us first focus on the aspect of data mining and profiling (Hildebrandt & Gutwirth, 2008), (Hildebrandt & Koops, 2007) which is even more problematic in the present context than in typical RFID situations (cf. also (Fischer-Hübner, 2007)), where the RFID tag is bound to an object, not necessarily a human being, and can be shared between human beings and hence is not a unique identifier for a person. Clearly typical standard data mining and profiling techniques can principally all be used within this special application.

In the example of the night club (section 4.1.1), we have shown actual as well as potential applications of data mining and profiling with respect to a simple ICT implants. While we do not know which of the potential techniques are actually being applied in this case, even the potential application should raise fears of privacy to the "user" i.e. the client of the bar. The main aggravation of the situation is based on the strong link between the person and the implant which typically lasts for a long time. From the point of view of profiling, this is a very good situation as the unique identifier remains stably attached to the person for a long time, hence "good" data without noise may potentially be collected and processed. Within the same use case consider for example the potential for determining interesting clients which always bring friends with them to the club: such a client is very valuable and may get some free drinks as "reward". This is nothing new when considering frequent shopper or loyalty cards from supermarkets. Yet the main difference is the strong link to the person and not to the card – and the card typically may be shared between several persons. So in this sense, we might enter into here a discussion on the aspects of treating persons differently based on their habits, like price reductions, etc.

The problematic issues are not only the communication parts of the ICT implants, but much broader, as Halperin *et al.* mentions in the context of current security directions in pervasive health care (Halperin *et al.*, 2008). This can be considered as a special but important case, if we consider that the number of ICT implants will grow massively in the near future. Halperin *et al.* mention three aspects (citing Venkatasubramanian K. & Gupta, 2007):

1. "efficient methods for securely communicating with medical sensors"
2. "controlling access to patient data after aggregation into a management plane"

Another approach would be to restrict the discussion to implants being *not* visible (because they are *im*planted), but again, to our understanding, this would not help the present discussion. And again, what exactly does *visible* mean in this context and why not extend this criterion to other not strictly visual aspects, like – while staying in the strictly human perspective – for example *tangible*. Going further, what would visibility mean to a human being augmented by say, X-ray vision, or RFID reading capabilities, etc.?

[53] In this context, one might be interested to look at the general discussion on how ethical responses to new challenging and revolutionary techniques might be developed (Moor, 2006).

3. "legislative approaches for improving security"

The second point is in fact dealing with a standard data aggregation problem and not treated here[54]; the third one is briefly discussed in Chapter 5; the first however, is crucial to the discussion here. Clearly, the problems are somewhat related to the case of RFID as often similar restrictions to processing power, transmission issues, power supply, etc. may occur, especially for ICT implants of small size.

While the example above treats a case where the person is willing to implant a device for having special privileges, in some situations a person may not have a broad choice. Consider the case of a pacemaker which typically is not optional if you need it. In the case where the capabilities of such a device are extended with – say – wireless communication,[55] the user typically does not have a choice. In some cases, the extension of capabilities may from a medical point of view make a lot of sense (for example to easily get historical data out of the pacemaker). However, this very extension is from the point of view of the "user" of the device (i.e. the patient) not always needed or even wanted, yet typically one has no choice anymore as only devices with the additional capabilities might be available, while devices without the capabilities being considered as old-fashioned and not produced anymore.[56] A result of this could be that effective detection of people with a pacemaker is possible using the wireless technique, which is not secure enough from a privacy point of view. Applications are manifold, from the very detection of people having pacemakers in critical environments (strong electromagnetic radiation occurring in a specialised industrial context may harm pacemakers), the "following" of such people on their way through a building (e.g. in a hospital, after treatment), behavioural profiling (assuming that the pacemakers are distinguishable), etc. While there are many "good" applications, all other usual problems of profiling may appear.

In the same context we have to consider the discussion on whether such extensions of capabilities are really wanted by the respective communities or their members. As a typical example, some parts of the deaf community are rather critical with respect to cochlear implants, due to various reasons which include medical issues, but also: "[e]xtreme proponents of this view regard giving a deaf child a cochlear implant or hearing aids as akin to 'correcting' the colour of a black person's skin by making them white"[57]. The *US National Association of the Deaf* writes in a position paper that "The media often describe deafness in a negative light, portraying deaf and hard of hearing children and adults as handicapped and second-class citizens in need of being "fixed" with cochlear implants."[58] Some precede the

[54] See for example (Hildebrandt *et al.* 2008) for general discussions in this context.

[55] Note that such wireless communication is not the future but the state of the art in pacemakers which operate in the 402- to 405-MHz band, with 250 Kbps bandwidth and have a read range up to five meters (Halperin *et al.* 2008).

[56] Consider in this medical context the situation of vaccination for small children in their first three years: Nowadays, vaccination for only one disease is not possible in Switzerland or very hard to get (sometimes using quite old vaccinations as no new individual ones are produced), so you as a "client" have to have the combined vaccination (typically three of them), hence progress makes your choice smaller.

[57] See: http://wallsmirrors.blogspot.com/2006/05/deafness-is-not-disability-argumentum.html

[58] See: http://www.nad.org/site/pp.asp?c=foINKQMBF&b=138140

argumentation with attributing community issues with respect to deafness, i.e. "The deaf community is a culture. They're much like the culture of the Hispanic community, for example, where parents who are Hispanic, or shall we say deaf, would naturally want to retain their family ties by their common language, their primary language, which is either Spanish or in our case its American Sign Language."[59]

The effect of an implant as in this example may hence provoke cultural effects which may or may not be accepted by the respective persons or communities.[60] The same issues might appear when considering ICT implants which give humans abilities which we do not have by nature.

With respect to future social acceptance, we again can look at results from the field of RFID implants, where some recent studies show that social acceptance is low (Perakslis & Wolk, 2006). In a study commissioned by the New Jersey Institute of Technology in 2002, 78.3% of responders said that they would not be willing to implant a chip in their body. Similarly, a study by CapGemini in 2005[61] reveals that the percentage of people "not at all & somewhat unwilling" was between 42 and 55%, while "very & somewhat willing" between 31% and 44% (dependent on application). In a recent poll ("Live vote") at the MSNBC site[62] to the question "would you like to be chipped?" 66% of the responders replied "no way". Interestingly, 27% of the people replied positively saying they would accept "if there was a good reason". The results of another MSNBC questionnaire done after publication on potential cancer risks related to RFID implants (see chapter 4.1.5) were much more negative[63]: 83% of answers (3841 respondents) said "No way..." and 6.8% responded "Of course. It's worth the risk..." remaining 10% "not sure". Although these surveys are not comparable (different conditions and target groups) and their statistical relevance is at least questionable, they have in common a high rejection rate to having an identification chip implanted. Basically the identification technologies have *per se* a low acceptance rate and even more so RFID implants, due to their nature of being *im*planted which is considered intrusive and rather 'creepy' – although placing the chip with a syringe cannot be considered as surgery – and many people are reluctant to have this done.

It is worth noting that social acceptance depends on the application field and is highest for lifesaving purposes. According to the aforementioned CapGemini survey, the percentage of people saying "not at all & somewhat unwilling" and "very & somewhat willing" for lifesaving was 42% and 44% respectively, the same for using biometrics for passenger identification in air travel, which is already in place. With respect to general ICT implants, one might therefore see dropping negative scores if there is no discussion about privacy issues in general (extending the identification issues from above).

Furthermore, typically ICT implants have access to private data measured from the body of the person, hence typically data which may not be recorded by some detached item. While restrictive use of such data within well-designed medical applications is surely fruitful for the

---

[59] See: http://www.cbsnews.com/stories/1998/06/02/sunday/main10794.shtml

[60] On the other hand, some people will also reject being "marked" for cultural and religious reasons, e.g. there are people who consider RFID implants as the "mark of the Beast [the Devil]", see section 3.2.

[61] See: http://www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf

[62] See: http://www.msnbc.msn.com/id/5439055

[63] See: http://www.msnbc.msn.com/id/20648530

patient, any abuse may lead to serious damage. The unauthorised collection of data from such devices, or – going further – active interaction with them in order to change some behaviour may be even more problematic. As an example consider deep brain stimulation for patients with Parkinson's disease. If such a stimulation device is controllable from outside (e.g. by wireless communication), one can easily imagine how its abuse may provoke dramatic results.

The *Report on the Surveillance Society* (Wood, 2006) mentions that "Surveillance society poses ethical and human rights dilemmas that transcend the realm of privacy" and further says that "ordinary subjects of surveillance, however acknowledgeable, should not be merely expected to have to protect themselves". Hence tools and abilities should be given to the "users" to control their implants and their communication to the external world completely.[64] Clearly, a problem here is the gap between the possible control of the device and the actual capabilities of the user.

With respect to RFID tags, the main problem with respect to privacy is the typical lack of control of the ICT implants. If wireless communication is available in the implant, how is the communication controlled, supervised or monitored by the person? In case of problems: how is the communication shut down (and afterwards turned on again)? Is there need for emergency access and how is authorisation done in this case?

In FIDIS deliverable D12.3 (Fischer-Hübner, 2007), we have focused on ethical aspects with respect to RFID tags. Clearly, the results and findings presented there can be transported and partially generalised to the field of ICT implants. In contrast to the case of RFID tags (Sotto, 2005), (UK RFID Council, 2006), there is to our knowledge no specific code of ethics or of conduct with respect to ICT implants available yet. However, general ideas from the versions of codes specific to RFID tags may to some extent carry over to ICT implants.

The *ACM Code of Ethics and Professional Conduct*[65] as well as the *British Computer Society Code of Conduct*[66] has been discussed in FIDIS deliverable D12.3 (Fischer-Hübner, 2007). Their content is not focused on RFID tags or on ICT implants specifically, yet the points discussed can be carried over to the present context. However, both are rather general codes containing general statements following the concept that – as mentioned in the ACM Code – "questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations". This issue was already taken into consideration by the so-called *Toronto Resolution* (Fawcett, 1994) starting from the observation that the detailed regulations or similar notions of ethical issues etc. are usually not possible. This so-called meta-code contains as a first part a preamble containing a text to be added to every code of ethics built on these baselines in order to fix to a certain degree the context of the newly built code. The second part of the meta-code consists of twelve rules to be followed while constructing any new code specific to an application domain.

---

[64] Clearly, some limited and specialised use-cases may require that the user cannot fully control the implant and its communication. An example is the tracking of prisoners using ICT implants, which clearly requires that the prisoner should not be able to change the functionality (or at least some of them) of the implant. Note however, that this special example is in the context of the monopoly on legitimate force of the state (German "Gewaltmonopol"), which in this case is considered as being accurately dominant over the free will of the prisoner.

[65] Association for Computing Machinery ACM, ACM Code of Ethics and Professional Conduct, (Adopted by ACM Council 10/16/92), http://www.acm.org/constitution/code.html

[66] The British Computer Society, British Computer Society Code of Conduct, 2001, http://www.bcs.org/upload/pdf/conduct.pdf

A fundamental question is whether a single code of ethics will be possible for the general case of ICT implants. We are not sure if the variety of possible ICT implants can allow the building of one code of ethics applicable in each case. Either we get a huge code, or one which is far to general to give help to the users in concrete applications. We might expect to get different codes for different types of ICT implants, yet in this case, what typology to be used is an open question. Perhaps one issue can be a typology based on the type of application, i.e. nowadays, a standard pacemakers is quite a simple implant in comparison with those used for deep brain stimulation. A major issue is clearly the raising of public awareness. In the case of RFID tags, this is happening following the discussions in the press, yet in the case of ICT implants this process is only starting.

In the present context, a main ingredient for ethically well founded applications of ICT implants must be the offering of privacy, or rather, privacy enhancing methods. This subject is treated in several facets in different FIDIS deliverables, and many concepts can be applied to different contexts. In this section we will not delve into this subject[67] about which Weber writes: "It is important to see that ICT implants and biometrics are not the beginning of a process of evaporating civil rights like privacy but only another brick in the wall. Furthermore, it is vital to understand that this problem cannot be solved by other and new technology – civil rights protection is a social and political task and not one of engineers" (Weber, 2006).

Among other issues, Halperin *et al.* consider several aspects of privacy and security goals (Halperin *et al.*, 2008) which gives a good overview of the problems – not all of them ethically focused – arising in this field (see also section 4.2):

1. authorisation
2. availability
3. device software and settings
4. device-existence privacy
5. device-type privacy
6. specific-device ID privacy
7. measurement and log privacy
8. bearer privacy
9. data integrity

Consider for example the device-existence privacy: knowledge of the existence of an implant might compromise the privacy of the person (cf. above). Authorisation must be done in a privacy protecting way using a secured protocol that is not giving any information – on the implant, the entity doing the authorisation, etc. – to a potential attacker. Even if the device reveals its existence to authorised entities, it must, following device-type privacy, usually not reveal its type (unless authorised to do so). Specific-device ID privacy means that an attacker must not be able to follow an ICT implant without being authorised to do so - a typical item, which has no specific-device ID privacy is a standard passive RFID tag which reveals its unique ID to any reader. Clearly, the implant must not identify (unless authorised to do so) its bearer – hence satisfy the bearer privacy.

[67] See for example FIDIS deliverables D13.1: *Identity and impact of privacy enhancing technologies,* D13.6: *Privacy modelling and identity,* D14.2: *Study on Privacy in Business Processes by Identity Management,* D12.3: *Holistic Privacy Framework for RFID Applications,* D3.16: *PET or PIT*, all available at http://www.fidis.net

In the context of ICT implants, some consider enhanced humans (cyborgs) as not being ethically problematic *per se*: "but should such entities, if indeed they are truly cyborgs, present an ethical problem?" (Warwick, 2003). We think however that ethical conflicts of serious extent might arise even in the case of "only" ICT implants (not already so-called cyborgs, cf. the section before), some of them being presented hereafter. At this point we are not able to present final solutions or guidelines for resolving these issues (see also section 6.3), but we present a list of conflicts, which is by no means exhaustive:

1. "Freedom" against "health": Consider the situation where medical reasons clearly indicate that that you should have a pacemaker implanted. If all devices applicable to your situation which are produced already contain some wireless communication device, you may either accept this fact and have such a device implanted or otherwise face the medical problems induced by not having a pacemaker which – in the worst case – might lead to serious life-threatening problems.
2. "Supervision" against "anonymity": In the same context as above, bearers of ICT implants may not be anonymous anymore. In some situations, other devices might identify you through your ICT implant, due to some wireless communication and a respective unique identifier. Supervision in this context may however be a crucial and desired issue, e.g. in a hospital environment, the medical staff might need to supervise a patient with an ICT implant newly implanted in order to guarantee convalescence after the operation. However, using privacy preserving technology, a big step should and can be made here in order to avoid supervision by non-authorised third parties.
3. "Self-determination" against "heteronomy", i.e. from a purely technical perspective, one may not be either able or allowed to change or even read the data contained within an ICT implant, possibly due to good reasons like the complexity, etc. This can be considered as a lack of self-determination (in a restricted sense), not allowing to control all of its own "parts of the body"[68]. In some sense, the data contained in the ICT implant can be seen as determining the "behaviour" of the implant with respect to an externally connecting device. Hence one looses the capability to control this "behaviour". From another point of view we also have the conflict between the ones capable of communicated with their own (or even other's) ICT implants and the ones who cannot due to whatever reasons.
4. "Security and privacy" against "safety and effectiveness": This must be regarded first in a technical perspective, see for example (Halperin *et al.*, 2008), but may also have ethical components attached. Typical problems might arise for example when controlling access to data on ICT implants in emergency situations, where different questions are to be answered by different parties, like: What *is* an emergency situation? Which situation – if some classification is available – gives access to what data? Can a medical doctor not better evaluate which access is needed in a situation and should – or even must – she override the restrictions previously specified by the patient in order to save life?

Probably the implants which are directly connected to our nervous system in some way will induce the most problematic ethical challenges. Consider the special case of deep brain

[68] In this context the question arises: what does "belong" to its own body? To what extent can ICT implants – which may be manufactured and even still owned by some company – be considered as belonging to ones body?

stimulation which is a first step in this direction. Such stimulation may provoke not only the expected effects, but indeed have some side effects, positive or negative, such as personality change.

Warwick states another fundamental dilemma to be considered here (Warwick, 2003): "Where the cyborgs represent a powerful ethical dilemma is in the case where an individual's consciousness is modified by the merging of human and machine."[69] Hence, he considers a dilemma arising within the context of consciousness, or mental "operations". However, in this context also the awareness of the person bearing this merging operation of human and machine should be taken into consideration. For the implant part itself, Warwick notes that "the biggest surprise for me during the experiment was that I very quickly regarded the implant as being "part of the body". Indeed this feeling appears to be shared by most people who have cochlear implants, or heart pacemakers" (Warwick, 2003). Although this statement was essentially made only about physical implants, could it be extended to implants which are in contact with our brain or even influence – say – in some sense our consciousness? This would seem to be a point for discussion.[70]

Consider now the enhancement of the human body in a general manner: As already noted, there is a possible discrimination of function between restoration or repair of human capabilities, diagnosis of a biological state of affairs, enhancement of human memory, vision, auditory perception, alertness or other human capabilities, and identification, surveillance, billing.[71] While this discrimination is in theory well defined, in practice we see major problems when actually being forced to discriminate especially between the repair and the enhancement aspect of an ICT implant. Where should the line be drawn? If a blind person gets her ability to see in a way that her vision is far more powerful than that of a "normal" person, shall this be considered as an enhancement? Should technical progress then be restricted to only allow restoration which does not go beyond "usual" capabilities?[72] A side question would then be how to measure this? Some researchers have made clear statements, "From a cybernetic viewpoint, the boundaries between humans and machines become almost inconsequential" (Warwick, 2003).

6.2 Opinion 20, March 2005 of the European Group on Ethics

In their 2005 opinion (Rodotà & Capurro, 2005), the European Group on Ethics discussed a series of principles that are at stake in the case of 'human implants', some of which have already been discussed under section 5.2. Hereunder we briefly summarise the principles they consider pertinent:

---

[69] This merging of human and machine might go on in the direction of merging humans to some extent by connecting their nervous systems through electronic channels (cf. also below). This can question the "boundaries" of the concept of a person; cf. also FIDIS deliverables 2.13: *Virtual Persons and Identities* and 17.2: *Abstract Persons and the law*.

[70] Clearly, one could start here discussing cyborg morals, ethics and the like. For this, we refer to (Warwick, 2003) as a starting point for further discussion and literature.

[71] For aspects concerning social acceptance see the following section 6.2.

[72] See also the discussion in the following sections.

- Human dignity, meaning that a person should be able to operate in self-determination in a free society
- Human inviolability, meaning that (parts of) the human body should not be commodified
- Privacy and data protection, meaning that 'human implants' should not convey sensitive personal data without adequate protection
- Precautionary principle, meaning that in cases of scientific uncertainty the introduction of specific technologies that generate unknown risk, require precautionary measures such as innovative research to investigate potential risk
- Data minimisation, purpose specification, proportionality and relevance, meaning that in as far as the data generated by the usage of human implants are personal data the rules of data protection must be applied
- Human autonomy, meaning that implants may never be used to manipulate individual citizens in a way that refutes their self determination in a free society

Their conclusion was that the existence of serious but uncertain risks requires application of the principle of precaution, with special attention to the difference between active and passive implants, reversible and irreversible implants and between offline and online implants. As to the purpose specification they note that this mandates a distinction between medical and non-medical applications, while as to the data minimisation principle they note that implants should be replaced by less invasive tools as far as possible. In their opinion the proportionality principle rules out the lawfulness of implants used exclusively to facilitate access to public premises. The integrity of the human body rules out that a data subject's consent is sufficient grounds for using human implants, while the human dignity principle would rule out usage of human implants that would turn the human body into an object that can be manipulated remotely and/or turn it into a mere source of information.

The European Group of Ethics also noted a shift from designing human implants for the purpose of observation (monitoring, diagnosis) to modification of human beings (enhancement, the advent of hybrids). This modification was deemed ethically relevant because the usage of online implants may turn individual persons into networked individuals over whom a certain amount of remote control could (potentially) be exercised.

6.3 Further exploration of wider ethical implications

In our opinion, the findings of the European Group on Ethics regarding 'human implants' leave many issues outside of the discussion. In this section we will try to summarise the wider implications, by looking into the ethically relevant consequences of four types of implants: (1) those that aim to restore or repair human capabilities, (2) those that aim to enable monitoring of biological conditions, (3) those that aim to enhance human capabilities and (4) those that aim to identify a human person.[73] In the next section we will briefly discuss human implants as an enabling technology for (group) profiling, a subject hardly touched upon in the Opinion. The relevant implications that we investigate are related to some of the central tenets of

73 Cf. (Hansson, 2005) which aims to provide a more or less systematic overview of what is at stake.

constitutional democracy that form the background of this analysis.[74] Below we summarise the implications and link them tentatively to the principles of democracy and the rule of law. This link is tentative because many of the implications regard more than one principle and most of the implications overlap (which does not mean that they can be reduced to each other).

- freedom from unreasonable constraints (liberty):

  Impact on the ethical issues surrounding transplantation and donation of human organs

  Impact on the need for involuntary interventions

  Impact on end of life decisions

  Impact on the borderline between repair and enhancement

- freedom to participate in democratic processes and public debate:

  Impact in terms of discrimination and segmentation

- freedom to participate on an equal footing in the economic market:

  Impact on distributive issues

  Impact on cultural developments

  Impact in terms of discrimination and segmentation

- due process:[75]

  Impact in terms of discrimination and segmentation

- privacy and identity (legal subjectivity):

  Impact on privacy

  Impact on the borderline between repair and enhancement

  Impact on the personality (changing one's sense of self)

  Impact on cultural developments

74 Cf. M. Hildebrandt and S. Gutwirth, FIDIS deliverable 7.4, Profiling: Implications for democracy and rule of law (2005). Also M. Hildebrandt and S. Gutwirth, Profiling the European Citizen. Cross-disciplinary Perspectives (2008), chapters 14 and 15.

75 Cp. Katja de Vries, From Due Process to Due Processing, in *FIDIS deliverable 6.7, Forensic Profiling* (2008).

While investigating potential ethical implications we stumble on the radical uncertainties of what the future holds for us (and – considering the developments – of the question: who is 'us'?). Moore's law implies that the developments are dynamic in an exponential way, meaning that we do not know what we do not know as far as the future is concerned.[76] This means that many of the implications need further exploration. At this point we do not offer answers, rather raise relevant questions.

6.3.1 Restoration of human capabilities

As indicated in section 6.1, the borderline between restoration of human capabilities and their enhancement will shift once specific types of enhancement become the norm. This in itself will be a consequence of the availability of these technologies, raising the question of consent as well as distributive fairness. If a certain enhancement becomes the norm a person may no longer feel free to decide against it, because she will probably be disadvantaged if she rejects it.[77] If certain enhancements are relatively expensive they may not be covered by medical insurance, thus creating or reinforcing the gap between those that can and those that cannot afford them.

The restoration of human capabilities, such as in the case of cardiovascular pacers, cochlear implants, deep brain stimulation for Parkinson's disease, or an insulin pump, may have ethical implications in as far as they:

1. reduce ethical dilemmas around donations and transplants. Implanting technological devices instead of body parts of other humans or animals may resolve some of the issues related to the need for donated body organs. Organ donation requires invasive interventions in the body of others and impact decisions on the threshold of life and death. The availability of artificial transplants will reduce the chance that another body will be used as a resource.[78]
2. increase the scope of end of life decisions, since survival may depend on the implantation, raising the issue of whether and when a device can be turned off when the patient is unconscious
3. raise distributive issues because insurance companies may not compensate expensive 'repair-implants', creating or reinforcing the gap between those that can and those that cannot afford them
4. blur the border between repair and enhancement, raising issues as to the difference between normalcy and disease, as discussed above

[76] Moore's law, formulated in 1965: 'the complexity of 'minimum cost semiconductor components' doubles once a year, every year, since the first microchip had been produced six years before', see Joel Garreau, *Radical Evolution. The Promise and Peril of Enhancing our Minds, our Bodies - and What it Means to be Human* (2005), at p. 49.

[77] Cf. Garreau, chapter 2 'Be All You Can Be'.

[78] For an intriguing narrative about creating and using a set of human beings as a resource of 'fresh organs' we refer to Kazuo Ishiguro's *Never Let Me Go* (2005).

5. induce personality change, especially in the case that implants are used that affect the brain or the central nervous system. Just like medicines used to reduce depression, psychosis or bipolar disease, the sense of self of a person may be seriously affected while a person may also not have any control over the dynamics of this change.
6. produce cultural effects because certain conditions, e.g. deafness, may become curable, while the Deaf World (claiming to speak for a linguistic and cultural minority) does not consider deafness a disability to be 'cured'
7. require involuntary interventions in the case that a patient is unconscious
8. impact privacy, for instance when they have been tagged with an RFID-tag in order to monitor their condition (see next subsection)
9. enable discrimination, for instance when they have been tagged with an RFID-tag that identifies a person as having a prosthesis

6.3.2 Monitoring of biological conditions and processes

This concerns the usage of implants for a diagnosis of biological state of affairs, such as biosensors like MEMSs (Micro Electro-Mechanical Systems) that monitor inaccessible parts of the body and collect data like blood pressure or glucose levels. The same devices can be extended for smart drug delivery or for alerting medical assistance in the case of risk.[79] These monitoring devices partly evoke the same issues as those related above. They may decrease or change the scope and nature of end of life dilemmas in as far as they provide early warning systems that allow more timely interventions; they will raise distributive issues in as far as they are considered as part of preventive medicine that is not covered by insurance companies. These two implications will combine when those who can afford implantations will survive acute health threats, while for those not 'monitored', help could arrive too late. Also, those who value their privacy may be at a disadvantage when they reject real time online monitoring via such devices. For this reason standard biological monitoring implants may become the rule, turning consent into a farce (insurance companies may refuse to pay unless one is enhanced with a monitoring implant).

The data collected by these implants will be part of the patient's electronic file, allowing refined profiling and – depending on who has access to these files – extensive social sorting by insurance companies, and (potential) employers. This could enable refined – but perhaps unjustified – price-discrimination.

Justice authorities may also be interested in screening such data, and in using implantable devices to control offenders convicted for sexual abuse while they are on parole. MEMS implants could also be used to monitor psychiatric patients, automatically providing smart drugs delivery, enforcing total compliance.

Biological monitoring devices can also be used for enhancement, see the next subsection.

---

[79] These devices are in still in development, see for general information:
http://www.devicelink.com/mpmn/archive/07/07/015.html and
http://www.memsinvestorjournal.com/2006/08/mems_packaging_.html, and e.g. on drug delivery:
http://www.technologyreview.com/Biztech/19784/and on MEMS used to 'train' cyborg-insects:
http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=571

6.3.3 Enhancement

Cosmetic surgery and neuropharmacology have already faced us with dilemmas arising from human enhancement, especially with regard to the dynamic borders between what is 'normal' and what is 'deviant'. In the case of cosmetics, deviance is usually connected with being less beautiful or attractive, while in the case of neuropharmacology deviance can for instance be connected with functioning at a lower than average level within one's professional life. In a competitive market the incentive to 'enhance' oneself may be so strong that it becomes difficult to understand such enhancement in terms of self-determination or consent. Usage of (ICT) implants for the enhancement of human memory, vision, auditory perception, alertness or other human capabilities, may have further ethical implications, partly reinforcing issues already in play with existing 'therapies' for enhancement. They will again raise distributive issues, depending on whether insurance companies will pay for them. Once certain devices are widely used they may create a new default position which will blur the border between repair and enhancement, as already discussed above. Enhanced vision, augmented auditory capabilities, reduced need for sleep and increased resistance to stress will induce a change in human identity, and may raise the question of what it is to be human. In as far as some will and others will not enhance themselves, the introduction of these technologies will produce cultural effects and a new segmentation of society (the enhanced and the 'ordinary'), (Warwick, 2003). In as far as the enhancement depends on online connections, privacy as well as autonomy will be at stake: who will have access to the data exchanged and who will be in control of the online connectivity? The enhanced may find ways to discriminate those less – or not – enhanced, and they may also be capable of protecting their privacy as well as prevent social sorting by outsmarting monitoring devices to their own advantage.

In the case of neural interfaces enabling a direct link between two or more human brains or between brain(s) and machines, entirely new issues arise. Such direct 'cyberthinking' could create cyborgs (human-machine hybrids) that plug into and out of others. This raises the question of what it is to be human in an even more radical manner, as well as questions such as whether such developments are desirable and who will decide on the design and introduction of these technologies (computer scientists, cybernetic experts, commercial enterprise or democratic publics). As to constitutional democracy, we may also have to reflect on whether cyborgs are legal subjects in their own right, capable of bringing about legal consequence (entering into contractual obligation, being liable for harm caused), and competent to vote and partake in public debate. Due to the fact that a person could plug in and out of direct neurological interfaces,[80] the issue of causality will become even more complex: which consequences should be attributed to which legal person?[81] A person could switch between being unplugged and being plugged into one or more other persons and/or smart machines. Can we still consider this person to be the same person, and if not, how do all these different cyborgs relate to the unplugged person?

[80] For first steps in this direction see for example Warwick's experiments with a one hundred electrode array implanted in the nerves of his arm, see section 3.2 and (Gasson *et al. 2005*)

[81] See FIDIS deliverables 2.13: *Virtual Persons and Identities* and 17.2: *Abstract Persons and the Law* (forthcoming).

6.3.4 Identification & surveillance

Here we look into the usage of human implants for the purpose of identification (e.g. to allow restricted access to information, to specific physical or online locations, competence to operate certain instruments or to take certain decisions, liability, payment of taxes), and surveillance (detection of security risks in the case of a convicted criminal on parole, immigrants waiting for a decision on their legal status, elderly or disabled, patients in a hospital, clients in specific environments like bars or other spaces for recreation). In other FIDIS deliverables, especially in D7.7 and those on RFID-systems, the threats of using microchips to identify and survey people have already been extensively analysed. As indicated previously, the difference between human ICT implants and external RFID tags is the fact that the link between a person and the tag is much stronger in the case of an implant. While not everybody is convinced of the fact that data on an RFID-tag are personal data in terms of the data protection directive, there can be little doubt that implants contain personal data, as discussed above under section 5.2. Besides the obvious impact on privacy, we can detect a number of other ethical relevant implications.

Human implants used for identification, tracking and tracing (surveillance) also raise distributive issues, because they allow refined profiling which will enable sophisticated social sorting for marketing purposes, as well as distribution of benefits within the welfare state. The welfare state has always been interested in keeping stock of individuals that make up its populations, having to control access to its redistributive operations.

The capacity to follow a person's everyday movements, depending on the implants she carries along will produce cultural effects, like new and dynamic segmentations of society, based on bottom-up group profiling. The question is to what extent a person can unplug from the system, without jeopardising her health, her safety or the access to her means of existence.

One could argue that this relates to involuntary interventions to the extent that a person is not aware of the profiles she matches, thus having no idea on what bases certain risks and opportunities are provided (Hildebrandt, 2008).

6.3.5 The issue of (group) profiling

As has been noted earlier in the context of RFID systems (FIDIS deliverable D7.7) and AmI (FIDIS deliverables D7.3, D7.7 & D7.9) the emphasis on data minimisation seems not wholly adequate in the case of refined (group) profiling. In as far as this concerns group profiles built on anonymous data, the protection or hiding of personal data may not be effective.

Firstly, in the case of Ambient Intelligence and less integrated smart applications, hiding one's data could make the environment less smart. In the case of medical applications this would involve taking substantial risks. To protect one's privacy in a situation where one actually wishes to share one's data in order to benefit from diagnostic tools, risk-monitoring or biological enhancement, a less reductive conception of privacy is needed. In that case privacy is not a matter of non-disclosure of personal data, but a matter of transparency. We follow Agre and Rotenberg's (Agre, Rotenberg, 2001) definition of the right to privacy as 'freedom from unreasonable constraints on the building of one's identity'. In as far as the implantation of artificial devices into human beings allows for the mining of knowledge that is relevant for the patient or enhanced 'hybrid', this knowledge should be made accessible and 'readable' for the person it concerns. Only in that case will the person be capable of making

informed decisions about 'building her identity', e.g. taking certain health-risks, dealing with insurance companies, changing one's lifestyle, negotiating with commercial enterprise about access to her personal profiles.

Secondly, data minimisation may not be effective because profiles are often constructed on the basis of massive amounts of data, mined from other people. This means that hiding one's data does not prevent profiles from being constructed, while one may still be matched with such profiles on the basis of a minimal disclosure of one's data. Group profiling on the basis of data mined from artificial implants could provide crucial epidemiological information about diseases and/or the impact of enhancement on bodily functions. Hiding such data would not really protect anybody, since the interest in those data is not an interest in the data of an individual person but an interest in the aggregate, statistical level of analysis. Blocking data would restrict scientific research and reduce the possibility to evaluate the long-term impact of artificial implants.

However, this does not mean that data should be shared indiscriminately. It rather means that profiling generates altogether different ethical dilemmas, related to human autonomy and fair treatment. Having shared one's data, one needs to be aware of the knowledge that may be inferred from them, making *transparency of data processing* the hall-mark of 'due processing', requiring adequate communication about the implications of profiling. This should raise the awareness how profiling allows for refined social sorting, price discrimination and manipulation. For this reason the fair information principles should be extended to include the principle of minimum knowledge asymmetry, requiring those that have implants and/or are hybrids to have adequate access to both the logic that rules decisions taken about them and – of course – the nature and consequences of these decisions. To make such a principle of minimum knowledge asymmetry operational we have detected an urgent need for legal and technological transparency enhancing tools (TETs).[82]

[82] See FIDIS deliverable 7.12: Biometric Behavioural Profiling (BBP) and Transparency Enhancing Tools (TETs).

7 Regulatory challenges of human ICT implants

Increasing technology innovation and product sophistication, combined with the anticipated convergence of ICT with nanotechnologies, biotechnology and the cognitive sciences (so called 'NBIC convergence' or 'emerging technologies')[83] appears destined to further challenge regulatory frameworks. This is, in the case of nanotechnologies, due to the ability to rapidly accelerate the miniaturisation processes required, the novelty of the properties that exist at the nanoscale, and the diversity of potential therapeutic and non-therapeutic applications associated with the convergence of technologies, and the ability of this convergence to blur conventional boundaries.

While the ICT sector has to date been a large investor in, and beneficiary of, nanotechnology research and development (Royal Society and Royal Academy of Engineers (RS-RAE), 2004), it is anticipated that the inclusion of nanoscale components in ICT applications will accelerate exponentially over the coming years. This is in part due to the increasing need for miniaturisation, a greater understanding of the novel properties displayed at the nanoscale, and the decreasing cost associated with nanofabrication processes (RS-RAE, 2004). Offering a new method of manufacturing within the traditional ICT sector, the ongoing and incremental convergence of these two ubiquitous technologies promises to play a fundamental role in future advances, including within the fields of, for example, healthcare, biomedical sciences, electronics and optoelectronics and military applications (Anton *et al.*, 2001). While these advances promise tremendous societal benefits, as with earlier technological advances, such benefits are likely to be accompanied by a range of potential physical, social, and ethical risks (Maynard, 2006), (Weckert, 2007). While many of these potential risks may not be unique to nanotechnologies, it may prove to be the case that the technology will accentuate many of these traditional risks and associated challenges. As noted earlier, one area in which nanotechnology convergence with ICT will play an increasingly important role in the short to medium term will be within the development of human implant technology, a development more likely due to increasingly sophisticated nanofabrication techniques. Weckert (Weckert, 2007) has suggested that the continual convergence of nanotechnologies and ICT will not result in the production of nanoscale ICT devices *per se*, but rather small, cheaper, and more powerful devices. The scaling down of implants will not only result in minimally invasive applications, but will give rise to a range of new applications and commercial usages, many of which are likely to exhibit dual functionality. And as discussed below, herein lays the challenge from a regulatory perspective.

It is anticipated that these implants will be utilised for therapeutic and non-therapeutic purposes, including for instance, surveillance purposes (Wood *et al.*, 2003), (Altmann, 2004), (Rodrigues, 2006). Bearing this in mind, by drawing upon a range of current and future applications, the aim of this section is to articulate a range of regulatory issues associated with

[83] See for instance, Roco, M.C., 'Nanotechnology: convergence with modern biology and medicine', *Current Opinion in Biotechnology*, 2003, 14, pp. 337-346; Roco, M.C., 'Science and Technology Integration for Increased Human Potential and Societal Outcomes', *Annals of the New York Academy of Science*, 2004, 1013, pp. 1-16; Roco, M.C. and W.S. Bainbridge, 'Converging technologies for improving human performance: Integrating from the nanoscale', *Journal of Nanoparticle Research*, 2002, 4, pp. 281-295; and Gordijn, B., 'Converging NBIC Technologies for Improving Human Performance: A Critical Assessment of the Novelty and the Prospects of the Project', *The Journal of Law, Medicine & Ethics*, 2006, 34(4), pp. 726-732.

human ICT implants. Attention is given to issues surrounding privacy and data protection with respect to access to health data and implications for personal surveillance.

7.1 Current and Future ICT Human Implants

To date, first generation human ICT implants have primarily included subcutaneous RFID devices, which have been designed primarily for personal identification and tracking purposes (Weber, 2006), (Gadzheva, 2007). These early implants have been increasingly for commercial purposes including, for example, to enable VIP clientele to gain access to venues, and for tracing kidnap victims, an application reportedly to have been used in Mexico and Russia (Gosset, 2004), (Gamboa, 2007), (Gadzhva, 2007) (see also section 4.1.1 above). While these implants have, until recently, been the size of a grain of rice, with dimensions of approximately 2mm by 12mm (Wolinsky, 2007), Hitachi has recently released the Mu-chip (or μ-chip) which are approximately 0.5mm by 0.5mm (Gamboa, 2007) and considered to be 'the world's smallest RFID integrated circuit' (Hitachi, 2007). While these chips are currently being utilised for applications such as inventory control and security and not for human implant purposes (Hitachi, 2007), their development is suggestive of future potential developments in the context of human ICT implants. While the company does not expressly discuss the manufacturing process underpinning the development of the μ-chip within the product information, in light of the ultra small nature of the μ-chips it is possible to speculate that nanofabrication processes have been employed as part of the manufacturing process. Given the spectacular miniaturisation of these engineered structures, and decreasing costs associated with their mass production, it is possible to further hypothesis that the continuing convergence of nanotechnologies with ICT will result in further miniaturisation of RFID devices in particular in the short to medium term.

Somewhat more controversial has been the development of RFID systems which use the unique numeric identifiers to link back to a database containing, for example, personal data such as a person's name, or their health, financial or security-related information. The US-based VeriChip Corporation has played a leading role in transferring this technology from the agricultural sector to human applications (Wolinsky, 2006). The VeriMed patient identification system has been assessed as a 'medical device' by the United States Food and Drug Administration (FDA), and evaluated on the basis of its therapeutic efficacy pursuant to the comprehensive pre-market regulatory framework established by the *Medical Device Amendments of 1976* (VeriChip, 2007a). Approval for the marketing of the system as a medical device in the US was granted by the FDA in October 2004 (VeriChip, 2007a), with reports of as many as 200 customers having been implanted within the first two years (Wolinsky, 2006). The company's current research and development focus is on the development and commercialisation of a 'self-contained implantable bio-sensing device included in an RFID microchip' for the purpose of real-time monitoring of blood glucose levels, which would thereby eliminate the ongoing need for invasive testing (VeriChip, 2007b).

7.2 Treating or Tracking? Regulatory Challenges

At first blush it may be difficult to distinguish what the regulatory tensions may be in respect to human ICT implants within the context of current EU regulatory frameworks. However, given the current rate of product innovation and commercialisation, the potential breadth of applications, including therapeutic and non-therapeutic applications, the pervasive nature of

the applications, and the increasingly dynamic nature of the field, a closer look suggests that human ICT implants will amplify a number of existing challenges within the current regulatory regimes. Moreover, as illustrated by this section, these tensions and challenges are likely to be further exacerbated by the convergence of nanotechnologies with ICT, and the development of nano-based ICT human implants. In doing so, this section briefly illustrates several current and future regulatory challenges in relation to therapeutic human ICT implants, including those incorporating nanotechnologies. In doing so, this section does not specifically address the potential tensions and challenges associated with non-therapeutic applications.

However, before we can examine the potential regulatory challenges associated with nano-based ICT human implants, it is important to first consider how nanotechnology-based products and applications, including those relevant to human ICT implants, are currently regulated. A review by Bowman and Hodge (2007) of four jurisdictions – Australia, the EU, Japan and the US – highlighted that at that time, no federal legislative body had amended their frameworks to expressly include nanotechnologies. This is not to say that nanotechnologies are not regulated *per se*, with commentators (Marchant and Sylvester, 2006), (van Calster, 2006) quick to emphasise that these nano-enabled products and processes fall under pre-existing regulatory frameworks and oversight mechanisms. Indeed, those actively engaged in nano-related R&D are subject to a complex web of legislation, codes of practice, industry standards and guidelines, in conjunction with general law requirements such as tort law, contract law, consumer protection laws and occupational health and safety laws. With this being the case, the issue at hand would not appear to be whether or not nanotechnologies are regulated, but rather whether or not these current regulatory regimes are appropriate for regulating this technology.

Enthusiasm for the development of human ICT applications, including those incorporating nanotechnologies, will ensure that companies such as the VeriChip continue to invest in research activities, including implant devices. Many of these devices will, for instance, monitor and contain sensitive medical information, which may then be subsequently transmitted to an external device (Rodotà & Capurro, 2005), (Pizzetti, 2006). Such sensitive personal information will be required to be protected in accordance with traditional privacy and data protection regimes, such as the data protection directive, which is 'applicable to all technologies, including RFID' (European Commission, 2007: 6). Yet as articulated by Gadzheva (Gadzheva, 2007), 'no legislation governs specifically the implanting of RFID microchips in the human body, particularly in terms of privacy and data protection'. Accordingly, she suggests that this current oversight, when combined with the continual advances being made possible by, for example, microelectronics and nanotechnology, may be problematic in ensuring an individual's privacy is protected. It is also important to recognise that within the EU, non-therapeutic human ICT implants, regardless of whether or not they contain nano-materials, are not expressly covered by existing regulations relating to privacy and data protection.

The OECD has recommended that these specific privacy concerns relating to the collection of 'data related to identified or identifiable individuals…should be considered as a priority challenge to the adoption of the technology' (OECD, 2007). The OECD has stated that if left unaddressed, these privacy concerns may act as a barrier to the widespread adoption of the technology. This would appear to be particularly the case in relation to all current and further human ICT implants that have the potential to be used for other, non-therapeutic purposes, such as real time tracking or surveillance purposes (OECD, 2007). These potential dual

purpose applications not only raise issues in relation to privacy and security, but also with respect to informed consent, and questions relating to whether or not the system will or should be regulated as a medical device.

One way to alleviate these concerns would be to amend the current regulatory framework. However, given the inherent difficulties associated with predicting the developmental trajectories of the technologies combined with the pace of innovation, as well as the inherent functions and characteristics of future devices, it is arguably too early at this stage to fully articulate the dimensions of any such regulatory framework. Accordingly, one practical way to address potential privacy and security threats would be to encourage the early development and implementation of so-called 'privacy-enhancing-technology' or 'security and privacy-by-design' within the human ICT implant system (Henning *et al.*, 2004), (European Commission, 2007). Such an approach would provide greater flexibility and enable these systems to be specifically tailored to meet the various challenges associated with different human ICT implant applications, including nano-enabled medical devices.

Turning our attention to the public health perspective, manufacturers or importers of all new 'medical devices' will be required to subject their product to stringent pre-market testing and approval processes to ensure the safety and efficacy of each device pursuant to the requirements set out in the Council Directive 93/42/EEC (the 'Medical Devices Directive'). Importantly, any such medical devices will also be subject to stringent post-marketing surveillance systems should evidence subsequently emerge that the product raises safety concerns (Chai, 2000), (Kent & Faulkner, 2002), (Taylor, 2006). This regulatory framework will apply equally to medical devices, whether or not they incorporate ICT components, and/or nanotechnologies.

Looking specifically at public health issues and human ICT medical device implants which incorporate engineered nanoparticles, it is important to recognise that concerns have been raised in relation to the potential toxicity of some free engineered nanomaterials (Oberdörster *et al.*, 2005), (Nel *et al.*, 2006), (Teeguarden *et al.*, 2007), (Oberdörster *et al.*, 2007). However, the RS-RAE (RS-RAE, 2004) have concluded that were such nanoparticles embedded in a matrix – such as the case with a nano-enabled ICT implant – any such risks are likely to be low during the viable life of the device. However, given that relevant regulatory frameworks for medical devices are most likely to only be concerned with evaluating risks in relation to human health, tensions may arise in relation to the disposal of any such device, particularly the subsequent release of the said nanoparticles into the environment. Despite increasing research on the potential environmental impact of engineered nanoparticles, little is still known about the ultimate fate and impact of the majority of engineered nanoparticles on the environment (Colvin, 2003), (Holsapple *et al.*, 2005).

In addition to these tensions and challenges, Weckert (Weckert, 2007) has also suggested that there is the potential for therapeutic applications to converge with more controversial applications designed for human enhancement purposes. Should applications develop down this trajectory, societies will not only have to address any associated regulatory concerns, but also the myriad of broader ethical and social issues.

8 Conclusion

While considered by many to be within the realm of science fiction, human ICT implants have actually been developed for many years in a medical context. Such devices, keeping in step with developments of other fundamental technologies, are becoming increasingly complex, and functionality continues to grow. Further to this, we are now seeing simple passive technologies, such as RFID, being routinely implanted in healthy humans. While passive RFID implants have recently caused somewhat of a polemic, society has readily accepted restorative technologies such as pacemakers and deep brain stimulation systems, which have become notably advanced in their function, based on their healthcare merits.

A variety of identity related issues are already present in state of the art devices. When considering passive implants for identification, for instance, a major potential issue relates to the loss of privacy through being identified without one's consent or awareness. Despite the short communication range of today's RFID implants, there is still a risk that they may be misused for the physical tracking of a person. Placing readers at both sides of door frames would enable the detection of implants in users' arms and capturing the stored information, without the consent or even the awareness of the users. In a coercive attack, an attacker forces an authorised user to provide his identification and authentication credentials. Such a security threat may occur for any identification and authentication method, but for RFID implants it carries the risk of physical harm, as an attacker could cause injury by extracting the implant from the victim's body. Therefore, it has been argued that RFID implants may be appropriate for identification of people but, regardless of any future development of technical security solutions, they cannot provide secure authentication. Some argue further that they should be designed to be easy to clone, in order to make their extraction by an attacker unnecessary (Halamka *et al.*, 2006). Another kind of threat is that of the unauthorised replication of information on an RFID tag which may lead to a replay attack, i.e. repeating the same authentication sequence as the one provided by an authorised person and thus stealing another person's identity. Also, currently deployed RFID implants do not yet include options for the advanced encryption or tag authentication through a challenge-response protocol, which would counter the replay attack technique.

The basic foundations of advanced ICT implant devices are, however, being developed for clear medical purposes, and it is reasonable to assume that few would argue against this progress for such noble, therapeutic causes. Equally, as has been demonstrated by cosmetic surgery, we cannot assume that because a procedure is highly invasive, people will not undergo it. So, while we may be some way away, there is clear evidence that devices capable of significant enhancement will become reality, and most probably will be deployed in applications beyond their original purpose.

These applications alone introduce challenging questions. Indeed the increasing commercialisation of human ICT implants has generated debate over the ethical, legal and social aspects of the technology and its products. However, technological advancement is a part of our evolution, and the next step of forming direct bi-directional links between human and machine is moving inexorably closer. It is clearly timely to entertain the idea, and to have debate regarding the potential use of this more advanced technology in individuals with no medically discernible need. A number of wider moral, ethical and legal issues stem from such applications and it is difficult to foresee the social consequences of adoption long term which may fundamentally change our very conception of self and sense of identity. Intervention with regard to the possible negative impacts should clearly take place at an early point such that we

are not left relying on purely legal measures. Nevertheless, it has started to become a common understanding that the technology is not *per se* 'negative'.

At a legal analysis level, the implantation of ICT devices may challenge the right of bodily integrity for every human being, as a further expression of the right to self-determination. Moreover the use of human ICT implants allows the development of vast numbers of applications that will enable the tracking, tracing and profiling of the individual, as the unique number of the implant and/or the information stored on it can be linked with great certainty to an identified or identifiable natural person. The processing of such information shall follow the principles on the processing of personal data, as they are described in the European data protection directive.

The use of ICT implants, especially in the medical sector, has been most welcome as it has introduced devices such as cardiovascular pacers, cochlear implants, deep brain stimulators for Parkinson's disease, and insulin pumps. Notwithstanding the positive impact of such devices to the health condition of the patients, the restoration of human capabilities and especially the enhancement of existing ones are not free of ethical issues. Given the current situation, it is not too soon to start real debate. To this end, the European Group on Ethics in Science and New Technologies have published their opinion on the use of ICT implants and notes that implants, if not used properly, may prove to be a threat to human dignity, by at the very least not respecting an individual's autonomy and rights. Such dangers are already present with current medical ICT implant devices, where even simple basic access control is not implemented.

It is clearly evident that technological innovation will play a significant role in driving industrial innovation and economic growth in jurisdictions such as the EU. The continual convergence of emerging technologies with other, more traditional technological platforms such as ICT, promises a range of new products and applications that will enhance human health and well-being. The development of human ICT implants in particular is one such area, and this is particularly so in relation to therapeutic applications. However, at this early stage, greater regulatory and scientific certainty is required. And herein lays the challenge: regulating emerging risks, including health, privacy and security risks, against the broader public interest without compromising the development of a promising and powerful technology. The foundations for the acceptance of all human ICT implants must be themselves designed and built as a matter of priority to ensure their acceptance and commercial success.

9 Bibliography[84]

Agre, P.E. and Rotenberg, M., *Technology an Privacy: The New Landscape*, MIT Press, Cambridge, Massachusetts, 2001.

Altmann, J., 'Military Uses of Nanotechnology: Perspectives and Concerns', *Security Dialogue*, 35(1), 2004, pp. 61-79.

Anton, P. S., Silberglitt, R. and Schneider, J., *The Global Technology Revolution: Bio/Nano/Material Trends and Their Synergies with Information Technology by 2015*, RAND National Defense Research Institute, Arlington, 2001.

Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data', WP136, 20 June 2007.

Article 29 Data Protection Working Party, 'Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive', WP126, 26 September 2006.

Article 29 Data Protection Working Party, 'Working document on data protection issues related to RFID technology', WP105, 19 January 2005.

Article 29 Data Protection Working Party, 'Working document on the processing of personal data relating to health in electronic health records (EHR)', WP131, 15 February 2007.

Australian Government, Department of Health and Ageing Therapeutic Goods Administration, *A Review of the Scientific Literature on the Safety of Nanoparticulate Titanium Dioxide or Zinc Oxide in Sunscreens*, 16 January 2006.

Ayoade, J., 'Roadmap to solving security and privacy concerns in RFID systems', *Computer Law & Security Report*, Vol. 23, n° 6, 2007, pp. 555-561.

Bailey, D.V., Boneh D., Goh E-J., Juels, A., 'Covert channels in privacy-preserving identification systems', *ACM Conference on Computer and Communications Security*, 2007, pp. 297-306.

Berleur, J., Brunnstein K., (eds), *Ethics of Computing – Codes, spaces for discussion and law, Chapmand & Hall*, 1996.

Bowman, D. and Hodge, G., 'A Small Matter of Regulation: An International Review of Nanotechnology Regulation', *Columbia Science and Technology Law Review*, 2007, 8, pp. 1-36.

Buchta, A., Dumortier J., Krasemann H., 'Chapter 5: The Legal and Regulatory Framework for PRIME', in Simone Fischer-Hübner & Christer Andersson (ed.), *D14.0.a: Framework V0*, PRIME (Privacy and Identity Management for Europe) Project, 15 June 2005.

Bungard, D. *et al.*, Orientierungshilfe 'Datenschutzgerechter Einsatz von RFID', Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 2006.

Bygrave, L., *Data Protection Law – Approaching its Rationale, Logic and Limits*, Kluwer International, 2002.

[84] Note that all hyperlinks were last accessed on the 30.09.2008 unless otherwise indicated.

Carey, P., *E-Privacy and Online Data Protection*, Butterworths, 2002.

Chai, J.Y., 'Medical Device Regulation in the United States and the European Union: A Comparative Study', *Food and Drug Law Journal*, Vol. 55, 2000, pp. 57-80.

Clarke R., *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, 1997, available online at: http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Colvin, V.L., 'The potential environmental impact of engineered nanomaterials', *Nature Biotechnology*, 21(10), 2003, pp. 1166-1170.

Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the committee of the regions – Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*, COM(2007)96 final.

Commission of the European Communities, *Results of the Public Online Consultation on Future Radio Frequency Identification Technology Policy; "The RFID Revolution: Your voice on the Challenges, Opportunities and Threats"*, Brussels, 15.3.2007, SEC (2007) 312, COM(2007) 96 final.

Cosgrove, G. R., 'Neuroscience, Brain, and Behavior V: Deep Brain Stimulation', Transcript – session 6, June 25, The President's Council on BioEthics, 2006, http://www.bioethics.gov/transcripts/june04/session6.html

Cuijpers, C., Roosendaal A. & Koops B.J. (ed.), *D11.5: The legal framework for location based services in Europe*, FIDIS (Future of Identity in the Information Society) Project, 12 June 2007.

De Bot, D., *Verwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001, p.403.

Delgado, J. M., 'Instrumentation, working hypotheses, and clinical aspects of neurostimulation', *Applied Neurophysiology*, 40 (2–4), 1977, pp. 88-110.

Dumortier, J. & Goemans, C., "Privacy Protection and Identity Management", in Blažič, B., Schneider, W., Security and Privacy in Advanced Networking Technologies, Ios Press, 2004, p.193.

ECP. NL., *Privacyrechtelijke aspecten van RFID*, report prepared by the ECP.NL. Platform voor eNederland for the Dutch Ministry of Economic Affairs and in cooperation with the RFID Platform Nederland and GSI Nederland, May 2005, available online at http://www.rfidconsultation.eu/docs/ficheiros/Privacyrechtelijke_aspecten_van_RFID.pdf

EICAR European Expert Group for IT-Security, Task force on RFID, *Leitfaden: RFID und Datenschutz*, http://www.eicar.org/rfid/infomaterial/RFID-Leitfaden-100406.pdf

Elliot, V., 'Speed through the check out with just a wave of your arm', *The Times*, 10 October 2006, available online at: http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article666972.ece

EU Press Release, *Commission proposes a European policy strategy for smart radio tags*, IP/07/332, Brussels/Hannover, 15 March 2007.

Eudes, Y., 'Digital boys', *Le Monde*, 11.4.2006, pp. 22-23.

European Court of Justice, Lindqvist v. Sweden, 6 November 2003, Case C-101/01, 50.

European Data Protection Supervisor, 'Opinion on the communication from the Commission and the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007) 96', 20 December 2007.

Fawcett, E., 'The Toronto Resolution', *Accountability in Research*, Vol. 3, 1994, pp. 69-72.

Fiedeler, U., Krings B. J., 'Naturalness and Neuronal Implants – Changes in the perception of human beings', *EASST-Conference*, Lausanne, Switzerland, 2006.

Fischer-Hübner S. & Hedbom, H. (ed.), *D12.3: A Holistic Privacy Framework for RFID Applications*, FIDIS (Future of Identity in the Information Society) Project, 2007. Available at: http://www.fidis.net/

Flint, D., 'RFID tags, security and the individual', Computer Law & Security Report, Vol. 22, 2006, p.165.

Fukuyama, F., *Our Posthuman Future; Consequences of the biotechnology revolution*, New York: Picador, 2002.

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

Garfinkel, S. L., Juels, A., Pappu A., 'RFID Privacy: An Overview of Problems and Proposed Solutions', *IEEE Security & Privacy* 3(3), 2005, pp. 34-43.

Garfinkel, S., "An RFID Bill of Rights", *Technology Review*, October 2002, p. 35.

Gasson, M. N., Hutt, B. D., Goodhew, I., Kyberd, P., and Warwick, K., (2005a) 'Invasive Neural Prosthesis for Neural Signal Detection and Nerve Stimulation', *International Journal of Adaptive Control and Signal Processing*, Vol.19:5, 2005, pp. 365-75.

Gasson, M. N., Wang, S. Y., Aziz, T. Z., Stein, J. F., and Warwick, K., (2005b) 'Towards a Demand Driven Deep-Brain Stimulator for the Treatment of Movement Disorders', *MASP2005, 3rd IEE International Seminar on Medical Applications of Signal Processing*, London, UK, 3-4 November 2005, pp. 83-86.

Glasser D. J., Goodman J. W., Einspruch N. G., 'Chips, tags and scanners: Ethical challenges for radio frequency identification', *Ethics and Information Technology*, 2006.

Graafstra, A., (2007) 'Hands On', *IEEE Spectrum*, 44:3, pp. 18-23.

Halamka, J., Juels, A., Stubblefield, A., Westhues, J., 'The Security Implications of VeriChip cloning', *Journal of the American Medical Informatics Association*, Vol. 13, 2006, pp. 699-707, http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/verichip/Verichip.pdf

Halperin, D., Heydt-Benjamin, T.S., Fu, K., Kohno, T., Maisel, W.H., 'Security and privacy for implantable medical devices', *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, Vol. 7, No. 1, 2008.

Hansson, S.O., 'Implant Ethics', *Journal of Medical Ethics*, Vol. 31, No. 9, 2005, pp. 519-525.

Hartman, R.G., 'The Face of Dignity: Principled Oversight of Biomedical Innovation', *Santa Clara Law Review* Vol. 47, No1, 2007, pp. 55-92.

Heise Online News, 'Data protectionists call for RFID code of conduct', http://www.heise.de/english/newsticker/news/75263, 2006.

Heise Online News, ‚Neue Vorstöße zur RFID-Selbstregulierung der Industrie', http://www.heise.de/newsticker/meldung/73621, 2006.

Henning, J. E., *et al.*, *Privacy Enhancing Technology Concepts for RFID Technology Scrutinised,* Technical Report RVS-RR-04-02, University of Bielefeld, Germany, October 28, 2004, http://www.rvs.uni-bielefeld.de/cms/publications/RVS-RR-04-02

Hildebrandt, M., 'Who is Profiling Who: Invisible Visibility', in *Reinventing Data Protection?* (forthcoming, 2008).

Hildebrandt, M., Gutwirth, S. (eds), *Profiling the European Citizen - Cross-Disciplinary Perspectives*, Springer, 2008.

Hitachi, *Hitachi RFID Solutions*, 2007, available at: http://www.hitachi-eu.com/mu/

Hogle, L.F., 'Enhancement Technologies and the Body', *Annual Review of Anthropology*, Vol 34, 2005, pp. 695-716.

Holsapple, M. P., *et al.*, 'Research Strategies for safety Evaluation of Nanomaterials, Part II: Toxicological and Safety Evaluation of Nanomaterials, Current Challenges and Data Needs', *Toxicological Sciences*, Vol. 88, No.1, 2005, pp. 12-17.

Holznagel B. & Sonntag M., 'A Case Study: The JANUS Project' in Nicoll, C., et al (eds.), *Digital Anonymity and the Law – Tensions and Dimensions*, TMC Asser Press, The Hague, 2003.

Hossain, P., Seetho, I. W., Browning, A. C. and Amoaku, W. M., 'Artificial means for restoring vision', *BMJ*, 330, 2006, pp. 30-3.

ICAO, *Machine Readable Travel Documents - Technical Report Development of a logical data structure – LDS for optional capacity expansion technologies, Revision –1.7, 18.05.2004*, available online at: http://www.icao.int/mrtd/download/documents/LDS-technical%20report%202004.pdf.

Israel, C. and Barold, S., 'Pacemaker Systems as Implantable Cardiac Rhythm Monitors', *American Journal of Cardiology*, Vol. 88, No. 4, 15 August 2001, pp. 442–445.

ITU, *The internet of things, Executive summary*, November 2007, available online at http://www.itu.int/internetofthings/

Juels, A., 'RFID security and privacy: a research survey', *IEEE Journal on Selected Areas in Communications*, Vol.24, No2, 2006, pp. 381-394.

Juels, A., Brainard, J.G., 'Soft blocking: flexible blocker tags on the cheap', Proceedings of the 2004 ACM workshop on Privacy in the electronic society, 2004, pp.1-7.

Juels, A., Rivest, R.L., Szydlo, M., 'The blocker tag: selective blocking of RFID tags for consumer privacy', Proceedings of the 10th ACM conference on Computer and communications security, 2003, pp 103-111.

Kardasiadou Z. & Talidou Z., *Legal issues of RFID technology*, Legal-IST, IST-2-004252-SSA, D15, 2006.

Kent, J. and Faulkner, A., 'Regulating human implant technologies in Europe - understanding the new era in medical device regulation', *Health, Risk & Society*, Vol. 4, No.2, 2002, pp. 189-209.

Kent, J., 'Malaysia car thieves steal finger', *BBC News*, Kuala Lumpur, 2005.

Kessler, D. A., 'The basis of the FDA's decision on breast implants', *New England Journal of Medicine*, Vol. 326, No.25, 1992, pp. 1713–1715.

Koops, B. J. & Groothuis, M., 'Constitutional Rights and New technologies in the Netherlands', in: Leenes, R.E., Koops, E.J. and De Hert, P. (Eds.), *Constitutional Rights and New Technologies*, T.M.C. Asser Press: The Hague, 2007, pp. 159-197.

Koops, E.J., Van Schooten, H. & Prinsen, M.M., *Recht naar binnen kijken*, ITeR 70, Sdu Publishers, The Hague, 2004

Kosta E., Meints M., Hansen M. & Gasson M., 'An analysis of security and privacy issues relating to RFID enabled ePassports', in Venter H., Eloff M., Labuschagne L., Eloff J. and Von Solms R. (eds.), *New approaches for Security, Privacy and Trust in Complex Environments*, IFIP International Federation for Information Processing, Volume 232, Boston, Springer, 2007, pp. 467 – 472.

Kuner, Ch., *European Data Protection Law – Corporate Compliance and Regulation*, Oxford University Press, Second edition, 2007.

Lebedev, M., Nicolelis, A., 'Brain-machine interfaces: past, present and future', *Trends in neurosciences,* 29 (9), 2006, pp. 536-546.

Leenes, R.E., Koops, E.J. and De Hert, P., *Constitutional Rights and New Technologies – A comparative study*, T.M.C. Asser Press, The Hague, 2007.

Marc Langheinrich, 'RFID and privacy', in Milan Petkovic and Willem Jonker(eds.), *Security, Privacy, and Trust in Modern Data Management*, Springer, Berlin Heidelberg New York, July 2007, pp. 433–450.

Marchant, G. E. and Sylvester, D. J., 'Transnational Models for Regulation of Nanotechnology', *The Journal of Law, Medicine & Ethics*, 2006, 34(4), pp. 714-725.

Marshall, K. P., 'Has Technology Introduced New Ethical Problems?', *Journal of Business Ethics*, Vol.19, 1999, pp. 81-90.

Maynard, A. D., 'Nanotechnology: A research strategy for addressing risk', *Project on Engineering Nanotechnologies*, Vvol. 3, July 2006.

Maynard, A. D., *et al.*, 'Safe handling of nanotechnology', *Nature* (444) 16 November 2006, pp. 267-269.

McGee, E. M. and Maguire, G. Q., 'Becoming borg to become immortal: regulating brain implant technologies', *Camb Q Healthc Ethics*, Summer 2007, 16(3), pp. 291-302.

Millán, J., *et al.*, 'Brain-actuated interaction', *Artificial Intelligence*, 159, 2004, pp. 241-259.

Moan, C. E., and Heath, R. G., 'Septal stimulation for the initiation of heterosexual activity in a homosexual male', *Journal of Behavior Therapy and Experimental Psychiatry,* 3, 1972, pp. 23-30.

Moor, J. H., 'Why we need better ethics for emerging technologies', *Ethics and Information Technology*, Vol. 7, 2005, pp. 111-119.

Müller J., 'Ist das Auslesen von RFID-Tags zulässig?', *DuD* 28, 2004, p. 215.

Münzberg, H., 'Aufklärung der Konsumenten wird der Knackpunkt für RFID', Capgemini, 2005 http://www.de.capgemini.com/presse/pressemitteilungen/archiv_2005/rfid/

National Nanotechnology Initiative, Nanotech Facts: *What is Nanotechnology?*, 2007, available at: http://www.nano.gov/html/facts/whatIsNano.html

Nel, A., *et al.*, 'Toxic Potential of Materials at the Nanolevel', *Science*, 311, 2006, pp. 622-627.

Oberdörster, G., *et al.*, 'Review: Principles for characterizing the potential human health effects from exposure to nanomaterials: elements of a screening strategy', *Particle and Fibre Toxicology*, 2(8), 2005, pp. 1-35.

Oberdörster, G., Stone, V., Donaldson, K., 'Toxicology of nanoparticles: A historical perspective', *Nanotoxicology*, 1(1), 2007, pp. 2-25.

OECD, *Radio Frequency Identification (RFID): A Focus on Information Security and Privacy*, Working Party of Information Security and Privacy, Paris, 2007.

Olds, J., and Milner, P. M., 'Positive reinforcement produced by electrical stimulation of septal area and other regions of rat brain', *Journal of Comparative and Physiological Psychology, 47,* 1954, pp. 419–427.

Perakslis, C., Wolk, R., 'Social acceptance of RFID as a biometric security method', *IEEE Technology and Society Magazine*, Vol. 25, No. 3, 2006, pp. 34 – 42.

Pitkänen, O. & Niemelä M., 'Privacy and data protection in Emerging RFID-Applications', *Paper presented at the EU RFID Forum 2007, RFID Academic Convocation*, 14 March 2007, available online at: http://www.rfidconvocation.eu/Papers%20presented/Business/Privacy%20and%20Data%20Protection%20in%20Emerging%20RFID-Applications.pdf

Pizzetti, F., 'The Challenge of RFID Technology', *paper presented at the European Data Protection Spring Conference*, Budapest, 24-25 April 2006.

Quinn, M. J., *Ethics for the Information Age*, Pearson, 2006.

Quirchmayr, G. & Wills, C. C., 'Data Protection and Privacy Laws in the Light of RFID and Emerging Technologies', in Lambrinoudakis C., Pernul G., Tjoa A.M. (Eds.), *Trust, Privacy and Security in Digital Business*, TrustBus 2007, LNCS 4657, Springer Berlin / Heidelberg, 2007, pp.155-164.

Reuter, L., 2003. *Modern Biotechnology in Postmodern Times?*, Dordrecht: Kluwer Academic Publishers, p. 57.

Rieback, M., Crispo, B., Tanenbaum, A.S., 'Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags', *Security Protocols Workshop*, 2005, pp 51-59.

Rodotà, S., and Capurro, R. (eds), *Ethical Aspects of ICT Implants in the Human Body*, Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, 2005, pp. 18-23D.

Rodrigues, R., 'The Implications of High-Rate Nanomanufacturing on Society and Personal Privacy', *Bulletin of Science, Technology & Society*, 2006, 26(1), pp. 38-45.

Romo, R., Hernandez, A., Zainos, A., Brody, C. D., Lemus, L., 'Sensing without touching: psychophysical performance based on cortical microstimulation', *Neuron*, 26, 2000, pp. 273-8.

Rotter, P., 'A Methodological Framework for the Assessment of Security and Privacy Risk for RFID Systems', *IEEE Pervasive Computing* (forthcoming, 2008).

Rouse, J. G., *et al.*, 'Effects of Mechanical Flexion on the Penetration of Fullerene Amino Acid-Derivatized Peptide Nanoparticles through Skin', *Nanoletters* Vol.7, No.1, 2007, pp. 155-160.

Royal Society and Royal Academy of Engineering, *Nanoscience and nanotechnologies: Opportunities and uncertainties*, RS-RAE, London, 2004.

Sandel, M., *The Case against Perfection; Ethics in the age of genetic engineering*, Cambridge, Massachusetts, London, The Belknap Press of Harvard University Press, 2007.

Sharp, L. E., *Bodies, commodities, and biotechnologies: death, mourning, and scientific desire in the realm of human organ transfer*, New York, Columbia University Press, 2007.

Smith, J.R., *et al.* 'RFID-based techniques for human-activity detection', *Communications of the ACM (Special issue on RFID)*, Vol. 48, no. 9, September 2005, pp. 39 – 44.

Sotto, L. J., 'An RFID Code of Conduct', *RFID journal*, available at: http://www.rfidjournal.com/article/view/1624/, 2005.

Stajano, F., Anderson, R. J., 'The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks', *Security Protocols Workshop*, 1999, pp. 172-194.

Talwar, S. K., Xu, S., Hawley, E. S., Weiss., S. A., Moxon, K. A., and Chapin, J. K., 'Rat navigation guided by remote control', *Nature*, 417, 2002, pp. 37-8.

Taylor, M. R., 'Regulating the Products of Nanotechnology: Does FDA Have the Tools It Needs?', Woodrow Wilson International Centre for Scholars, Washington DC, 2006.

Teeguarden, J. G., *et al.*, 'Particokinetics In Vitro: Dosimetry Considerations for In Vitro Nanoparticle Toxicity Assessments', *Toxicological Sciences*, 95(2), 2007, pp. 300-312.

Thacker, E., *The Global Genome; Biotechnology, Politics, and Culture*, Cambridge, Massachusetts: The MIT Press, 2005.

The Royal Society & The Royal Academy of Engineering, Nanoscience and nanotechnologies: opportunities and uncertainties, *Nanoscience and nanotechnologies*, July 2004, pp. 2-11.

UK RFID Council, *A UK code of practice for the use of radio frequency identification (RFID) in retail outlets*, release 1.0, 2006.

van Calster, G., 'Regulating Nanotechnology in the European Union', *Nanotechnology Law & Business,* 3(3), 2006, pp. 359-372.

van der Ploeg, I., 'Biometric Identification Technologies: Ethical Implications of the Informatization of the Body', *BITE Policy Paper,* no. 1, 2005.

van Est R., Malsch I. & Rip A., *Om het kleine te waarderen... Een schets van nanotechnologie: publiek debat, toepassingsgebieden en maatschappelijke aandachtspunten*, Den Haag: Rathenau Instituut, 2004.

Venkatasubramanian K. & Gupta S., 'Security for Pervasive Healthcare,' Security in Distributed, Grid, Mobile, and Pervasive Computing, Xiao Y. (ed.), CRC Press, 2007, pp. 349–366.

VeriChip, 'Company: Our RFID Tags', 2007a, available at: www.verichipcorp.com.

VeriChip, 'News Release: VeriChip Corporation to Unveil Plans for Self-Contained Implantable RFID Glucose-Sensing Microchip at Grand Hyatt in New York on December 4', 28 November 2007b, available at: http://www.verichipcorp.com/news/1196258532

Want, R., 'The Bionic Man', *IEEE Pervasive Computing*, Vol. 8, 2008, pp 2-4.

Warwick, K., 'Cyborg morals, cyborg values, cyborg ethics', *Ethics and Information Technology*, Vol. 5, 2003, pp 131-137.

Warwick, K., Gasson, M. N., Hutt, B. D., Goodhew, I., Kyberd, P., Andrews, B. J., Teddy, P., and Shad, A., 'The Application of Implant Technology in Cybernetic Systems', *Archives of Neurology*, Vol.60(5), 2003, pp. 1369-73.

Warwick, K., *Identity and Privacy Issues raised by Biomedical Implants*, IPTS Report 67, 2002, available at: http://ipts.jrc.ec.europa.eu/home/report/english/articles/vol67/IPT5E676.htm.

Weber, K., 'Privacy invasions', *EMBO reports*, 7, 2006, pp. s36-s39.

Weber, K., 'The next step: privacy invasions by biometrics and ICT implants', *ACM Ubiquity*, Vol. 7, Issue 45, 2006, pp 1-18.

Weckert, J., 'An approach to nanoethics', in G. Hodge, D. Bowman and K. Ludlow (eds), *New Global Regulatory Frontiers in Regulation: The Age of Nanotechnology*, Cheltenham, Edward Elgar, 2007, pp. 49-66.

Wichmann, T. and DeLong, M. R., 'Deep Brain Stimulation for Neurologic and Neuropsychiatric Disorders', *Neuron*, 52:1, 2006, pp. 197-204.

Wolinksky, H., 'Tagging products and people', *EMBO reports*, 7(10), 2006, pp. 965-968.

Wolpaw, J., *et al.*, 'Brain-computer interfaces for communication and control', *Clinical Neurophysiology,* 113, 2002, pp. 767-791.

Wood, D. M., (ed.), *A Report on the Surveillance Society – For the Information Commissioner by the Surveillance Studies Network*, 2006, http://www.privacyconference2006.co.uk/index.asp?PageID=10

Wood, S., Jones, R., Geldart, A., 'The Social and Economic Challenges of Nanotechnology', *Economic and Social Research Council*, London, 2003.

Wustenberg, W., 'Effective Carcinogenicity Assessment of Permanent Implantable Medical Devices: Lessons from 60 years of Research Comparing Rodents with Other Species', 2007 available at: http://www.verichipcorp.com/files/RodentSarcomagenesis092807Wustenberg.pdf

Zeng, F. G., 'Trends in cochlear implants', *Trends in Amplification*, 8(1), 2004 pp. 1-34.

Zoontjens, P. J. J., 'Artikel 11', in: Koekkoek, A.K. (Ed.), *De Grondwet*, Deventer, W.E.J.Tjeenk-Willink, 2002.

Zwenne G-J. & Schermer B., *Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen* [Privacy and other legal aspects of RFID: unique identification from a distance of products and people], s-Gravenhage, Elsevier Juridisch, 2005, http://www.nvvir.nl/doc/rfid-tekst.pdf