European Parliament

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Economic and Monetary Affairs

Employment and Social Affairs

Environment, Public Health and Food Safety

Industry, Research and Energy

Internal Market and Consumer Protection

The Use of Chip Implants for Workers

Study for the EMPL Committee

EN

2017

The Use of Chip Implants for Workers

DIRECTORATE GENERAL FOR INTERNAL POLICIES
POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY

The Use of Chip Implants for Workers

STUDY

Abstract

This paper briefly explains the technology of RFID chip implants; explores current applications; and considers legal, ethical, health, and security issues relating to their potential use in the workplace.

Compulsory use would be likely to encounter legal and ethical challenges. Even voluntary use might be subject to challenges, for example, on data protection grounds. It seems that the risks of adverse health effects in humans might be considerably less than some have suggested, although they cannot be entirely discounted without better evidence. Contrarily, although there are indications of improvements in recent years, the benefits in terms of enhanced security might not be deliverable with the vulnerability of current RFID chip technology.

This document was prepared by Milieu/IOM Ltd at the request of the Committee on Employment and Social Affairs of the European Parliament

IP/A/EMPL/2017-12
PE 614.209

January 2018
EN

This document was requested by the European Parliament's Committee on Employment and Social Affairs (EMPL).

AUTHOR(S)

Richard GRAVELING, IOM Consulting Ltd, Edinburgh, UK.
Thomas WINSKI, IOM Consulting Ltd, Edinburgh, UK.
Ken DIXON, IOM Consulting Ltd

Contributions by:
David CABRELLI, School of Law, University of Edinburgh, Edinburgh (legal)
Marc DESMULLIEZ, School of Engineering and Physical Sciences, Heriot Watt University, Edinburgh (technical)
Murdo MACDONALD, Society, Religion and Technology Project, Church of Scotland, Edinburgh (ethical)

Peer review:
Hilary Cowie, IOM Consulting Ltd, Edinburgh, UK.
Joanne Crawford, IOM Consulting Ltd, Edinburgh, UK.
Claire Dupont, Milieu Ltd, Brussels

RESPONSIBLE ADMINISTRATOR

Stefan SCHULZ

EDITORIAL ASSISTANT

Laurent HAMERS

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact Policy Department A or to subscribe to its newsletter please write to:
Policy Department A: Economic and Scientific Policy
European Parliament
B-1047 Brussels
E-mail: Poldep-Economy-Science@ep.europa.eu

Manuscript completed in January 2018

This document is available on the Internet at: http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

CEO	Chief executive officer
CT	Computed Tomography
ECHR	the European Convention on Human Rights
EU	European Union
FDA	Food and Drug Administration
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
ID	Identification
ISO	International Organization for Standardization
MIM	Man-in-the-middle
MRI	Magnetic resonance imaging
PIN	Personal Identification Number
RFID	Radio-Frequency IDentification
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom

LIST OF FIGURES

EXECUTIVE SUMMARY

Background

This paper presents various issues relating to the possible use of RFID chip implants in the workplace. Commissioned against a background of awareness of a growing number of voluntary uses of implants, it briefly explains RFID chip technology; explores current applications; and examines the legal, ethical, health and safety, and security issues relating to their potential use in the workplace.

The Technology

Implantable **RFID chips** consist of three parts: an **integrated circuit** that stores information, a means of acquiring **power** for that circuit, and an **antenna** for receiving and transmitting signals between that circuit and an (external) **reader**. These parts are encapsulated within a biocompatible material (usually a form of glass) for insertion under the skin. Some versions of the chips, such as those implanted in animals usually incorporate a coating that apparently promotes cell growth around the chip.

The chip is used in conjunction with a reader that broadcasts an electromagnetic signal that any RFID chip within its range and signal frequency will respond to. Drawing its power from this signal, the RFID chip responds with an encrypted signal that is decoded by the reader. The information contained in this signal depends on the application. Thus, in the case of a simple implanted RFID chip used for identification, the signal might be some form of identification code which is processed and analysed to permit (or refuse) access. More complex approaches can involve including a secondary form of identification on the chip, such as a photograph of the wearer for biometric analysis, or a retinal scan for similar purposes. In some applications, such as medical uses, the chip can also carry information about the wearer such as medical notes.

Use in the Workplace and Elsewhere

Estimates of the extent of the use of RFID chip implants across all applications in humans vary from 2 000 to 10 000 worldwide, although there is no systematic record. It could be suggested that those providing such numbers have a degree of vested interest in maximising their profile.

Chips almost all seem to have been implanted solely on a voluntary basis, not always for work-related applications. One exception might be within the Mexican Attorney General's Office where press reports suggest that a large number of staff were chipped as part of an access-control system for part of the department (some reports also suggest that they were also intended as an anti-kidnap measure). Reports do not indicate whether or not this was voluntary.

Legal Issues

Although other legislation is relevant, the main legal challenges to the compulsory use of RFID chips in the workplace would seem to derive from data protection and human rights legislation. Even where RFID chip use was truly voluntary this legislation would still be relevant, especially in respect of data protection. In the case of voluntary applications, it would be necessary to ensure that the use was genuinely voluntary and that no disadvantage was seen to accrue to those individuals who declined to have a chip implanted or that any pressures (direct or indirect) were exerted on those invited to participate.

Ethical Concerns

In an overlap with legal arguments, ethical concerns stem in part from Articles 1 and 3 of the Charter of Fundamental Rights of the EU relating to the inviolability of human dignity and the human body. Further ethical issues relate to health and safety concerns; the efficacy of

the technology as a secure system; equity and choice; and (again in a parallel with legal issues) religious concerns.

Health and Safety Worries

Concerns have been expressed over the health and safety of RFID chip implants in four main areas: carcinogenicity; migration; interactions with MRI signals and the impact on pharmaceutical effectiveness. There have been no systematic studies of health impacts in human wearers.

There are a number of reports of carcinogenic effects, mainly in specific strains of mice. However, it appears that this probably reflects the unique sensitivity of these species and is not a trans-species phenomenon. Potential mechanisms suggest any similar effects in humans to be unlikely (although currently impossible to discount completely with the present state of knowledge).

Studies of the potential interactions between MRI scanning and chip implants appear to have excluded any significant effects, although local details on a scan can be physically masked by the chip overlying the area of interest. This problem can easily be overcome by inserting the chips into areas of the body where scans are not likely to be required.

It is suggested that inter-species differences in the characteristics of sub-dermal layers makes significant migration unlikely, although this cannot be categorically excluded. Early reports of implanted chips suggested the upper arm as an injection site, although more recent applications seem to favour the web of skin between the thumb and first finger (usually of the left hand in right-hand dominant individuals). This has the benefit of being relatively unobtrusive as well as perhaps less likely to encounter significant migration due to anatomical constraints compared to the upper arm.

Concerns regarding the impact of RFID technology on the efficacy of pharmaceuticals appear to stem from the proposed use of RFID tags as a security measure to label containers of pharmaceuticals. This would therefore involve scanning of the bulk compound. Any risk of an effect *in vivo* in scanning the compound circulating within the blood stream when briefly scanning for an RFID chip would be extremely limited as only a small proportion of the substance would be exposed during scanning.

Possible Security Problems

It would seem that, at present, the RFID chip technology (which is essentially similar to that used in credit cards and similar smart card systems) is not entirely secure. Security concerns include eavesdropping; cloning; disabling; and unauthorised tag modification. Although since their initial development there have been a number of schemes promoted to increase their security, usually with some form of encryption, it seems from the literature that each idea is swiftly followed by other researchers reporting some way of breaching the security measure proposed.

Overall Themes

One integrated theme regarding the use of RFID chips in the workplace would seem to be that of human rights; covering the inviolability of the human body and an individual's right to privacy. These issues would seem to reflect both ethical concerns and the legal provisions currently in place safeguarding those rights. It would seem that legal measures to reduce those rights, in order to allow compulsory RFID chip implants in the workplace, would need to reflect over-riding demands, perhaps on the grounds of national security, sufficient to justify overturning those provisions. As part of this it would almost certainly be necessary to demonstrate that there was no effective alternative to their use. The evidence that the RFID technology is insecure can be seen as undermining the case for such a development, at least at present.

However, even were such technological challenges to be overcome, it must be recognised that the use of such implants evokes strong objections (including religious concerns) and any compulsion would need to provide for appropriate exemptions in such circumstances.

Given such challenges, unless there is seen to be an overwhelming need or demand for implantable RFID chips in the workplace, then adopting a waiting game would seem to be the preferred option.

Where implant use is voluntary (as is the case at present) then legal considerations in respect of data protection still apply with regard to any information which might be collected by data logging systems as part of such use regarding access, patterns of use, etc. It has also been suggested that a degree of regulation of their implantation is desirable, whether implantation is voluntary or compulsory.

1. INTRODUCTION: OBJECTIVES OF THE PAPER

This paper presents various issues relating to the possible use of RFID chip implants in the workplace.

Specifically, the paper addresses:

- Current state of play regarding the use of radio-frequency identification (RFID) chip implants for workers, by exploring the technology involved (Summary of Technology Involved, Chapter 2); and ongoing and planned cases of workplace use (Workplace Uses, Chapter 3).
- Issues associated with the use of chip implants for workers:
    - Legal issues (Chapter 4).
    - Ethical considerations (Chapter 5).
    - Health and safety hazards/risks (Chapter 6).
    - Security issues (Chapter 7).

A concluding chapter then draws these various strands together in an integrated narrative (Chapter 8).

Although a number of extensive reviews on RFIDs and implants have been identified, these are frequently not specific to RFID implants, nor do they usually relate to their use in a workplace context. For example, Sade (2007) writes of RFIDs in a medical context in addressing the ethical issues (where medical benefits add a further layer of complexity to be considered) while Hildebrandt and Anrig (2012) write of the ethical issues relating to Information and Communication Technologies (ICT) implants in general, not just RFIDs. The present paper extracts issues from these commentaries relevant to implanting RFIDs in a workplace context.

Implantable RFID chips can be passive – designed to be 'read only' – or active, where data can be stored on the chip and the device has a 'read-write' capability. Although chips are also available that transmit a signal (allowing them to be used for tracking applications) the power requirements for such devices mean that they need to be a larger size (to contain a battery capable of storing and providing the necessary power) or need to be connected to a separate power source. Both of these factors mitigate against their ready use as implanted devices. Only the passive devices are considered in this paper, although many of the considerations concerning their use will also apply to active devices.

2. SUMMARY OF TECHNOLOGY INVOLVED

KEY FINDINGS

- RFID chips come in passive and active forms with the passive form primarily addressed in this paper.
- Passive chips are 'read only', allowing information stored on them to be accessed by an appropriate reader. Active chips are 'read & write' allowing additional information to be written to the chip *in situ*.
- The first implantable RFID chips for humans were patented in around 1997.
- The biocompatibility of RFID chips is covered by parts of ISO 10993.
- The RFID chip contains an antenna, a power storage device and an integrated circuit.
- RFID chip systems require the chip, a reader and a network and/or a computer.

This Chapter briefly explores (and explains) the basic form and function of implantable RFID chips.

The particular type of chip in question is known as a passive RFID (read only) as opposed to more sophisticated 'active' devices which can have additional data added to them in-situ or can transmit a tracking signal (Sade, 2007). As noted earlier, this paper refers primarily to the passive versions as these are the type used in existing workplace applications. However, the use of active RFID chips is briefly considered where appropriate.

The engineering principles underlying current RFID technology were first reported in 1948 (Stockman, 1948). However, the first patent for using human-implanted RFID chips was not granted until July 1997 as "an apparatus for tracking and recovering humans"[1]. A "syringe-implantable" device for animal use had been patented a few years earlier in 1993[2].

The patented device was intended to be used as a safeguard against kidnapping and to facilitate prompt medical emergency procedure in the case of acute illness, for example a heart attack. In 2004, a human-implantable microchip, called VeriChip®, received FDA approval as a medical device.

As well as their use for animal human tagging, RFID chips are used in a wide variety of applications ranging from passport control to toxic and medical waste management (Roberts, 2006).

The chip consists of three parts: an integrated circuit, a means of acquiring power from the reader, and an antenna for receiving signals from and transmitting signals to a reader.

For human (and animal) use, these must be encapsulated within a biocompatible material (usually a form of glass). Non-implantable devices used for commercial applications or animal applications may be encapsulated in polymers that are unsuitable for human implantation.

The chip material in contact with human tissue must not harm, inflame or change the composition of that tissue. Undesirable local or system effects in the human body must be avoided. Moreover, the chemical stability of the encapsulating packaging is essential, with good resistance to attacks from the harsh internal environment. Inside the human body, hydrolytic, oxidative and enzymatic mechanisms take place that can modify the chemical structure of polymers leading to biodegradation (Donaldson, 1976). Glasses and ceramics can withstand long periods of resistance to gas or fluid ingress (defined as permeability) ranging from months, or tens of years, depending on the material thickness.

---

1 Personal tracking and recovery system US 5629678 A

2 Syringe-implantable identification transponder. US 5211129 A

Assessment of the biocompatibility of implanted medical devices is covered by ISO 10993 with extensive *in vitro* and *in vivo* tests required. Tests include cytotoxicity, sensitization, irritation, introcutaneous reactivity, acute systemic toxicity or pyrogenicity, subchronic toxicity, genotoxicity, implantation, chronic toxicity and carcinogenicity, depending on the class of medical devices considered. Implantable RFID chips would be covered by relevant parts of this Standard.

As noted above, some versions of implantable RFID chips incorporate a coating over part of the glass sheath. Various accounts present this as a non-slip layer, to reduce/prevent chip migration, or as a coating to encourage 'assimilation' into body connective tissue by supporting cell growth. Alternatively, versions without such a coating can be regarded as reducing the extent of assimilation into body tissues and therefore of easing the subsequent removal of the chip should that become necessary. However, it follows that these will be more liable to migrate, to the extent that this is possible (see Chapter 6). Figure 1 shows an example of an implantable glass RFID chip.

Figure 1: An RFID chip on a hand (for scale)

Source: Chip photos courtesy of Three Square Market, River Falls, Wisconsin

The RFID chips are used as part of a system that has four component parts:

- **The RFID chip** (also known as a tag) stores information about the chipped person and sends this information back to the reader when a signal of the correct frequency is sent to the chip by the RFID reader for interrogation. As it is a TRANSmitter and a resPONDER, RFID chips are classified as 'transponders'. As noted above, there are two main categories of chip. The passive chip gets its electrical power from the electromagnetic waves emitted by the RFID reader. The active chip has its own battery that tends to limit its useful life and add additional components to be contained within the device. Both types of chip have their own antenna (or coil).
- **The RFID reader** is a device that broadcasts an electromagnetic signal that any RFID chip within range and operating on the same frequency will respond to. Drawing its power from this signal, the RFID chip will respond with an encrypted signal. The RFID reader will decode this and pass the resulting information to a network.
- **The network** gets the decrypted information from the reader and transmits it to a computer for processing. Sometimes, a simple interface between the computer and the reader is used instead of a network.
- **The computer** (also called the host or controller) controls the RFID reader with software controls. It processes the information received from the network to enable an operator to make a decision.

The type of information transmitted depends on the application. Thus, in the case of a simple implanted RFID chip used for identification, it might be some form of identification code which is processed and analysed to permit (or refuse) access to an area or installation. More complex devices can include a secondary form of identification on the chip. For example, it is understood that a photograph of the wearer, or a retinal scan can be included which would permit the use of facial or biometric identification to enhance security.

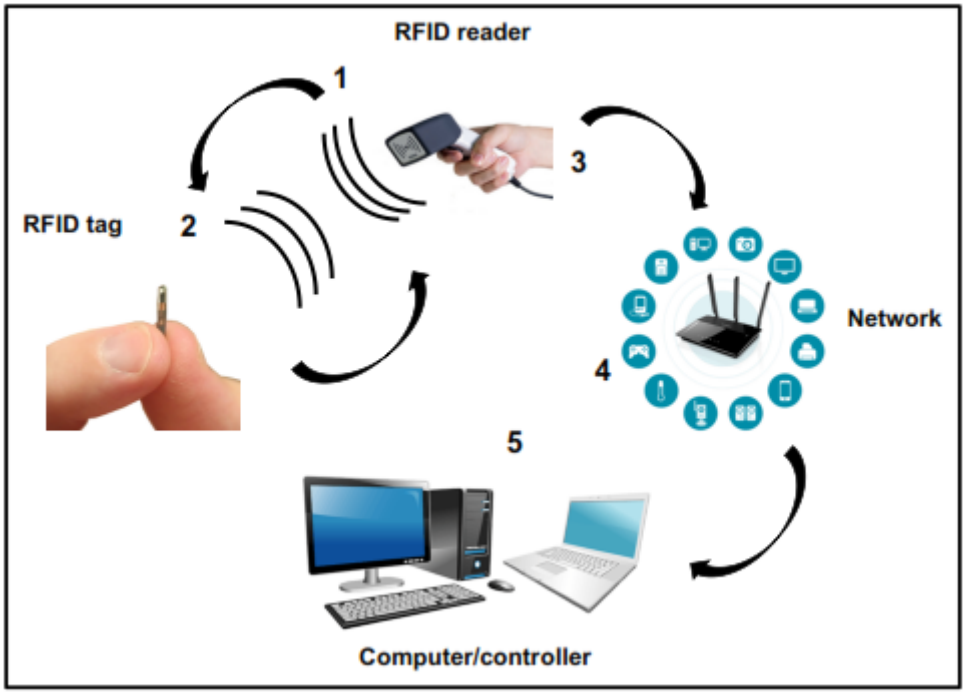
Note that the RFID reader, network and computer can physically be a single device and that the 'operator' can be an automated function. Figure 2 illustrates such a system in schematic form.

Indications of the basic operation of a chip system are provided by Hassan et al (2015), who summarised the basic operations of a RFID system (referring to tags rather than chips):

- The tag enters the RF field of the reader.
- RF signal powers the tag.
- The tag transmits its data.
- The reader captures data.
- The reader sends data to the computer.
- The computer sends data to the reader.
- (The reader transmits data to the tag) – Not in a passive device.

Not all systems necessarily include all these steps. For example, there is no necessity for data to be returned to the chip in a purely passive device (although some otherwise passive systems include such a mechanism as part of security encryption procedures). The ID and other characteristics (time, location, etc.) might then be stored on a computer for future reference and analysis.

Figure 2: Components of an RFID system and mode of operation



Source: Marc Desmulliez & Richard Graveling

The chips have the potential to have additional information stored on them, which can then be read directly without the need for recourse to other devices. This provides the basis for a number of medical applications where medical information relating to the 'wearer' is included on the chip to avoid any need to interrogate a computer system.

Although not necessary for understanding this basic functionality, the RFID chips and readers used for implantation utilise what is known as **near-field coupling** (also called **magnetic induction coupling**) in which the reader generates a magnetic field. Any device passing through the proximity of this magnetic field, such as an RFID chip, will create a voltage that can charge a capacitor in the chip. This stores enough energy to power the integral semiconductor within the chip. Once this is powered, the identification data that it holds is

then transmitted by the coil of the chip which creates its own magnetic field. This produces a disturbance in the magnetic field of the reader that the reader will detect and decode. The information represented by the decoded signal has thus wirelessly been transmitted from the chip to the reader.

Although generally presented in the context of ID systems, requiring the chip to be held close to the reader, the technology exists to install more powerful reader/transmitters. According to Singh et al (2017) the read range for passive chips is up to about 40 feet (~12 metres), although it is likely that the smaller size of chip used for implant purposes will significantly limit this range as increasing the read range of the chip requires the use of a larger antenna within it.

3. WORKPLACE USES

KEY FINDINGS

- Estimates of the number of chips implanted worldwide range from 3 000 – 10 000.
- To date, although some companies have adopted the technology, this seems to be limited to a very small (but well-publicised) number, almost all of which provide them on a purely voluntary basis.
- Most of the wearers appear to be private individuals who do so 'for convenience' (e.g. to unlock doors) or to embrace the technology.
- In terms of utility, the most significant adoption would seem to be that of the Swedish Rail company SJ who enable wearers to utilise their chip to verify ticket details.
- In a workplace context the most significant reported application would appear to be that involving the Mexican Attorney General where press reports indicate the use of RFID chips as part of enhanced security access. It is not known whether or not this use was voluntary.

3.1. Introduction

This chapter explores:

- Current and previous workplace applications.
- Current extent of workplace use.
- Current and previous workplace users.

A number of applications of RFID chip implants were identified through press and other reports on the internet. From these, contacts were identified and approached for details relating to dates adopted, type of chips used, number of workers implanted, what the chips were being used for, observations regarding their use, controversies and lessons learned. Opinions were also gathered in respect of perceptions and awareness of issues such as health and security.

Searches sought to identify **Manufacturers** of the RFID chips, **Providers** of the chips for others to apply, organisations who could be regarded as **Users** of RFID chip technology and **Wearers** (those individuals with chips inserted). As a further channel, information was sought from animal users (vets) regarding the source of their chips, in an alternative approach to identifying chip manufacturers.

3.2. Manufacture

Many of the early reports regarding the human use of RFID chips referred to a common **manufacturing** source, VeriChip®. Believed to be the first organisation to gain Food and Drugs Administration (FDA) approval for the use of their chip in humans, VeriChip® was made by VeriMed (part of PositiveID) but, in 2010, PositiveID ceased marketing the VeriChip® apparently due to 'poor acceptance'[3]. A minority partner (Digital Angel) continued to market RFID chips. However, after merging with Veriteq they also ceased marketing the devices for human implantation.

In the UK, RFID chips for animal use are **provided** by PETtrac, who also provide an accompanying animal ID service for tracing purposes. PETtrac is part of AVID ID Systems Inc who **manufacture** and **provide** these devices in North America, Spain and the UK. Enquiries through their UK base indicated that, following instructions from their US parent

[3] http://www.implantable-device.com/2011/12/30/verimeds-human-implantable-verichip-patient-rfid/

company, they do not approve their products for human use. No other animal chip manufacturer has been identified.

Enquiries of Three Square Market, a USA-based company who promote the use of RFID technology (including RFID implants) indicated that the RFID chips they provide are **manufactured** by a company called Cybernise. It has not been possible to trace this US-based company, which appears not to have any internet profile, for further information.

One source[4] suggests that Biohax (see below) buy-in the actual chip as a commercially available device, add an antenna and encapsulate these within the glass cylinder. However we have been unable to confirm this as the company is currently subject to confidentiality agreements with its supplier.

No further information regarding RFID chip manufacture for human use has been identified.

3.3. Providers, Users and Wearers

Three Square Market can be regarded as **Providers** and **Users.** They also include **wearers** amongst their workforce. In telephone discussions, the President indicated that they were relative newcomers to the field, having only adopted the technology this year. They see their main interest as the uses to which RFID chips or tags can be put – which extend beyond their use in human implants – and they primarily develop RFID applications to include implanted and non-implanted applications.

The President estimates that they have implanted around 1 000 people on a voluntary basis (although they also offer the chip in a wearable wristband option) and considered a figure of around 5 000 globally to be a reasonable estimate. He was unaware of any reports of adverse reactions to these implants, indicating that he had one personally. He regarded the implanted chip as 'noticeable', although it generally went unremarked unless attention was specifically drawn to it.

The President of Three Square Market conceded that there were issues relating to the security of the technology at present, meaning that current applications could be vulnerable, but indicated that he felt solutions to this vulnerability to be relatively close. He indicated that he understood that requiring workers to receive an implanted device was illegal in current US law.

In a recent, non-work development of interest, the Swedish rail company SJ is understood to be trialling a system where travellers can use a chip to 'store' their train ticket. Details of their ticket are stored on the SJ ticket system and their chip code provides a link to those details[5]. However, SJ are not offering to carry out implants themselves but making the ticket facility available to those who already have an RFID chip implanted. According to press reports, it is suggested that about 2 000 people in Sweden already have a chip implant.

This figure of 2 000 was reiterated by the CEO of a second company Biohax (based in Sweden), who also **Provide** and **Use** RFID chips. The CEO, himself a **wearer**, indicated that he was an early adopter of the technology having personally had a chip implant in 1996. They provide (implant) individuals with the chip for personal use, although they do encourage adopters to generate further interest through their employer. To date, the Biohax CEO has no indications of any employer persuading or coercing a worker to have an implant. He was strongly against this due to it being a violation of personal integrity. He also indicated that it would be illegal in Sweden to do so. As well as being personally responsible for implantations he has removed four chips, two of which were in himself (he experimented with alternative body sites at one time).

[4] https://www.nanalyze.com/2017/08/who-makes-rfid-chip-implants-humans/

[5] http://www.independent.co.uk/travel/news-and-advice/sj-rail-train-tickets-hand-implant-microchip-biometric-sweden-a7793641.html

He indicated that the other two were removed for personal reasons and that there were no indications of adverse effects of the implantations. However, he was very aware that the implantation process itself carried potential health risks and was strongly in favour of regulation/certification of this process to ensure that it was carried out in suitably aseptic conditions. He was aware of some of the reported health concerns (in mice) although he was not concerned as he felt that these were not applicable to humans and might be a reflection of the type of (coated) chip used.

On the issue of migration he was aware that the chips could remain mobile for some time (in that they could become realigned with other body structures) but was unaware of any more severe migration.

On security, the Biohax CEO also acknowledged the vulnerability of the technology to hacking or other interference. He indicated that he always adopted a secondary form of security such as a Personal Identification Number (PIN) where this was a concern, although for non-critical uses (such as gym access) this did not apply.

A further **provider** is the organisation Dangerous Things, who supply an RFID kit for self-administration (including an insertion syringe) over the internet[6]. Through this, any would-be **wearer** can access the technology and self-inject.

3.4. Workplace Applications

Searching the literature for examples of workplace applications regularly leads to hearsay or descriptions of workplace cases without any names or details. Below are examples of cases identified in the literature, with some available details:

- Mexican legal department – Foster and Jaeger (2007) cite a claim that "the attorney general of Mexico and 18 of his staff had chips implanted to allow them to gain access to certain high-security areas". This seems to be a reduction from earlier reports that 160 staff had received such implants with more perhaps to follow. Neither report documents whether or not this was a voluntary programme, although indications that the chips were a requirement for staff to be able to enter a new anti-crime information centre suggests a degree of compulsion[7]. Roberts (2006) also reports this application, stating that it was intended as a kidnap control measure as well as being used for access purposes.
- CityWatcher.com – Two workers were implanted with an RFID chip for the purpose of increasing the layer of security within their organisation. Ease of integration into their current system was described as an attractive quality. However, a vulnerability to hackers was later identified and shared with CityWatchers who reported to not have been aware of the vulnerability[8].
- EpicCenter – Approximately 150 workers were implanted at the beginning of January 2015. The purpose of this was to allow access through secure doors and the main benefit was reported to be convenience. No controversies were described[9].
- A Belgian marketing company NewFusion has been reported as 'offering' their workers the chips. "The chips contain personal information and provide access to the company's IT systems and headquarters, replacing existing ID cards". The report does not indicate how many have accepted the offer[10].

---

6 https://dangerousthings.com/shop/xnti/

7 http://www.nbcnews.com/id/5439055/ns/technology_and_science-tech_and_gadgets/t/microchips-implanted-mexican-officials/#.WISe5mdLFsc

8 http://www.wnd.com/2006/02/34751/

9 http://www.bbc.co.uk/news/technology-31042477

10 http://www.dailymail.co.uk/sciencetech/article-4203148/Company-offers-RFID-microchip-implants-replace-ID-cards.html

Estimates of the number of implants in use vary widely and are not available from any accredited source. The sources suggest from 2 000 to 10 000. As well as those figures indicated by providers during telephone interviews they include:

- "So far around 3,000 people in Sweden have a microchip." (2017)[11].
- "Despite the limited uses, human chip implant manufacturer Dangerous Things told AFP that there are now around 10,000 "cyborgs" — or humans with digital chips in them — across the globe." (2015)[12].
- "around 2,000 people have already been injected with RFID implants for humans" (2017)[13].

[11] http://www.dailymail.co.uk/sciencetech/article-4876326/3-000-Swedish-commuters-using-microchips-travel-cards.html#ixzz4sXaLONRl

[12] http://www.nowtheendbegins.com/over-10000-people-have-now-received-a-permanent-human-rfid-microchip-implant/

[13] https://www.nanalyze.com/2017/08/who-makes-rfid-chip-implants-humans/

4. LEGAL ISSUES

KEY FINDINGS

- Although other legislation is relevant, the main legal challenges to the compulsory use of RFID chips in the workplace would seem to derive from data protection and human rights legislation.
- Data protection would encompass ongoing and subsequent use of data acquired through chip use.
- Human rights considerations stem, in particular, from Article 8 of the European Convention on Human Rights ("ECHR"), which safeguards a worker's right to respect for his private and family life.
- The technology appears to provoke significant opposition on religious grounds amongst some parties and this might lead to issues regarding religious discrimination legislation.

4.1. Introduction: Current Legislation of Relevance

At EU level, there is no specific, tailored and/or comprehensive legislation, case law or regulatory regime banning, restricting or controlling the use of microchip implants by employers. The only foray in the EU regulatory field to date in this regard is the Active Implantable Medical Devices Directive of 1990[14] (and subsequent amendments)[15]. However, this does not prescribe how employers ought to use microchips in the workplace, but simply harmonises the use, inspection procedures and safety aspects of implantable microchips in the medical context and sector throughout the EU. For obvious reasons, this is largely irrelevant to the issue of workplace practices, although some of the issues addressed might be of relevance in a workplace context.

As such, whether employers have the power to coerce their workers to accept such implants is a matter that is governed by the general principles and rules of EU labour law and human rights law, as well as the National laws of each of the member states of the EU ("Member States").

There are six principal areas of Labour Law that will be engaged where an employer requires a worker to have a microchip implanted for the purposes of monitoring the activities or location of its workers. It is likely that, even if just used on a voluntary basis for 'simple' applications such as gaining access to a building, the potential exists for the fact that the person is within the building to be recorded and stored for future use.

The six areas are:

- Data protection regulation.
- The human rights of workers under Article 8 of the European Convention on Human Rights ("ECHR"), which safeguards a worker's right to respect for his private and family life.
- The legal obligations of the worker to follow reasonable instructions and orders of the employer, i.e. to accede to requests to microchipping.
- The law of constructive dismissal.

[14] Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices OJ No L 189 of 20 July 1990.

[15] Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market.

- Religious discrimination laws, e.g. where the implantation of a microchip under the skin of a worker or somewhere in or on the worker's body does not conform to his/her religious beliefs or amounts to a fundamental breach of that religion.
- Laws governing the ownership and continued use of the microchip and the data stored on the chip when the employment relationship is terminated.

As noted above, a number of these issues apply whether the implants are voluntary or compulsory.

4.2. Data Protection Regulation

Turning to the potential for employer liability in the case of data protection law, these laws primarily intend to ensure that workers have voluntarily consented to the collection, maintenance and processing of any personal data or sensitive personal data about them. Since microchipping involves the collection, maintenance and processing of such data, the data protection laws are engaged. Whether the actual implantation is voluntary or compulsory, consideration must be given to the purposes any information collected as a result of their implantation might be used for.

Data Protection regulation is one area where the EU has the sole power to legislate by virtue of Article 16 of the Treaty on the Functioning of the European Union (TFEU). The EU's General Data Protection Regulation ("GDPR")[16] which comes into force in May 2018 demands a very high standard of consent from workers, which must be given by **clear affirmative action** establishing a **freely given, specific, informed** and **unambiguous** indication of the worker's agreement to their personal data being processed[17]. If the employer wants to use personal data for new or different purposes, it must update the privacy notice and obtain a new consent if relying on consent to justify personal data processing[18].

An employer relying on consent to process personal data from their workers must satisfy the following requirements under the GDPR[19]:

- Consent must be specific and informed which includes information on the right to withdraw consent.
- Consent must be freely given.
- Consent must be unambiguous and take the form of an affirmative action or statement.
- For certain types of personal data processing, the consent must be explicit.
- When consent is given in a document that also concerns other matters, the request for consent must be:
    - Presented in a manner that is clearly distinguishable from the other matters.
    - In an intelligible and easily accessible form.
    - In clear and plain language.

Any failure to comply with such requirements would amount to a breach of the law, enabling a worker to claim compensation.

As noted above, even where the implantation itself is voluntary, applications of that chip within the workplace raise the potential for data protection issues if the use of that chip is

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[17] GDPR Art. 7.1

[18] See GDPR Art 13(3).

[19] See GDPR Arts 4(11), 7, 9, 49 and Recitals 32, 33 and 50.

recorded in some way by an employer. Similar considerations will also apply in the case of non-workplace uses such as a club or gymnasium.

The individual worker is still required to give their informed consent regarding the uses that any information will be put to by the employer, including any transfer to third parties; and the employer still needs to comply with each of the requirements under the GDPR.

4.3. Human Rights

The human rights of workers under Article 8 of the ECHR (which directs that "everyone has the right to respect for his private and family life, his home and his correspondence") will be engaged by workplace microchipping. The relevant issue to be resolved in this context is whether (even where the original implant is voluntary) the microchipping of workers and consequent recording of data regarding the use of that chip would constitute the collection of personal data about the worker. It would have to be decided whether that amounted to an interference with his/her 'private life', since the concept of 'private life' is construed very broadly: see Niemietz v Germany[20] and Bărbulescu v. Romania[21]. At issue is whether the restrictions on the employee's private life in terms of microchipping are proportionate. The relevant stages to be adopted in terms of the 'proportionality' test were clarified by the ECtHR in Bărbulescu v. Romania[22]. This case related to the surveillance and monitoring of an employee's electronic communications. As similar considerations might apply to the use of RFID chips, Box 1 details these stages.

Box 1: Bărbulescu v Romania

Bărbulescu v Romania [2017] IRLR 1032, 1047–1048

Judgment of the Grand Chamber of the ECtHR:

… proportionality and procedural guarantees against arbitrariness are essential. In this context, the domestic authorities should treat the following factors as relevant:

(i) whether the employee has been notified of the possibility that the employer might take measures to monitor [the microchip and data], and of the implementation of such measures. While in practice employees may be notified in various ways depending on the particular factual circumstances of each case, the [ECtHR]t considers that for the measures to be deemed compatible with the requirements of Article 8 of the [ECHR], the notification should normally be clear about the nature of the monitoring and be given in advance;

(ii) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy. In this regard, a distinction should be made between monitoring of the flow of [data stored on the microchip] and of their content. Whether all [data] or only part of [it has] been monitored should also be taken into account, as should the question whether the monitoring was limited in time and the number of people who had access to the results (see Köpke v Germany…). The same applies to the spatial limits to the monitoring;

(iii) whether the employer has provided legitimate reasons to justify monitoring the [microchip and data] and accessing their actual content... Since monitoring of the content of [the microchip and data] is by nature a distinctly more invasive method, it requires weightier justification;

(iv) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the [microchip and

[20] (1992) 16 EHRR 97.

[21] [2017] IRLR 1032.

[22] [2017] IRLR 1032.

data]. In this connection, there should be an assessment in the light of the particular circumstances of each case of whether the aim pursued by the employer could have been achieved without directly accessing the full contents of the [microchip and data];

(v) the consequences of the monitoring for the employee subjected to it… and the use made by the employer of the results of the monitoring operation, in particular whether the results were used to achieve the declared aim of the measure (see Köpke v Germany…); (vi) whether the employee had been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature. Such safeguards should in particular ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality. In this context, it is worth reiterating that in order to be fruitful, labour relations must be based on mutual trust (see Palomo Sánchez v Spain…). Lastly, the domestic authorities should ensure that an employee whose communications have been monitored has access to a remedy before a judicial body with jurisdiction to determine, at least in substance, how the criteria outlined above were observed and whether the impugned measures were lawful (see Obst… and Köpke v Germany…).

Whether an employer or a Member State of the EU is liable for a breach of human rights law will be context-dependent and vary from case to case. As such, there is no definitive answer to the question whether microchipping is unlawful under labour law, since it will depend on the nature and extent of the harm done to the worker (see Chapter 6), which is weighed against the employer's need to engage in microchipping to fulfil a legitimate commercial objective. As such, each case will turn on its own facts and circumstances.

At the core of this will be Article 8(2) of the ECHR. This states:

> *"**Article 8(2)***
>
> *There shall be no interference by a public authority with the exercise of this right[23] except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

In the context of voluntary use, the fact that the worker has consented will be a factor that tempers or dilutes the "harm" or level of interference (caused by the microchipping) to the worker for the purposes of the proportionality exercise. The lower the level of harm or interference experienced by the worker, the more likely that the microchipping will be lawful, although the employer would still need to establish that it was urgent or pressing for it to achieve a legitimate commercial objective. Additionally, freeing workers from the hassle, cost and security risks of having to have or use PINs, passcodes and access cards, or from losing them, can possibly be seen as a legitimate pressing social need or aim in justifying the intrusion[24].

A key issue will be that of proportionality. The test will be whether the harm caused by the interference associated with the microchipping is proportionate to the legitimate aim or social need invoked by the employer. This will involve a balancing of the employer's need to engage in microchipping to achieve the legitimate objective that it has identified, against the level of interference in the employee's privacy and harm done to the employee as a result. In this regard, the greater the interference or harm suffered by the employee, the more pressing and urgent it must be for the employer to apply microchipping to achieve the legitimate objective. The reality of this balancing test is that, if there is a less restrictive means of the

[23] For his private and family life, his home and his correspondence.

[24] See the discussion in J. Reidy, "One Step Closer to Robots Taking Over" (2017) 34 Business NH Magazine 33.

employer achieving the legitimate objective, then the employer – and the Member State – is likely to lose the case in any legal proceedings taken.

Nonetheless, it is opined that it would be an unusual case where an employer is not in breach of human rights law if it uses microchips in the workplace. At the very least, in cases successfully defended by an employer, it is likely that the employer's use of the device would need to be passive. It would be an exceptional case for a court to hold that there had been no breach of human rights law where the device has been used in an active capacity, or the worker has not given his/her voluntary consent at the very least, or the worker is unaware of the existence of the device. Furthermore, it would be incumbent on an employer to disclose the consequences (and also the possibility) of transference of the data to third parties, such as the police and prosecution authorities[25].

As a final point it is interesting to note that if it is alleged by an employee that his/her employer has engaged in microchipping for the purposes of conducting unlawful monitoring or surveillance of the employee's activities (in non-compliance with Article 8(2)), then any legal action raised by the employee will need to be against a Member State, rather than the employer. This is because Article 8 of the ECHR only permits vertical legal action to be taken by a private citizen against the State, on the basis that the State has failed to ensure that its National laws prevent such unlawful managerial behaviour.

4.4. Legal Duties of Workers

A further area where workplace microchipping will be affected by the Labour Laws of the Member States of the EU is in relation to the legal obligations of the worker to follow the reasonable instructions and orders of the employer, i.e. whether there is a legal duty imposed on workers to accede to requests to microchipping.

Unlike Data Protection laws, policy and legislative competence in the context of the regulation of the basic obligations of workers and employers is retained by the Member States. As such, the EU has no power to promulgate legislation in this particular context. Where an employer exercises their managerial prerogative to instruct an employee to follow one of its instructions or orders, most legal systems will support the employer's command by insisting on performance from the employee.

However, if the implantation of a microchip gives rise to health and safety issues (see Chapter 7), there is a strong argument that such a managerial instruction would be unreasonable and unlawful and the worker is under no obligation to accede to the request. For example, both German and UK law provide for exceptions where certain commands issued by employers will not be clothed with legality. In this event, the worker is not bound to conform to the instruction and will not be in breach of the law for non-performance.

Under such circumstances, it is likely that were the employer to compel the worker to be microchipped, the Labour Laws of the Member States would rule that there has been a breach of Labour Law. Such a breach will have different consequences depending on the Member State, e.g. in some Member States it will be possible for the worker to claim compensation or to treat him/herself as constructively dismissed.

Where the worker volunteers to be microchipped, this particular area of the law will assume no relevance, since this branch of the law is concerned with the legal position where a worker refuses to comply with an employer's order.

4.5. Law of Constructive Dismissal

The Member States currently maintain sole jurisdiction to promulgate laws governing the dismissal of employees and the termination of the contract of employment. However,

[25] *Bărbulescu v. Romania* [2017] IRLR 1032 and *Vukota-Bojic v Switzerland* [2017] IRLR 94.

technically, the EU does have power under Article 153(1)(d) of the TFEU to pass laws that regulate the powers of dismissal of employers.

In a number of the Member States of the EU, a concept known as "constructive dismissal" is recognised. This is not an outright dismissal by the employer, but describes a situation where an employer's behaviour is so serious that it amounts to a repudiatory breach of the employment contract, which enables a worker to treat him/herself as "constructively dismissed" and to terminate their contract. The fact that a command issued by the employer to the worker that the latter ought to be microchipped could have health and safety implications (or might run contrary to their religious beliefs) results in the engagement of the law of constructive dismissal.

It is not essential to the establishment of constructive dismissal that the employer's order is imposed without the worker's consent. Where the worker agrees to comply, but the health and safety implications for workers are so serious that the employer's behaviour qualifies as a repudiatory breach of contract, this will therefore empower the worker to make a constructive dismissal claim.

4.6. Religious Discrimination Laws

The EU has competence pursuant to Article 19 of the TFEU and has passed the Framework Directive governing the protection of employees and workers from discrimination on the basis of their religious belief. This would apply for example where the implantation of a microchip under the skin of a worker, or somewhere in or on the worker's body, does not conform to his/her religious beliefs or amounts to a fundamental breach of that religion[26]. Assuming that every worker is treated the same; and that no workers adhering to a particular religious faith (or none), are being singled out for special adverse treatment, then any claim would need to be one of indirect rather than direct religious discrimination.

For such a claim to be established, the microchipping must put workers possessing the same religious belief as the claimant worker at a particular disadvantage when compared with other workers (who do not adhere to that religious belief). The microchipping must not be objectively justifiable by the employer on the basis of a legitimate aim, or be appropriate and necessary to achieve that aim. If a less restrictive means of achieving the employer's real business need or legitimate aim is found to exist, or the microchipping cannot be shown to be appropriate and necessary, the defence will be rejected and the claim likely to succeed.

4.7. Ownership of Data

Labour and data protection laws governing the ownership and continued use of the microchip (and the data stored on the chip) will be a significant issue when the worker leaves the employment of the employer. First, the ownership of the chip itself and the data collected and stored would be governed by the express terms of the contract of employment. These terms will be produced by the employer and as such, would specify that the chip and the data are owned by the employer. In the absence of express terms, the implied default law would have to develop as the use of the technology became more pervasive in the workplace.

The GDPR explicitly provides for an individual's "right of erasure" and "right to be forgotten". When the employer initially requires the employee to be microchipped, Article 13(2) of the GDPR prescribes that it must furnish the employee with several pieces of information, and part of that information concerns the employee's "right of erasure". The employer must therefore give the employee the right to access the data collected and stored on the microchip in terms of Article 15 of the GDPR. Article 17(1) of the GDPR directs that employees have a general right to the erasure of personal data concerning them without undue delay, while

[26] Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation.

Article 17(2) of the GDPR includes a “right to be forgotten”. However, these are to some extent balanced by Article 17(3) that states that both the right to erasure under Article 17(1) and the right to be forgotten under Article 17(2) do not apply to the extent that they would collide with certain public policy interests.

This relates to the conservation of data collected as a result of the microchipping after the microchip is disabled or removed.

5. ETHICAL CONSIDERATIONS

KEY FINDINGS

- In an overlap with legal arguments, ethical concerns stem in part from Articles 1 and 3 of the Charter of Fundamental Rights of the EU that relate to the inviolability of human dignity and the human body.
- Further ethical issues relate to health and safety concerns; the efficacy of the technology as a secure system; equity and choice; and (again in a parallel with legal issues) religious concerns.

5.1. Introduction

The ethical issues surrounding the use of RFID chips implants are complex and wide reaching, often overlapping with (or interacting with) other aspects of their use. In some instances, the issues depend upon the particular field of application. For example, Monahan and Fisher (2010) raise concerns about their use in health environments, including the possibility that, perhaps because it eases the process, those patients with a chip implanted might receive some priority in treatment.

As an example of some of the ethical issues identified in a workplace context, in 2005, the European Group on Ethics in Science and New Technologies to the European Commission published an opinion on ethical aspects of ICT implants. Although its focus was much wider than RFID chip implants (which were referred to briefly in one subsection), some of the issues raised are relevant to such devices. The opinion cites Article 1 of the Charter of Fundamental Rights of the EU (2000) as stating that: "Human dignity is inviolable. It must be respected and protected"[27]. It further cites Article 3 of the same Charter, which establishes the principle of inviolability of the human body[28]. Although a legal document, the legal provisions address what can be seen as ethical issues and are therefore explored here.

The opinion then sets out a series of what are termed "Fundamental ethical principles"[29] which include:

- Human dignity.
- Non-instrumentalisation.
- Privacy.
- Non-discrimination.
- Informed consent.
- Equity.
- The Precautionary Principle.
- Value conflicts.

Although some of these may be of limited relevance to RFID chip implants, they should still be considered (even if to dismiss them). Clearly, as noted above, there are considerable potential overlaps with legal and other aspects, for example in respect of legal safeguards in place for personal data protection and privacy; or the precautionary principle when it comes to the lack of knowledge regarding the health effects of potential long-term implantation.

How these might be addressed, other than by not permitting the technology, should also be considered (see Chapter 8).

---

[27] Cited in: European Group on Ethics in Science and New Technologies, (2005) p15

[28] Ibid, p16

[29] Source: European Group on Ethics in Science and New Technologies, (2005) pps22-23

5.2. Safety

One of the primary areas of ethical concern must be safety. Ensuring the health and safety of an employee is a major responsibility for all employers, and failure to address this issue adequately as the technology is deployed would be a significant failure on their part. As is apparent from Chapter 6 below, little is known about the safety and risks to health of these devices. Foster and Jaeger (2008) suggest that the knowledge of suggested carcinogenic effects in implanted rodents was not necessarily initially made known to human wearers, an issue that has clear ethical implications (whether concerns about similar effects in humans are justified or not).

Asking (or in the future possibly requiring) individuals to have such a device inserted, when we cannot be sure that they are safe, has clear ethical implications. Recent years have seen the emergence of the 'precautionary principle' by which, if something is not known to be safe (as opposed to there being no evidence that it is unsafe) then this is regarded as a strong argument against its introduction.

As well as any consideration of the health issue of chips when in place under the skin, there appears to have been little formal evaluation of their removal, for example on termination of employment. Although it appears that the chip can relatively easily be disabled or 'wiped' this still leaves the physical device *in situ* and needing to be surgically removed. Available anecdotal accounts relating to this (derived from a mixture of accounts posted on the internet and personal accounts from interviewees) range from the casual dismissal of it as an issue; to the view that it requires considerable surgical intervention as a consequence of it becoming embedded in connective tissue. Thus, in addition to any assurances given to potential wearers regarding the safe insertion and wearing of devices, it must also be made clear whose responsibility it will be to ensure safe removal, inactivation and disposal of the chip at the end of the employment period (or even if the individual changes their mind about having one implanted).

As a further consideration, as well as any potential impact on physical health, consideration must be given to possible mental health issues – again with ethical implications. If a person receiving an implant feels that they are required to modify their behaviour as a consequence of doing so, this may have a significant effect on their mental health- especially if they already feel vulnerable or insecure, or have a pathological tendency towards mistrust or suspicion. Assurances must be given that any detrimental effects on the mental and emotional health of employees who are chipped will be monitored and mitigated.

5.3. Efficacy

Although in some situations they are promoted based on 'convenience' in work situations the concept of a chip implant is often 'sold' to potential wearers on the basis of enhanced security. Given that there appear to be doubts about this (see Chapter 7) the ethics of using this argument must be questioned (see for example, Perakslis and Michael, 2012). In this context, Glasser et al (2007) raise an interesting issue in questioning a society in which moral considerations are given a lower priority than business or security. Even if security concerns were effectively addressed this dilemma would remain.

5.4. Privacy / Dignity

According to Monahan and Fisher (2010), "loss of privacy is the main concern that ethicists and others have about RFID implants", echoing the views of others such as Glasser et al (2007). Depending on how (and where) they are used, the chip presents the possibility of being able to monitor the wearer in some way (for example, logging the time a wearer spent in different areas accessed using chip readers) which could be seen as an invasion of privacy. As noted earlier, the technology exists to extend the 'read' range of readers, enabling monitoring over a greater area. Chapter 4.7 raised legal questions regarding the ownership

of data. Here we see a moral dimension as well, regarding different ways in which information made available through using an implanted chip might be used (or perhaps mis-used).

Furthermore, the chips can be reprogrammed within the body, altering their use and purpose from that initially agreed and consented to. Clearly, if changes are made by the employer, it is essential that the worker is fully informed of any changes before they are effected, and an opportunity to raise concerns be given. However, as referred to in the context of security (Chapter 7), the chips are not necessarily secure and the possibility that they might be 'hacked' by a third party with malicious intent cannot be discounted.

Additionally, in a further possible overlap with the legal issues, the insertion of a chip can be regarded as breaching the integrity of the human body or violating human dignity.

5.5. Religious Beliefs

Some religious views may preclude the insertion of an implant (there is some evidence of some very strongly held views in this regard including the suggestion that they are the 'Mark of the Beast' [e.g.30,31]) and the requirement to do so (or perceived pressure to do so) may be seen as a form of religious discrimination (see also Chapter 4.6). For some religions, any intrusion into the human body, even on the strongest of medical grounds, is unacceptable and it is difficult to see how the insertion of an ID chip as a requirement for employment could be tolerated under such circumstances.

5.6. Equity

In most employment situations, employer and worker do not enjoy equivalent status. The employer usually has some capacity to influence the decision made by the worker, as there is usually an exchange of assets (salary or other benefits) in return for the worker providing their labour or skills. This has significant implications for the equity of any arrangement.

However, a worker might find that, not only is access to certain areas of physical space denied to them on the basis of their failure to accept the use of a chip, but that progression or promotion within the company may also be restricted if they do not demonstrate loyalty in this way. As noted earlier, similar concerns regarding detrimental effects on non-wearers were identified by Monahan and Fisher (2010) in respect of the use of such implants in a patient care situation.

While in many situations this may not be a significant concern, it is possible that undue coercion and control may be facilitated through this. This may be especially true where the inequality between employer and worker is pronounced; for example in those who feel unable to voice objection for fear of losing their only source of income or security. There is a need to protect the most vulnerable in our society from exploitation and it is feasible that pressure to retain employment might result in workers accepting situations that, given a free choice, they would otherwise choose not to do.

5.7. Informed Consent

Although the need for informed consent appears to be an obvious expectation (see Section 4.7 relating to data protection and the GDPR), Glasser et al (2007) raise some interesting questions regarding how freely such consent might be given; and safeguards that might be required to protect vulnerable individuals. For example, if agreeing to having a chip implanted was a condition of employment with a certain organisation then the need of an individual for such employment might override any concerns they might have about accepting such a condition of service. It might therefore be considered necessary to introduce safeguards to

[30] http://www.catholic.org/news/technology/story.php?id=74365

[31] https://rcg.org/realtruth/articles/101105-001-prophecy.html

avoid against such an eventuality. However, the authors also raise a contrary view, namely that protecting people from their own decisions freely given might be seen as patronising and unacceptable. Clearly, issues such as the availability of alternative employment for the individual concerned will contribute to this aspect of any debate.

6. HEALTH AND SAFETY HAZARDS/RISKS

KEY FINDINGS

- Concerns have been expressed over the health and safety of RFID chip implants in four main areas: carcinogenicity; migration; interactions with MRI systems; impact on pharmaceutical effectiveness. There have been no systematic studies of health impacts in human wearers.
- There are reports of carcinogenic effects of RFID chips in some animals (mainly specific strains of mice). However, it appears that this is likely to be a feature of the unique sensitivity of these species and not a trans-species phenomenon. Potential mechanisms (such as 'foreign body carcinogenicity' which has been documented) suggest any similar effects in humans to be unlikely (although impossible to discount completely).
- Detailed studies of the potential interactions between MRI scanning and RFID chip implants appear to have excluded any significant effects, other than the risk of local details being masked by the chip image.
- Although anecdotally RFID chips can 'move' under the skin this appears to be a local reorientation. It is suggested that inter-species differences in sub-dermal layers makes significant migration unlikely although, in the absence of anything more than anecdotal evidence, this cannot be categorically excluded.
- Concerns regarding the impact of RFID technology on the efficacy of pharmaceuticals appear to stem from proposed use of RFID tags to label containers of pharmaceuticals. The scanning of bulk material presents a very different situation to that of pharmaceuticals circulating in the blood, where any risk of an effect would be extremely limited.

6.1. Introduction

In exploring the scientific literature in respect of RFID chip implants, the overriding impression is one of a lack of good quality information on health/safety effects. Information on actual effects on humans, rather than possible effects, is virtually non-existent; and information on their use in other animals raises issues regarding cross-species applicability. For example, what reliable information on the risk in humans can be derived from a laboratory study of mice (possibly specifically bred for susceptibility to adverse health effects)? Other papers regarding adverse effects in animals (often companion animals such as dogs and cats) are frequently case reports involving just one or two animals.

Concerns have been expressed that, as well as any health issues that might arise from the implantation process itself (which clearly must be carried out in accordance with appropriate hygiene and infection controls), having an implanted chip might have adverse health impacts including:

- Carcinogenic effects (e.g. Albrecht 2010, Blanchard et al, 1999).
- Adversely affect (or be adversely affected by) the use of devices such as MRI scanners (e.g. Baker & MacDonald, 2010, Steffen et al, 2010).
- Migration under the skin (e.g. Albrecht 2010) with potentially adverse consequences;
- Impact on the efficacy of pharmaceuticals (e.g. Sade, 2007).

Each of these concerns (and any others that emerge) will be explored in turn.

A further issue to consider (and which will again be explored) relates to the implications surrounding the subsequent removal of an implanted RFID chip (for example on ceasing employment).

One caveat to be placed on the information below is that it is believed to be approximately 20 years since the first documented implantation of RFID chips in humans (although there are some anecdotal reports of earlier uses). Since that time, the technology and materials used in such chips have changed. It is possible that some of the effects experienced were specific to the type of chip being used, rather than being applicable to any chip implants. Unfortunately, relevant details of chip construction that could be used to establish this are not always available.

6.2. Possible Carcinogenic Effects

Albrecht (2010) reported on a review of the literature relating to 'the safety of implantable microchips', identifying eleven papers spanning the period between 1990 and 2006. On the basis of this review the author concluded that there was 'a clear causal link between microchip implants and cancer in mice and rats' (p348); and that it 'appeared' that they could cause cancer in dogs. Given the potential impact of such an effect it is worthwhile exploring this in a little more detail.

The first report identified by Albrecht was a brief conference abstract (Johnson, 1996 as cited by Albrecht, 2010) and so had little detail other than that they had found tumours in <1 % of mice and that these were described as 'foreign-body sarcomas'. The author cited an earlier review on this topic (Brand et al, 1976 as cited by Albrecht, 2010) that reviewed the topic of 'foreign body tumorigenesis' concluding that it was independent of the material of the foreign body.

The next paper, Tillman et al (1997) described the incidental observation of cancerous growths in 36 of 4 279 mice (0.8 %). In their discussion, the authors cite six earlier papers, covering a variety of different animal species (in relatively small numbers), none of which identified cancerous growths. In response to the failure of another study (Rao & Edmonson, 1990) to identify cancerous growths they suggest that variations in genetic susceptibility might account for this, although the smaller number of mice in the earlier paper (~140) might also have played a part.

The next paper was another conference abstract. In this case the authors (Palmer et al 1998) examined 800 mice and found tumours in 16 (2 %) of these. The authors comment that the mice in question were a specific strain and that earlier studies they had conducted in other strains had not found any such growths, adding weight to the views of Tillman and colleagues of a strain-specific susceptibility.

This theme is also echoed by the next paper (Blanchard et al, 1999). In their work, 18 out of 177 mice developed cancerous growths at the implant site (~10 %). The purpose of the paper and the research it reported was to explore the use of this transgenic strain. The strain had been bred specifically to have a deficiency in a tumour-suppressing gene; and the study was planned to demonstrate their resultant susceptibility to cancer. The authors refer in their introduction to their prior experience (nearly ten years) of using the implants without adverse effects.

Elcock et al (2001) reported on studies using rats rather than mice. Two separate but related studies found an 0.96 % and 0.58 % incidence of tumours in a total of over 1 000 rats, again of a specific strain. Again, in their discussion, the authors refer to earlier work in a variety of animal species that had failed to find any such effect.

The final study examined tumours collected from mice in a number of different experiments. In all, 52 tumours were collected from experiments involving a total of 1 260 mice (~4 %), again of a specific strain bred for carcinogenicity testing (Le Calvez et al, 2006).

Although these studies serve to indicate a potential for carcinogenesis associated with the use of RFID implants, there are clearly questions regarding the potentially intentionally susceptible strains of animals (mainly mice) used in many of the studies that have found effects; and the inter-species relevance of the findings. It is of particular interest that all of

the authors refer to previous experience with no tumours. It is not known whether the RFID chips used were coated (which would encourage tissue growth round the device) or uncoated.

One mechanism referred to in a number of these papers is that of carcinoma associated with foreign bodies. In their paper reporting three cases, Jennings et al (1988) describe foreign body tumorigenesis as 'not proven definitively in man', although they then demonstrate, through their reported cases in humans, that it is possible. In an earlier paper, Brand & Brand (1980) draw parallels to the (low) incidence of cancers associated with 'implanted' foreign bodies (including material 'accidentally acquired' – for example as a war injury). However, in contrast, a more recent paper on investigations of such acquired foreign bodies (Gaitens et al, 2016) found no signs of neoplasms in tissue surrounding the foreign body.

In a recent review on the carcinogenicity of implantable materials, Williams (2014) presented a broad assessment targeted at implantable devices in general, not specifically RFID chips. Commenting on the general use of animals to assess biocompatibility, the author states that "such tests are rarely predictive of performance in humans" (p579). Specifically on carcinogenicity the author expresses an even stronger view, stating that:

> "…species specificity considerations mean that extrapolation from observations of tumors around biomaterials in rats and mice to clinical use in humans is scientifically invalid." (p579)

Although addressing implants from a much wider perspective, this latter comment would appear to be relevant to any debate on the carcinogenicity of RFID implants suggesting that even the tests for human biocompatibility might be flawed.

As is often stated, it is difficult to prove an absence of effects. However, despite evidence and concerns based on experiences with other species, it would seem that any risk of carcinogenesis in humans receiving RFID chip implants is at most minimal.

6.3. Other Possible Dermal Effects

There is a considerable body of evidence from the medical literature regarding adverse effects of subdermal implants for cosmetic (e.g. Alijotas-Reig et al, 2013) and other purposes. This is clearly a complex field given the wide variety of materials used and it is far from clear to what extent (if any) they might relate to RFID implants. For example, Frank et al (1993) reported on a study of the use of contraceptive implants inserted into the upper arm of patients. The vast majority of reported side-effects related to the contraceptives released by the implants. However, in a small minority of cases (2.7 %) there were reports of problems with the carrier rods themselves, including the rod migrating, being spontaneously expelled, or developing a localised infection. These could be relevant to RFID implants.

The documented existence of such effects counsels caution in respect of RFID implants. Although the risk of carcinogenic effects may be minimal, there might be risks of other adverse dermal reactions which, although apparently rare (Kunjur & Witherow, 2013), should be explored.

6.4. Possible Effects on MRI Use

One concern expressed in some quarters relates to adverse reactions in MRI scanning. It is understood that the magnetic metallic content of RFID chips is very low and can be reduced further in chips specifically intended for implantation.

In a brief review of possible risks associated with RFID implants, Rotter et al (2012) cite the FDA as raising the possibility of an incompatibility between RFID implants and the use of MRI scanners.

In a small on-line publication, Lamberg (2004) reported on studies in which 'several' devices were tested. Although the circumstances of testing are unclear these do not appear to have been tested *in-situ*. The author refers to 'device movement' stating that the forces measured were low, with little chance of migration occurring as a result. There was no noticeable

heating; and image distortion occurred only in the immediate vicinity of the chip. However, after MRI scanning one device failed to function. Given the very limited data presented and no corroboration of statements such as references to the force needed to tear a device from tissue, little reliance can be placed on this paper.

Steffen et al (2010) reported on experimental studies in which they explored the effects of MRI exposure on RFID Chips (referred to as tags). By way of background they cite what appears to be the paper by Lamberg as showing 'no adverse effects for patients" (p2/9). Although the main focus of the study was external tags the study does provide useful insight into the impact of MRI (and CT) scanning on the device itself. Passive transponder tags were used. Both 1.5 T and 3 T MRI scanners were used.

With a large tag (76x45 mm, which is much larger than those currently implanted), some heating (max 3.6°C) was measured beneath the tag after 15 minutes of scanning using 1.5 T MRI. Such temperatures exceed those defined in current guidelines or standards regarding implants.[32,33] International standard ISO 14708-1:2014 E requires that no outer surface of an active implantable part of any medical device be greater than 2ºC above the normal surrounding body temperature of 37ºC during implantation, normal operation, or single-fault conditions. However, with the smaller tag (31x14 mm), which was still large by implantable tag standards (1.5°C max), or with the more powerful 3 T MRI system (<0.8°C), lower temperatures were obtained. Although possibly generating some awareness of heating, effects of this magnitude would be unlikely to result in tissue harm if repeated with an implanted chip.

Measurements of induced accelerative force were recorded as <1 N kg^{-1}, described by the authors as "generally not or minimally perceptible" (p 7/9). However, it is not known how these effects would relate to smaller implanted tags.

The authors did report that the tag device did block the image underneath them, and distort the image for a short distance around the tag. As might be expected the effect was markedly less for the smaller tag. For an even smaller implanted tag, located in a peripheral area of the body, this is unlikely therefore to be of any clinical significance.

Finally, the authors reported that neither MRI nor CT scan use had any negative effect on the integrity of the tags themselves which remained both readable and re-programmable after exposure.

As noted, this study was carried out on larger RFID chips than would be implanted. Baker & MacDonald (2011) attempted to simulate *in vivo* conditions using a gel-filled 'phantom'. As with the work of Steffen and colleagues the authors found limited heating effects (~0.4°C); forces around 2 000 times lower than the force found to be required to displace a device in a sheep; no damage to the function of the RFID chips; and MRI scan artefacts in the vicinity of the implant.

Although restricted by the lack of specific *in vivo* studies (where objective measurement of factors such as force and temperature would be problematic) the available evidence appears to suggest that any negative impact of an RFID on subsequent MRI scanning of the individual would be minimal.

6.5. Migration

Chapter 6.3 briefly addressed the issue of migration in respect of the forces that would be exerted on an implanted RFID chip during MRI scanning. Some sources have also raised

[32] ICNIRP (1998) Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz). International Commission on Non-Ionizing Radiation Protection. Health Phys, 74, 494-522.

[33] ANSI/IEEE (2005) IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz. IEEE Std C95.1-2005 (Revision of IEEE Std C95.1-1991).

wider concerns regarding the passive (mechanical) migration of such devices within the body (e.g. Sade 2007). It is interesting to note here that the concern referred to by Sade is that such migration might make the RFID potentially difficult to extract rather than any concern regarding the adverse impact of the migrated device.

In animal species, the risk of such migration appears to be recognised. Le Calvez et al (op cit) describes the use of chips fitted with a polypropylene sheath as an anti-migration measure; a feature also referred to by Albrecht (op cit). However, perhaps because of the use of such measures, there appears to be no published documentation regarding the extent to which migration occurs in animals, much less in humans. Anecdotally it has been suggested that the characteristics of human skin differ from those in other species and that, as a result, migration is much less likely to occur. However, again anecdotally, some recipients of RFID chips do refer to them re-orienting themselves, for example to be better aligned with the movement of structures in the hand and isolated reports from the literature of contraceptive rods migrating, referred to earlier, might also be relevant.

A number of papers refer to implanted chips becoming encapsulated by connective tissue and, once this occurs, the risk of migration appears to be reduced. Reflecting this, Baker & MacDonald (op cit) recommend waiting three months before subjecting an implanted animal (dog) to an MRI scan to allow sufficient time for this encapsulation to occur.

To date there is no formally collated information or systematic study available to document the extent to which sub-dermal chip migration is possible in humans, or the extent of any migration should it occur, although it seems to be a minimal risk. It is however recognised that migration of foreign bodies can occur within the body. For example, Lyons and Rockwood (1990) report on a review of reports of the migration of surgical pins used in shoulder surgery. In contrast, Hoffman et al (1999) report on studies of materials for use in cosmetic lip implantation where the implanted material becomes encapsulated by cell growth and therefore does not migrate. It would seem likely that the location of the implant within dermal or sub-dermal layers, rather than within deeper body tissues, as well as the material involved, are important factors here.

6.6. Effect on Pharmaceuticals

In suggesting possible concerns regarding the physical risks to patients posed by RFID chips, Sade (op cit) states that “It has not been determined whether RFID tags might affect the efficacy of pharmaceuticals.” In support of this the author cites two sources. The first of these (Ingeholm et al, 2006 as cited in Sade, 2007) could not be sourced but, from references elsewhere, it does not appear to focus specifically on implanted chips. The second (Wasserman 2006 as cited in Sade, 2007)) definitely does not, referring to the use of RFID chips in the supply chain to ensure the *bone fide* nature of drugs. In this context, the concern would appear to be that of direct exposure of the bulk drug to the radio frequencies of the reader, rather than the circulating drug within the human patient.

Uysal et al (2010) reported on a systematic evaluation of this issue on pharmaceuticals with a protein base, in view of the well-documented sensitivity of protein-based materials to heating (denaturing). Using the five main frequencies of radio waves used in RFID, the authors subjected ‘multiple products’ (covering hormones, vaccines and immunoglobulins) to a level of radiation twice that permitted by the Federal Communications Commission (the US regulatory body for radio communications). Assays for purity and potency after 24 hours continuous irradiation found no detectable deterioration in any product.

Given this evidence, combined with the radically different sphere of application (and the fact that most of the circulatory system would be unexposed), there would seem to be little justification for any such concerns being translated to the current application.

7. SECURITY ISSUES

KEY FINDINGS

- It would seem that, at present, the RFID chip technology (which is essentially similar to that used in credit cards and similar systems) is not entirely secure.
- Security concerns include eavesdropping; cloning; disabling; and unauthorised tag modification.
- Although efforts are continuing to counter these concerns there remain doubts and uncertainties.

7.1. The issues

Citing a number of sources themselves, Darcy et al (2011) list what the authors refer to as the "most dominant [issues] with regard to RFID security" (p10):

- Eavesdropping: The act of setting up an additional reader to record tag data.
- Unauthorised Tag Cloning: Copying tag data onto an additional tag to gain the same privileges.
- Man-in-the-Middle (MIM) Attack: When an external object pretends to be either a tag or reader between actual tags and readers.
- Unauthorised Tag Disabling: When an external reader disables a tag not allowing it to be utilised again.
- Unauthorised Tag Manipulation: Manipulating the tag data using an external reader.[34]

In a more recent paper Singh et al (2017) suggest some further concerns including:

- Further Eavesdropping: An intruder reader intercepts the signals between the chip and the legitimate reader.
- Traffic Analysis: The existence and location of a chip is monitored, without necessarily interrogating the chip.
- Spoofing: Also known as satirising, where another device is used to simulate a genuine chip.
- Denial of service attack: Chips can be adulterated to disable them.

Roberts (2006) reports on the free availability of software that can read and reprogramme RFID tags, suggesting that the security issues are widespread. Although other papers (e.g. Dimitriou 2005) suggest that possible solutions for the most basic security concern of cloning might become available, current indications are that there continue to be problems. For example, while Baghery et al (2014) wrote of improvements to RFID authentication protocols to enhance security, these suggestions were soon countered by the presentation of flaws (Safkhani & Bagheri, 2016). Although there is an extensive body of literature, especially on software architecture and programming, these offer little additional insight into the broad issues of RFID chip security and will not be documented in detail here.

Other than acknowledging their existence, such security issues do not appear to have been discussed in any detail specifically in respect of RFID chip implants, although papers such as that by Halamka et al (2006) suggest that some chips might be vulnerable to cloning. Despite this, there are perceptions that RFID chips offer a more secure means of ensuring workplace security, especially amongst younger adults ('Millennials') (Perakslis & Michael, 2012).

This lack of focus possibly reflects the fact that human implanted chips remain very much a niche (some might say hobby or novelty) market. The vast majority of chip implants are made in animals and there would seem to be little value in cloning the chip code of a pet dog

[34] Source: Darcy et al (2011) pps 10-11

(for example). However, if the applications of human RFID chips were to grow, and were to become associated with high level security applications then interest in their security (and in attacking that security) would be likely to increase.

7.2. Solutions

As noted above, there has been virtually no focus on chip security as far as applications involving human implants are concerned. An approach understood to be commonly adopted by RFID chip manufacturers with non-implanted chips is that of 'kill tag' technology where the RFID chip is automatically disabled by illegal attempts to interrogate it (Roberts, 2006). Although this might be an effective approach for non-implanted chips this raises the prospect of defunct chips within the body needing to be removed (and a potential need for a replacement to be inserted).

Another approach is where identifiers are exchanged between the reader and the chip and routinely updated, in a process called 'mutual authentication' (Dimitriou, 2005). Risalat et al (2017) have recently written of a new authentication protocol, based on a regularly updated 'secret key value' (that seeks to ensure that only authorised readers can access chip information). The authors claim that this is "secure and immune to different kinds of attacks". It remains to be seen whether this represents a breakthrough – or a challenge to others to break it, as appears to have been the case in the past.

In broad terms, discussions for the purpose of this paper with individuals working in the industry suggest that, although efforts are being made to resolve such problems, they remain valid concerns at present. Although opinions vary as to the extent to which potential solutions might be forthcoming in a not too distant time-frame, it would seem that the technology itself is susceptible to security intrusion. For example, one long-term 'user' of the technology indicated that he adopts a second line of security such as a PIN where he feels that this is warranted. Interestingly he also indicated a reluctance to use biometric data stored on the chip for this purpose because of this perceived vulnerability and the consequent risk of personal identity theft (see also Kosta *et al,* 2007). Despite the ability to encrypt such information he felt that it remained vulnerable.

Others suggest that it is not a significant issue at present – although this could be because the nature and extent of current applications do not warrant the effort involved. Halamka et al (2006) suggest that RFID chips remain free from 'attack' because there is relatively little to be gained from doing so (although, as some reports of computer system hacking suggest, some people do so 'because they can'). Clearly however that could change if the technology became used more widely, or if it was known to be used in selected security applications where there was more value in gaining access.

As a guide, the technology used is basically similar to that utilised in bank credit and debit cards using 'chip and pin technology' and the fact that such cards usually rely on a second form of ID (such as the PIN) is indicative of the security involved (See for example, Fan *et al* 2005). Other applications of RFID chips include e-passports which, as Kosta *et al* (2007) discuss, have security issues which could also be applied to RFID implants.

These issues are important, as the existence of such security concerns is likely to impact on consideration of the ethical and legal issues surrounding the use of RFID chip implants, given that enhanced security has sometimes been presented as a positive benefit from the use of implanted chips (and sometimes provides the main rationale for their use).

8. CONCLUSIONS: INTEGRATED OVERVIEW OF THE ISSUES RAISED BY CHIP IMPLANTS FOR WORKERS

KEY FINDINGS

- In existence for around 20 years, human implantable RFID chips come in passive and active forms. The passive form is considered here.
- Advocates of the use of RFID chip implants suggest that they confer benefits in terms of ease and convenience compared to the alternative technologies (e.g. smart cards) that they replace.
- Despite well-documented concerns about the possible adverse health effects of such implants (most notably reports of carcinogenetic activity) there is no evidence of such effects in humans (as opposed to experimental animal strains). However, although there is reasonable incidental evidence suggesting such effects as being unlikely, there is also no specific evidence of no effect.
- Literature on surgical and cosmetic implants suggests that, although adverse reactions are rare (and do not appear to include carcinogenetic effects) both migration of implanted materials and adverse health reactions can occur and should be explored further.
- One integrated theme would seem to be that of human rights; covering the inviolability of the human body and an individual's right to privacy. These issues would seem to reflect both ethical concerns and the legal provisions safeguarding those rights.
- It would seem that legal efforts to overturn those rights for compulsory implant use in the workplace would need to reflect over-riding demands, perhaps on the grounds of national security. Here however, the evidence that the RFID technology is insecure, and the lack of specific assurances regarding adverse health effects can be seen as undermining the case for such a development.
- However, even where such technological challenges are to be overcome, it must be recognised that the use of such implants evokes strong objections (including religious concerns) and any compulsion would need to provide for appropriate exemptions in such circumstances.
- Where implant use is voluntary (as is the case at present) then legal considerations in respect of data protection still apply with regard to any information regarding access, patterns of use, etc. which might be collected as part of such use.
- There are also cross-cutting issues regarding legal and ethical considerations, where supposedly voluntary use included any degree of perceived coercion or where those with such implants might be considered to receive different treatment.

8.1. Overall implications

From the preceding chapters it will be apparent that there are legal, ethical, health and security issues surrounding the potential use of RFID implants. It will also be apparent that these issues often overlap and are interrelated. However, these have to be seen against the convenience that such devices are regarded as providing compared to, for example, having to retain and use a smart card.

8.2. Health issues

Probably foremost amongst the issues are those relating to health. Legal and ethical considerations are often predicated on the assumption that there are either no risks to human health, or those risks are relatively minor and at a level where they can be regarded as acceptable, subject to informed consent. However, the challenge here is that the case in respect of potential health risks can be regarded at best, in the terms of the (uniquely) Scottish verdict of 'not proven'. There are clearly concerns about health risks, some of which, such as those relating to interference with or adverse effects from MRI use and interactions with pharmaceuticals, can it seems be discounted.

Probably the main health concern which can less readily be discounted is that of potential carcinogenic effects. Conflicting opinions and evidence, summarised earlier, suggest that, on balance, there is no significant risk of carcinogenetic activity of RFID chip implants in humans. However, all such evidence can be regarded as inferential and it would be difficult to provide categorical assurances of safety. The principle of informed consent requires a good and clear understanding of the risks to which the individual is consenting. At present it would be difficult to formulate a clear and unequivocal statement of those risks, sufficient to justifiably permit compulsion without an overriding need. Even where implantation was voluntary this should only be undertaken with a clear explanation (and acceptance by the recipient) of the potential risks.

Although no case reports have been seen regarding other adverse health effects of implanted RFID chips there is evidence from the field of cosmetic surgery in particular to suggest that, in a small minority of cases, adverse health reactions or migration of materials from the implant site can occur. Although the materials used obviously differ (which is likely to significantly impact on the degree of risk) the demonstrated occurrence of such effects does at least suggest a need for caution, especially before any provisions for compulsory implantation are contemplated.

Application of the precautionary principle would seem to suggest that, if we do not know RFID chip implants to be safe (as opposed to knowing that they are unsafe, or perhaps how unsafe they are), then can we ethically implant them, even on the basis of 'informed consent'? Legal arguments would suggest that, in order to legitimately obtain informed consent, we would need confidence in the information we were providing as the basis for that consent. However, where implantation is truly voluntary (without any suggestion of coercion) then informed consent on the basis of current knowledge (and uncertainty) is likely to be considered acceptable.

8.3. Security concerns

The issue of overriding need presents a connection to the next cross-cutting issue, that of security. Considerations of legal and ethical issues suggest that compulsory use of implants would need to have a very strong justification, such as a matter of national security, to warrant the personal intrusion involved. The test of no alternative viable solution would also be important here. Many of the press and informal reports surrounding the use of RFID chips focus on the convenience of the technology, of not having to carry a card for example, rather than enhanced security. This appears to stem from a recognition amongst those promoting the use of the technology that they are inherently insecure (in the same way as bank card PIN technology is vulnerable). Until such concerns are successfully addressed it would therefore appear to be difficult to justify a requirement for a chip implant on the grounds of security, as such an implant would perhaps be no more secure than the card it replaces.

Clearly, they do offer 'security' in the sense that the chip is harder to lose than a separate card or other device might be – although a chip embedded into a close-fitting ring would offer a degree of such security unless deliberately removed.

Apart from the adverse implications on security grounds for their application, the fact that the implanted chip can be detected by others raises uncertainties over what personal security vulnerabilities might be created in those who have them implanted. This was apparent in the comments of one long-term user (and advocate for the technology) regarding the vulnerability of personal identifiers held on the chip.

8.4. Ethical barriers

Ethically, those receiving such an implant voluntarily should also be made aware of the potential security limitations and risks. Chapter 5 identified a number of potential ethical barriers to compulsory use of RFID chip implants. Whatever the security applications (and assuming that the health and RFID security concerns can be adequately addressed) it must be acknowledged that there will be some individuals who will be opposed to their use on religious or other grounds.

Some such views appear to be quite vehemently held (e.g. viewing the RFID chip as 'the mark of the beast'[35,36]). There is no way of knowing how many people hold such views, but they must be recognised and accommodated as appropriate.

8.5. Legal issues

There is no specific, tailored and/or comprehensive legislation, case law or regulatory regime banning, restricting or controlling the use of microchip implants by employers in the EU or in any of the member states of the EU ("Member States"). As such, whether employers have the power to coerce their workers to accept such implants is a matter that is governed by the general principles and rules of EU labour law and human rights law, as well as the National laws of each of the Member States. Some of these provisions apply to both compulsory and voluntary applications of the technology. Thus:

- The GDPR demands a very high standard of consent to microchipping from workers, which must be given by clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the worker's agreement to their personal data being processed.
- There is no definitive answer to the question whether microchipping is unlawful as a breach of a worker's human rights, since the appropriate response will depend on the nature and extent of the harm done to the worker, which is weighed against the employer's need to engage in microchipping to fulfil a legitimate commercial objective.
- If the implantation of a microchip gives rise to health and safety issues, there is a strong argument that such a managerial instruction would be unreasonable and unlawful.
- A managerial instruction to a worker to implant a microchip without consent can give rise to a constructive dismissal based on health and safety concerns.
- In terms of EU indirect religious discrimination law, if the microchipping is not 'appropriate', 'necessary', or 'proportionate' to achieve a real need, objective or aim that the employer has identified, its objective justification defence will not be satisfied.
- It will only be in exceptional circumstances that (i) the ownership of the microchip would be vested in the worker, or (ii) the employer would have the legal authority to insist that it and other third parties retain any data collected and stored on the microchip at all times, including once the worker has moved on to another employer.

[35] https://rapturewatcher.wordpress.com/vital-facts-about-the-mark-of-the-beast-rfid-chip-human-barcode-666/

[36] Revelation 13:16-17 & 14:9-10

8.6. Overall outcome

The possible use of RFID chips in the workplace raises a complex interaction between health, security, ethical and legal issues. In relation to their possible compulsory use, there is no specific legal instrument relating to such compulsory implantation of RFID chips into workers. However, it appears that such implants would encounter significant legal challenges in respect of current EU law, in particular relating to data protection and human rights (including the sanctity of the human body). Clearly, although laws can be changed or amended, the current uncertainties over the health implications of such implants and the wider security issues of RFID chips tend to run counter to any such use that could be sanctioned at present. Although it is theoretically possible to sanction their use on the grounds of overriding security, current concerns regarding the security of the chips themselves would tend to obviate any such arguments. In addition, although there is evidence to suggest that they are over-estimated, present uncertainties over possible health effects makes it impossible to give assurances regarding adverse health impacts. It seems likely that the same aspects would undoubtedly leave such applications vulnerable to legal and ethical challenge in the future, without a fundamental rethink of personal human rights and the sanctity of the human body.

In respect of voluntary use in the workplace, it should be established that such use is entirely voluntary and that no coercion exists (for example in the form of preferential treatment of wearers – other than perhaps the convenience imparted to the wearer through using the chip). In such cases, potential wearers should be fully informed of the possible health risks (and the doubts and uncertainties regarding those risks) and of the security liabilities relating to RFID chip technologies.

Finally, there is no specific regulatory provision currently in place regarding the process of implantation; in the form of minimum hygiene standards or other requirements. Although the current voluntary use is outside the scope of this paper it is noted that at least some of the advocates for the use of the technology believe such controls to be necessary and, if compulsory workplace use were to be sanctioned, such considerations would be a definite requirement.

8.7. Future considerations

As noted above it appears likely that any attempt to formally permit or sanction the compulsory use of RFID chip implants in workers would be subject to considerable opposition, especially in respect of human rights and the sanctity of the human body. As part of this it would seem likely that there would be challenges on religious grounds leading to claims of religious discrimination.

With the present state of knowledge it would seem that there would be strong grounds for legal challenges on the basis of potential or perceived adverse health effects; and on the grounds that such implants would not offer the looked for additional security (over non-implanted solutions) which could otherwise form part of any justification for their use.

On this basis, unless there are significant pressures and priorities relating to advancing this technological application, it would seem defensible to adopt a watching brief and re-assess knowledge after an appropriate time.

However, although this would seem to be a viable solution in relation to technological developments in enhanced security (where there does seem to be a significant and ongoing research community), the same does not appear to apply in respect of possible health effects. Current applications appear to be relatively piecemeal and uncoordinated, with little focus on claimed health effects. It would seem likely that no significant advances in knowledge in respect of possible health impacts in humans are likely to emerge without some form of positive action being taken.

Two avenues of investigation would seem to be worth investigating in this regard.

Desk-top medical research

The first is to commission desk-top research from appropriate experts (in, for example, dermal medicine and oncology) to formally explore the scientific and medical literature relating to sub-dermal implantation to provide an authoritative evidence-based theoretical review on the health risks potentially associated with the implantation of RFID chips. This would encompass carcinogenicity and other dermal effects.

Longitudinal study of health effects

Secondly, although the logistics of such a study would be challenging, definitive answers on possible health effects would best be provided through a longitudinal (prospective) study of chip recipients. Given the expectation that, based on the reported animal studies, the incidence of such effects would be low, care must be taken to ensure that any such study is large enough to have sufficient statistical power to identify any such effects (or their absence) with any certainty. Given the recognised inter-species differences in cancer susceptibility there would seem to be little merit in pursuing studies in animal models, unless an appropriate surrogate species can be identified. Even here, if shorter-lived species such as rats or mice were employed it might be difficult to replicate the effects of implantation over the longer term.

Even if definitive evidence was available to demonstrate that such devices were both secure and safe, it would seem to be highly likely that significant challenges would remain on ethical, moral and religious grounds; and that stringent data management regulations and guidance would be required.

On this basis, unless there is seen to be an overwhelming need or demand for the compulsory implementation of implantable RFID chips in the workplace then adopting a waiting game would seem to be the preferred option.

However, even in voluntary systems, workers (and others) need some protection. With self-administered chip injection kits available on the internet, consideration should be given to a need to regulate their implantation (in the same way as others such as acupuncturists and tattooists come under appropriate controls). Whether such controls should be national or EU-based is beyond the scope of this paper, but with clear potential risks of infection, contamination, etc., both from the chip itself and the implantation procedure, some provision for such protection would seem to be justified.

REFERENCES

This list of references is divided into those cited in the text above and those reviewed but not formally cited.

- Albrecht, K. (2010, June). Microchip-induced tumors in laboratory rodents and dogs: A review of the literature 1990–2006. In Technology and Society (ISTAS), 2010 IEEE International Symposium on (pp. 337-349). IEEE.
- Alijotas-Reig, J., Fernández-Figueras, M.T., Puig L. (2013) Inflammatory, immune-mediated adverse reactions related to soft tissue dermal fillers. Seminars in Arthritis and Rheumatism, 43, 241-258.
- Baghery K., Abdolmaleki B., Akhbari B., Aref MR. (2014) Privacy analysis and improvements of two recent RFID authentication protocols. 2014 11th International ISC Conference on Information Security and Cryptology, 137-142.
- Baker, M. A., & MacDonald, I. (2011). Evaluation of magnetic resonance safety of veterinary radiofrequency identification devices at 1 T. Veterinary Radiology & Ultrasound, 52(2), 161-167.
- Blanchard, K. T., Barthel, C., French, J. E., Holden, H. E., Moretz, R., Pack, F. D., ... & Stoll, R. E. (1999). Transponder-induced sarcoma in the heterozygous p53+/-mouse. Toxicologic pathology, 27(5), 519-527.
- Brand, K. G., & Brand, I. (1980). Risk assessment of carcinogenesis at implantation sites. Plastic and reconstructive surgery, 66(4), 591-594.
- Darcy, P., Pupunwiwat, P., & Stantic, B. (2011). The challenges and issues facing the deployment of RFID technology. In Deploying RFID-Challenges, Solutions, and Open Issues. InTechOpen: Downloaded from: http://www.intechopen.com/books/deploying-rfid-challenges solutions-and-open-issues
- Dimitriou, T. (2005) A Lightweight RFID Protocol to protect against Traceability and Cloning attacks. First International Conference on Security and Privacy for Emerging Areas in Communications Networks. IEEE, 59-66.
- Donaldson, P.E.K. (1976) The encapsulation of microelectronic devices for long service life, IEEE Trans. Biomed. Eng., 23, 281-285.
- Elcock, L. E., Stuart, B. P., Wahle, B. S., Hoss, H. E., Crabb, K., Millard, D. M., ... & Lake, S. G. (2001). Tumors in long-term rat studies associated with microchip animal identification devices. Experimental and Toxicologic Pathology, 52(6), 483-491.
- Fan, C-I., Chan Y-C., Zhang Z-K,. (2005) Robust remote authentication scheme with smart cards. Computers & Security, 24, 619-628.
- Foster, K. R., & Jaeger, J. (2007). RFID inside. The murky ethics of implanted chips. IEEE Spectrum, 44, 24-29.
- Foster, K. R., & Jaeger, J. (2008). Ethical implications of implantable radiofrequency identification (RFID) tags in humans. The American Journal of Bioethics, 8(8), 44-48.
- Frank, M.L., Poindexter, A.N., Cornin, L.M., Cox, C.A., Bateman, L. (1993) One-year experience with subdermal contraceptive implants in the United States. Contraception, 48, 229-243.
- Gaitens, J. M., Centeno, J. A., Squibb, K. S., Condon, M., & McDiarmid, M. A. (2016). Mobilization of metal from retained embedded fragments in a blast-injured Iraq War veteran. Military medicine, 181(6), e625-e629.
- Glasser, D.J., Goodman, K.W., Einspruch, N.G. (2007) Chips, tags and scanners: Ethical challenges for radio frequency identification. Ethics and Information Technology, 9, 101-109.
- Hoffmann, C., Schuller-Petrovic, S., Soyer, H.P., Kerl, H. (1999) Adverse reactions after cosmetic lip augmentation with permanent biologically inert implant materials. Journal of the American Academy of Dermatology, 40, 100-102.

- ISO 10993 Biological evaluation of medical devices. (20 parts) Geneva: ISO
- ISO 14708-1 2014 Implants for surgery - Active implantable medical devices - Part 1: General requirements for safety, marking and for information to be provided by the manufacturer. Geneva: ISO
- Jennings, T. A., Peterson, L., Axiotis, C. A., Friedlaender, G. E., Cooke, R. A., & Rosai, J. (1988). Angiosarcoma associated with foreign body material. Cancer, 62(11), 2436-2444.
- Kosta, E., Meints, M., Hansen, M., Gasson M. (2007) An analysis of security and privacy issues relating to RFID enabled ePassports. SEC 2007: New Approaches for Security, Privacy and Trust in Complex Environments pp 467-472
- Kunjur, J., Witherow, H. (2013) Long-term complications associated with permanent dermal fillers. British Journal of Oral and Maxillofacial Surgery, 51, 858-862.
- Lamberg, J. (2010). Magnetic resonance imaging & VeriChip™ RFID human implant at 1.5 Tesla. University of Minnesota Twin Cities.
- Lyons, F.A, Rockwood, C.A. (1990) Migration of pins used in operations on the shoulder. Journal of Bone and Joint Surgery, 72, 1262-1267.
- Monahan, T, Fisher, J.A. (2010) Implanting inequality: Empirical evidence of social and ethical risks of implantable radio-frequency identification (RFID) devices. International Journal of Technology Assessment in Health Care, 26, 370-376.
- Palmer, T. E., Nold, J., Palazzolo, M., & Ryan, T. (1998). Fibrosarcomas associated with passive integrated transponder implants. Toxicol Pathol, 26, 170.
- Perakslis, C., & Michael, K. (2012, October). Indian Millennials: Are microchip implants a more secure technology for identification and access control?. In Technology and Society in Asia (T&SA), 2012 IEEE Conference on (pp. 1-9). IEEE.
- Rao, G. N., & Edmondson, J. (1990). Tissue reaction to an implantable identification device in mice. Toxicologic Pathology, 18(3), 412-416.
- Risalat N.A.M., Hasan M.T., Hossain M.S., Rahman M.M. (2017) Advanced real time RFID mutual authentication protocol using dynamically updated secret value through encryption and decryption process. 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), 788-793.
- Roberts, C.M. (2006) Radio frequency identification (RFID). Computers & Security, 25, 18-26.
- Sade, R. M., & American Medical Association. (2007). Radio frequency ID devices in humans. CEJA Report 5-A-07.
- Safkhani, M., Bagheri, N. (2016) A note on the security of two improved RFID protocols. International Journal of Information Security, 8, 155-160.
- Stockman, H. (1948) Communication by means of reflected power. Proc. IRE, 36, 1196-2014.
- Uysal I, DeHay P.W., Altunbas E, Emond J-P, Rasmussen R.S., Ulrich D. (2010) Non-thermal effects of radio frequency exposure on biologic pharmaceuticals for RFID applications. RFID, 2010 IEEE International. 266-273.
- Williams, D. F. (2014). Carcinogenicity of implantable materials: experimental and epidemiological evidence. International Urogynecology Journal, 25(5), 577-580.

- Bacheldor, B. (2007). AMA issues ethics code for RFID chip implants. RFID Journal.
- Carminato, A., Vascellari, M., Marchioro, W., Melchiotti, E., & Mutinelli, F. (2011). Microchip-associated fibrosarcoma in a cat. Veterinary dermatology, 22(6), 565-569.
- Dahlborn, K., Bugnon, P., Nevalainen, T., Raspa, M., Verbost, P., & Spangenberg, E. (2013). Report of the federation of european laboratory animal science associations working group on animal identification. Laboratory animals, 47(1), 2-11.
- European Group on Ethics in Science and New Technologies, Opinion on the ethical aspects of ICT implants in the human body (16 March 2005, Opinion N° 20) (Luxembourg: Office for Official Publications of the European Communities, 2005)
- Friggieri, A., Michael, K., & Michael, M. G. (2009, May). The legal ramifications of microchipping people in the United States of America-A state legislative comparison. In Technology and Society, 2009. ISTAS'09. IEEE International Symposium on (pp. 1-8). IEEE.
- Gasson, M. N., Kosta, E., & Bowman, D. M. (2012). Human ICT implants: From invasive to pervasive. In Human ICT Implants: Technical, Legal and Ethical Considerations (pp. 1-8). TMC Asser Press.
- Halamka, J., Juels, A., Stubblefield, A., & Westhues, J. (2006). The security implications of VeriChip cloning. Journal of the American Medical Informatics Association, 13(6), 601-607.
- Hassan, A. S., Hussein, R. T., & Abboud, I. K. (2015). Attendance System Based on Radio Frequency Identification Technology. Journal of Engineering and Development Vol, 19(06).
- Heffernan, K. J., Vetere, F., & Chang, S. (2016, May). You Put What, Where?: Hobbyist Use of Insertable Devices. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 1798-1809). ACM.
- Heffernan, K. J., Vetere, F., & Chang, S. (2017). Towards insertables: Devices inside the human body. First Monday, 22(3).
- Hildebrandt, M., & Anrig, B. (2012). Ethical implications of ICT implants. In Human ICT implants: technical, legal and ethical considerations (pp. 135-158). TMC Asser Press.
- Ishihata, H., Tomoe, T., Takei, K., Hirano, T., Yoshida, K., Shoji, S., ... & Horiuchi, H. (2007). A radio frequency identification implanted in a tooth can communicate with the outside world. IEEE Transactions on Information Technology in Biomedicine, 11(6), 683-685.
- Jechlitschek, C. (2006). A survey paper on Radio Frequency Identification (RFID) trends. file:///F:/www/cse574-06/ftp/rfid/index. htm.
- Kelly, E. P., & Erickson, G. S. (2005). RFID tags: commercial applications v. privacy rights. Industrial Management & Data Systems, 105(6), 703-713.
- Kumar, V. (2008). Implantable RFID Chips. In The Future of Identity in the Information Society (pp. 151-157). Springer, Boston, MA.
- Le Calvez, S., Perron-Lepage, M. F., & Burnett, R. (2006). Subcutaneous microchip-associated tumours in B6C3F1 mice: a retrospective study to attempt to determine their histogenesis. Experimental and Toxicologic Pathology, 57(4), 255-265.
- Leaders, M. A., Calculator, V. S., Network, A. C. A., & Store, A. V. M. A. (2013). Microchipping of Animals. Backgrounder.
- Levine, M., Adida, B., Mandl, K., Kohane, I., & Halamka, J. (2007). What are the benefits and risks of fitting patients with radiofrequency identification devices?. PLoS medicine, 4(11), e322.
- Lewan, T. (2007). Chip implants linked to animal tumors. Washington Post, 8.
- Masters, A., & Michael, K. (2007). Lend me your arms: The use and implications of humancentric RFID. Electronic Commerce Research and Applications, 6(1), 29-39.
- Michael, K., Michael, M. G., & Ip, R. (2008). Microchip implants for humans as unique identifiers: a case study on VeriChip.

- Occhiuzzi, C., Contri, G., & Marrocco, G. (2012). Design of implanted RFID tags for passive sensing of human body: The STENTag. IEEE Transactions on Antennas and Propagation, 60(7), 3146-3154.
- Perakslis, C., Michael, K., Michael, M. G., & Gable, R. (2014, June). Perceived barriers for implanting microchips in humans: A transnational study. In Norbert Wiener in the 21st Century (21CW), 2014 IEEE Conference on (pp. 1-8). IEEE.
- Piesnack, S., Frame, M. E., Oechtering, G., & Ludewig, E. (2013). Functionality of veterinary identification microchips following low-(0.5 tesla) and high-field (3 tesla) magnetic resonance imaging. Veterinary Radiology & Ultrasound, 54(6), 618-622.
- Rotter, P., Daskala, B., & Compañó, R. (2012). Passive Human ICT Implants: Risks and Possible Solutions. In Human ICT Implants: Technical, Legal and Ethical Considerations (pp. 55-62). TMC Asser Press.
- Rotter, P., Daskala, B., Compañó, R., Anrig, B., & Fuhrer, C. (2012). Potential Application Areas for RFID Implants. In Human ICT Implants: Technical, Legal and Ethical Considerations (pp. 29-39). TMC Asser Press.
- Singh N, Bhatt J, Purohit KC. (2017) A survey on IoT and Security issues of RFID. International Journal Of Engineering And Computer Science 6(4): 21061-21066.
- Steffen, T., Luechinger, R., Wildermuth, S., Kern, C., Fretz, C., Lange, J., & Hetzer, F. H. (2010). Safety and reliability of radio frequency identification devices in magnetic resonance imaging and computed tomography. Patient safety in surgery, 4(1), 2.
- Tillmann, T., Kamino, K., Dasenbrock, C., Ernst, H., Kohler, M., Morawietz, G., Campo, E., Cardesa, A., Tomatis, L., & Mohr, U. (1997). Subcutaneous soft tissue tumours at the site of implanted microchips in mice. Experimental and Toxicologic Pathology, 49(3-4), 197-200.
- Urano, K., Suzuki, S., Machida, K., Sawa, N., Eguchi, N., Kikuchi, K., ... & Usui, T. (2006). Use of IC tags in short-term carcinogenicity study on CB6F1 TGrasH2 mice. The Journal of toxicological sciences, 31(5), 407-418.
- Vascellari, M., Melchiotti, E., & Mutinelli, F. (2006). Fibrosarcoma with typical features of postinjection sarcoma at site of microchip implant in a dog: histologic and immunohistochemical study. Veterinary Pathology, 43(4), 545-548.
- Werber, B., & Žnidaršič, A. (2015). The use of subcutaneous RFID microchip in health care-a willingness to challenge. Health and Technology, 5(1), 57-65.

CAT: QA-02-18-125-EN-C (paper)
CAT: QA-02-18-125-EN-N (pdf)

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

Documents

Visit the European Parliament website:
http://www.europarl.europa.eu/supporting-analyses

PHOTO CREDIT:
iStockphoto.com; Shutterstock/beboy

ISBN 978-92-846-2602-1 (paper)
ISBN 978-92-846-2603-8 (pdf)

doi:10.2861/34896 (paper)
doi:10.2861/15617 (pdf)

Publications Office

The Use of Chip Implants for Workers