Privacy-invading technologies : safeguarding privacy, liberty & security in the 21st century

Klitou, D.G.

7 HUMAN-IMPLANTABLE MICROCHIPS: Location-awareness & the dawn of the Internet of Persons

7.1 CHAPTER INTRODUCTION

In an age of sophisticated location-based services (LBS)[449] and GIS, and at the dawning of the 'ubiquitous information society' as a result of RFID, the development and deployment of HIMs, and their prospective added linkage to GPS satellites, for human identification and tracking purposes, may have certain security, health, convenience and commercial benefits. However, HIMs also raise serious concerns whether or not the existing legal framework in the US is adequately capable of protecting the core principles of privacy protection and democratic freedoms.

Section 7.2 explains the technology behind human-implantable microchips. Section 7.3 describes the social and privacy implications of the identification and tracking capabilities of human-implantable microchips and other location-based services. Moreover, the section focuses on how human-implantable microchips can change the nature of the public space and the way we view our bodies. However, for the most part, the ethical or moral issues surrounding the deployment of HIMs are not discussed. Section 7.4 outlines the security gains of human-implantable microchips. Section 7.5 outlines the security drawbacks and risks of human-implantable microchips. Section 7.6 reveals the scope of the actual deployment of human-implantable microchips in the US and abroad, and illustrates the potential further deployment. Section 7.7 describes the possible alternatives to human-implantable microchips. Section 7.8 gives an overview of the statutory law, case law, administrative decisions and soft regulations in the US of special relevance to human-implantable microchips. However, the medical, consumer and financial privacy issues associated with human-implantable microchips are

---

[449] Location-based services and applications allow users to benefit from services that make use of their accurate physical location accessible via, for example, cell phones, smartphones or mobile computing devices (MCDs), and include services to locate in real-time another person or to locate a place or object, such as the whereabouts of the nearest automated teller machine (ATM). Other types of LBS include emergency services, real-time traffic information, route information, and tourist information.

not thoroughly dealt with here[450]. Instead, the focus is on the privacy issues associated with the *identification and tracking capabilities*[451] of human-implantable microchips (RFID/GPS implants) and the legality of processing location information. Section 7.9 assesses and highlights the relevant deficiencies and dilemmas of the US legal framework in terms of safeguarding privacy and civil liberties, with regards to the potential deployment and use of human-implantable microchips. Section 7.10 proposes relevant policy and legislative recommendations to enhance the US legal framework. Section 7.11 concludes with some ending remarks.

For the purposes of this dissertation, HIMs are implantable RFID tags (hereinafter known as "RFID implants") and/or implantable GPS receivers/transponders (hereinafter known as "GPS implants") marketed or sold for human-implantation.[452] *HIMs, for the specific purposes of this dissertation, however, will not include biosensors, sensory amplifiers, cortical implants, cochlear implants, or any other medical device, including Proteus Biomedical's implantable ChipSkin™ or "chip in the pill" technology or the "SmartPill", which adds intelligence to implanted medical devices or medication, nor does it include micro-electrode arrays, wireless implantable sensors or implantable nanomachines.*

7.2 RFID/GPS IMPLANTS AND THE TECHNOLOGY BEHIND THEM

7.2.1 RFID implants

More than four decades ago, Westin had already predicted that "[e]xisting microminiaturized transmitters the size of a pinhead might be coded with an identification number,

---

450 The legislation and regulations that apply to credit and debit cards, such as the Truth in Lending Act and Regulation E, will likely apply, while consumer privacy will be protected to the extent that it is protected under existing laws, such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. see Willingham, Kristina M. Scanning Legislative Efforts: Current RFID Legislation Suffers from Misguided Fears, North Carolina Banking Institute, Volume 11 (2007), pp. 313-341.

451 While to some extent medical privacy issues are touched upon, it is not the central issue that is addressed.

452 HIMs could also be referred to as "ICT implants". see Weber, Karsten. The Next Step: *Privacy Invasions by Biometrics and ICT Implants* (Ubiquity, Vol. 7, Issue 45, 2005), available at: www.acm.org/ubiquity/views/pf/v7i45_weber.pdf; OPINION OF THE EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES TO THE EUROPEAN COMMISSION, Opinion No. 20, Adopted on 16/03/2005.

enclosed in a permanent capsule, and implanted under the skin by a simple and painless surgical operation" for locating individuals (1967, p. 86). At that time, this might have seemed somewhat science fiction, but today this is indeed taking place.

Animals and physical objects have been identified and tracked in supply chain processes using radio frequency identification (RFID) technology for some time now. However, we have moved beyond the use of RFID to expedite logistics and facilitate supply chain management. Now, RFID is becoming a technology of choice for identifying humans. For instance, in the EU, as Eurostat revealed, in 2009 'person identification' (albeit, not implanted) accounted for 56% of all RFID use by enterprises.[453]

RFID is a type of "automatic identification technology" (AIT) or "automatic identification and data capture" (AIDC) technology,[454] which provides the "means of [electronically] identifying things or individuals, collecting data about them, and automatically causing that data to be entered into a computer system, with no human interaction".[455] A RFID tag or microchip is the combination of an antenna coil and a silicon microchip with basic modulation circuitry and memory, and RFID tags can range from a fraction of a millimeter to several millimeters or centimeters.

In a way similar to CDs, RFID tags can be developed as read-only, read-write or write once, read many (WORM). Read-only tags contain data, which is added or 'written' during their manufacture, which cannot be changed, removed or augmented, similar to an original CD album commercially sold. Additional data can later be 'written' on read-write tags by command pulses from a read-write RFID interrogator/reader. The data on WORM tags is not set during their manufacture, but rather set the first time it is used, similar to a blank non-rewritable CD.

RFID tags can either be passive or active. The latter are powered by a battery and constantly transmit their data, while the former are activated by the radio frequency (RF) signal emanated from RFID readers/interrogators and only transmit their data when activated. In order to allow multiple RFID tags to be read simultaneously by a single reader without their signals interfering with each other, the reader employs an anti-collision algorithm, which controls access to the shared radio channel or frequency (Floerkemeier et al., 2005, p. 3).

---

453 For further information, see Eurostat news release at: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-19012010-BP/EN/4-19012010-BP-EN.PDF

454 Other types of AIDC technology or AIT include: bar codes, QR Codes, optical character recognition, and biometric technology.

455 The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, p. 2, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

When a passive RFID tag is in the presence of an appropriate RF signal, emanated continuously by an RFID reader's antennae, it sends in response its stored data (ID number, etc.) to the reader using the reader's own carrier signal. The reader can range from inches to several feet away and the direct line of sight or physical contact between the tag and reader is not required. Passive RFID tags also do not need a battery since they are powered by the reader's signal.

Each time a RFID tag or RFID implant is read, a tag read event (TRE) is generated, which can automatically be registered and stored in a computer database. TREs can contain, in addition to the unique ID number, the antenna's ID number that read the RFID tag or RFID implant (i.e. the location of the RFID reader) and a timestamp.

A RFID implant is a silicon-glass encapsulated, passive and read-only RFID tag, which is normally injected into the right hand or upper right arm by a doctor or medical practitioner using a syringe. Neither surgery nor sutures are required. However, RFID tags can also be implanted into human molars.[456] To enable bonding to human tissue and thereby prevent migration, RFID implants are coated with a polymer. A signal, currently at a low frequency of 125 or 134 kilohertz (KHz), emitted by the antennae of either a fixed location or a wireless handheld RFID reader, remotely activates the RFID implant causing it to transmit its unique ID number (in the case of VeriChip's RFID implant a 16-digit number) back to the RFID reader, which in turn is either wirelessly relayed automatically to a computer or entered manually. The number then can be used to identify the individual and access his or her additional personal information via a computer database or on the Internet, such as medical or financial information or even biometric data, such as a digitized photograph or fingerprint. Typically, around 20 cm is the read range for the low frequency ban of 125-134 KHz, but it can go up to one meter.[457] Currently, the size of implantable RFID tags can range from 8 to 12 mm in length and 1 to 3 mm in diameter. RFID implants can hold anything from 56 to 512-plus bits of data. However, with the advancement of RFID technology, cloud computing and miniature microprocessors, RFID implants (HIMs) will only get smaller and gain augmented data, processing and communication capacities and will be increasingly linked to the 'cloud'.

---

[456] see Thevissen, Patrick., et al. *Implantation of an RFID-tag into human molars to reduce hard forensic identification labor* (Fo*rensic Science International*, Volume 159, 2006), pp. 33-39.

[457] OECD Policy Guidance on Radio Frequency Identification (2008), pp. 33-34.

VeriChip,[458] the only official distributor of human-implantable RFID microchips,[459] first marketed their product as a means of assisting doctors and nurses in emergency situations by providing patient information.[460] When an unconscious patient is administered into a hospital, the medical staff can employ an RFID reader. If the patient has a RFID implant embedded, the reader will indicate its unique 16-digit ID number, which can subsequently be entered manually or wirelessly transmitted to VeriChip's web-enabled database to access the patient's medical and personal information. If the hospital has indeed adopted the VeriMed Patient Identification System protocol in their emergency rooms, medical staff can immediately access the patient's identification and health record – information that can prove vital in an emergency situation.[461] VeriChip implantees can access, via the Internet, the Global VeriChip Subscriber service or VeriMed Registry or VeriMed Health Link System to add personal healthcare information to VeriChip's web-enabled database.[462] The VeriChip RFID implant is 11.1mm x 2.1mm and can hold up to 128 bits of information.

Moreover, VeriChip Corp. (currently known as PositiveID Corp.) has even taken the "capabilities of RFID implantable microchips beyond simple identification" to create the "GlucoChip", which "combines an embedded bio-sensor system on an implanted RFID microchip" (i.e. RFID implant) that enables glucose levels in the body to be measured in real-time.[463] Therefore, while PositiveID Corp. (formerly known as

---

458 In 2009, VeriChip Corporation changed its name to PositiveID Corporation after completing its acquisition of Steel Vault Corporation. Throughout this dissertation, however, the company that created the first FDA approved RFID implant will still be known as VeriChip, in order to avoid confusion.

459 But, VeriChip certainly did not invent the concept of HIMs. see, e.g., U.S. Patent. No. 4,706,689, Issued to Daniel Man on 17 November 1987, which describes a device designed to be implantable behind the ear of a human. The device transmits a signal intended to enable tracking of the implantee. The device operates continuously and is designed to be recharged through external contacts.

460 As outlined later on, VeriChip has also marketed the use of its RFID implants for purposes beyond merely providing medical information when needed.

461 In June of 2007, the American Medical Association concluded that implantable "[r]adio frequency identification (RFID) devices may help to identify patients, thereby improving the safety and efficiency of patient care, and may be used to enable secure access to patient clinical information". American Medical Association, CEJA Report 5-A-07, p. 4, available at: http://www.ama-assn.org/ama1/pub/upload/mm/467/ceja5a07.doc

462 VeriChip and Microsoft have also entered into an agreement, whereby users of the VeriMed Health Link System will now be able to export their information to Microsoft's HealthVault. see Bacheldor, Beth. "Microsoft Partners With Implantable RFID Chip Maker VeriChip", *RFID Journal*, 2 December 2008, available at: http://www.rfidjournal.com/article/articleview/4477/1/1/

463 see http://www.positiveidcorp.com/products_glucochip.html

VeriChip Corp.) has apparently stopped marketing the VeriChip implant, the company has changed the name to "GlucoChip" and integrated additional capabilities.

7.2.2 GPS implants

GPS tracking devices have also become an accepted tool of law enforcement agents to covertly track suspects or overtly track sex offenders and of business owners to track employees, while other location-aware devices, such as GPS-enabled mobile phones and their corresponding applications have also become extremely popular.

The GPS is a US space-based Global Navigation Satellite System (GNSS) that provides reliable positioning services to civilian users on a continuous worldwide basis. The GPS is made up of three parts: 24 satellites orbiting the Earth; monitoring stations on Earth; and the GPS receivers owned by end-users. GPS satellites transmit signals from space that are picked up and identified by GPS receivers. The GPS receiver in turn calculates or triangulates its own position every second or few seconds, consisting of current longitude, latitude, altitude and time, based on the readings from the satellites with an accuracy of a few feet or better anywhere on Earth.[464] GPS receivers alone do not disclose location information. However, when combined with data transmission technology or cellular phone technology, GPS receivers can disclose the geographic coordinates to another party.

GPS implants are the combination of the technology of GPS and cell phones, creating an enduring sub-dermal personal locating device (PLD). The GPS implant uses GPS to accurately locate itself and the cellular phone network to transmit its location. The cellular phone network enables the GPS implant to continue to function in areas such as underground subway tunnels. GPS especially has some problems in urban areas, indoors and other GPS-impaired environments that lack direct line-of-sight to GPS satellite signals. But, A-GPS (Assisted GPS) and, as proposed by Darren Murph, a so-called "GPS repeater" can enhance the ability of GPS devices to receive signals indoors, underground and in dense urban areas.[465]

The way in which GPS implants are meant to work is the following. GPS satellites send a signal to the implant which then in turn relays a radio signal via the cellular phone network, using a built-in transponder or General Packet Radio Service (GPRS)

---

[464] see the US Government website on GPS, available at: http://www.gps.gov

[465] see Murph, Darren. "Underground / indoor GPS repeater maintains your position" (Engadget, 21 February, 2007), available at: http://www.engadget.com/2007/02/21/underground-indoor-gps-repeater-maintains-your-position/

module, to "push" a stream of accurate real-time geographic coordinates to a monitoring station where it can be digitally stored on Internet servers or computer databases to form what Morris et al. (2004) have termed "digital trail libraries".

GIS software can then plot the GPS implantee's movements and convert or interpret geographic coordinates into understandable street addresses. Integrating hardware, software and data, GIS allows users to view geographic coordinates or data in different ways and reveal relationships, patterns and trends in the form of maps, reports and charts. There are three views: the database view; the map view; and the model view.[466]

Despite earlier reports that GPS satellites are deteriorating,[467] the system is instead currently undergoing a multi-billion dollar upgrade, which will gradually replace satellites, meant to significantly improve accuracy and deliver new capabilities in the future.[468] Besides, an alternative or complementary to GPS is 'Galileo', the European GNSS currently being established by the EU and European Space Agency (ESA), with scheduled completion by 2013. Similar to GPS, Galileo will be an open service to everyone. GPS and Galileo will be capable of operating together, allowing future interoperable multi-signal receivers to receive signals from both systems, which is also expected to improve accuracy and reliability.

For now, the GPS element, in particular, requires the implant to be considerably larger than ordinary RFID implants and requires considerable more energy. GPS implants could be powered by a thermo-couple circuit that produces voltage from the fluctuations in body temperature or electromechanically through the movement of muscles in the body.[469] Even more revolutionary, a small external power source, attached anywhere on the human body with electrodes and using the human body's electrical conductive properties, could also possibly power the GPS implant.[470] Alternatively, however, as part of a Personal Area Network (PAN), RFID implants could perhaps

---

466 see the Guide to Geographic Information Systems, available at: http://www.gis.com

467 see Johnson, Bobbie. "GPS system 'close to breakdown'" (The Guardian, 19 May 2009), available at: http://www.guardian.co.uk/technology/2009/may/19/gps-close-to-breakdown

468 see Hennigan, W.J. *GPS is getting an $8-billion upgrade* (Los Angeles Times, 23 May 2010), available at: http://articles.latimes.com/2010/may/23/business/la-fi-gps-20100523

469 see U.S. Patent No. 5,629,678, Issued 13 May 1997, describes an apparatus for tracking and recovering humans utilizing an implantable transceiver powered electromechanically through the movement of body muscle.

470 see U.S. Patent No. 6,754,472, entitled "Method and apparatus for transmitting power and data using the human body", Issued to Microsoft Corporation on 22 June 2004. (Similarly, Xega, a security firm in Mexico, has also started offering HIMs that apparently send radio signals to a special GPS device carried by the implantee, which can then be used to determine the location of that person if he or she were to be kidnapped).

communicate with the GPS microchips and GPS applications already widely available within smartphones and, as a result, lower the energy requirements of HIMs.

7.3 LOCATION-AWARENESS AND THE DAWN OF *AN INTERNET OF PERSONS*

7.3.1 The capabilities of HIMs

The capabilities and privacy risks associated with HIMs are significant. Although VeriChip, for example, primarily markets their product (a RFID implant) for medical applications,[471] RFID implants can be used to identify and track/monitor the movements of living organisms, both human and animal.

However, as the staff of the Federal Trade Commission (FTC) rightfully point out, "RFID by itself is not a location-tracking technology".[472] There are significant infrastructure requirements. In order to enable RFID to track the movements of people, the widespread, strategic and registered placement of RFID readers, linked to computer databases, in synergy with RFID implants (or other RFID tags associated with persons one way or another), is required. Interoperable RFID readers, wirelessly linked to the Internet and positioned by public authorities and/or private entities at the entrance of airports, train stations, government buildings, stores/shopping centers, etc., throughout highways and cities, and attached to CCTV cameras, can enable the tracking of the daily movements of RFID implantees (or anyone for that matter in possession of a RFID tag coupled with personal information).

The potential widespread deployment of RFID-enabled mobile phones will only enhance that capability by increasing the number of RFID readers in the global infor-

---

471 However, VeriChip has promoted their RFID implant for other purposes.

472 RFID: Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report From the Staff of the Federal Trade Commission [hereinafter called "FTC staff report on RFID"], FTC, March 2005, p. 3, available at: http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf
Moreover, RFID technology and its applications do not always present threats to privacy and personal data protection. Examples of non-threatening RFID applications may include document management, supply chain management and other Business-to-Business services.

mation system.[473] In addition, the RFID readers can be integrated with GPS technology, similar to the scheme developed by EarthSearch Communications. For the most part, the tracking capabilities of RFID implants are proportional to the number of readers deployed in public. On the other hand, Wi-Fi based RFID systems, like the technology pioneered by AeroScout,[474] and the use of a higher RF signal, can considerably reduce the number of RFID readers needed to track the movements of millions and millions of people (implantees).

Like GPS satellites, RFID technology and the corresponding infrastructure will also play a significant role in changing the nature of the public space. As Rob van Kranenburg explains, "the satellite infrastructure [GPS] creates connectivity from above. The RFID infrastructure creates connectivity from below".[475] While the GPS network, combined with the cellular network, can constantly relay an individual's exact location anywhere, RFID is more effective and convenient for tracking individual's movements within buildings. The Ubisense system, for example, using RF technology, can reveal the exact location in real-time of any number of individuals in huge complex sites within 15 cm of accuracy and render this information in 3D visualizations on screens.[476]

The capability of RFID technology to track movements indoors and reveal habits and relationships of individuals was already demonstrated ironically on the British TV show *Celebrity Big Brother*. RFID readers were installed by Wavetrend in numerous locations within the 'Big Brother house', while the housemates were made to wear RFID tags. Wavetrend's AssetTrace allow the show's producers to view on a screen the floor plan of the house and each participant's location in real-time. According to the show's producers, the scheme will enable the TV show's psychologists to interpret the

---

473 There is a real possibility that RFID readers will be integrated into most new cell phones within a couple years. see Lomas, Natasha. "RFID could be in all cell phones by 2010" (ZDNet News, 25 June 2009), available at: http://news.zdnet.com/2100-9595_22-315292.html; Nokia and Samsung have already unveiled RFID mobile phone readers, and there were rumors that the next-generation iPhone (v.4) will have a built-in RFID reader. These rumors are substantiated by the fact that Apple has applied for a patent for a touch screen RFID tag reader. However, as of June 2010, this has yet to manifest and the just released iPhone v.4 does not have a RFID reader. The reasons for the delay could be the uncertainties of manufacturers due to the privacy concerns, lack of adequate standards and legal deficiencies.

474 see AeroScout, available at: http://www.aeroscout.com/content.asp?page=SystemOverview

475 van Kranenburg, Rob. The Internet of Things: *A critique of ambient technology and the all-seeing network of RFID*, Network Notebooks 02, Institute of Network Cultures (2008), p. 18, available at: http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf

476 see Ubisense, available at: http://www.ubisense.net/content/8.html

celebrities' behavior and question the housemates who have been voted off about their movements within the house.[477]

Essentially, RFID implants can broadcast the implantee's unique ID number, which may serve as a means of identification, to anyone or anything with a RFID reader within inches to several feet/meters away. The greater the radio frequency in which RFID implants operate, the greater the distance from which they can be read by RFID readers. The greater the 'read range' of RFID implants, the greater their capability to keep track of movements, and thus essentially the privacy-intrusive capability of RFID implants is, in part, directly proportional to the radio frequency.[478] However, a frequency higher than 125 or 134 KHz may be required to significantly improve the tracking capabilities of RFID implants, but not too high, as this would hamper the RF signal's capability of penetrating an implantee's flesh, since "low frequency signals penetrate liquids more easily"[479] and humans are mostly made up of water. Nevertheless, RFID readers with more powerful antenna could potentially read the RFID implants beyond their standard or nominal read range, known as the "rogue scanning range",[480] and the use of a second reader could "eavesdrop" on the RFID implant at a greater distance than the rogue scanning range.[481]

In addition to the distance at which RFID tags can be read, as the OECD Policy Guidance on Radio Frequency Identification also points out, the potential privacy invasion through the use of RFID is also likely to be proportional to the possibility of revealing "sensitive information about individuals through inferences and profiling", the degree of interoperability and the tracking capabilities.[482] With the increasing advancement of RFID technology, including augmented data, processing and communication capacities, the privacy-intrusive capabilities of RFID implants will equally increase.

---

477 see Swedberg, Claire. "RFID Works for Big Brother" (RFID Journal, 7 January 2009), available at: http://www.rfidjournal.com/article/articleview/4534/1/1; Savvas, Antony. "Celebrity Big Brother uses RFID technology to track housemates" (Computer Weekly, 6 January 2009), available at: http://www.computerweekly.com/Articles/2009/01/06/234068/celebrity-big-brother-uses-rfid-technology-to-track.htm

478 see OECD Policy Guidance on Radio Frequency Identification (2008).

479 *Ibid.*, p. 31.

480 see "A Holistic Privacy Framework for RFID Applications", Future of Identity in the Information Society, Simone Fischer-Hübner and Hans Hedbom (eds.)., Deliverable D12.3, p. 69, available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp12-del12.3.A_Holistic_Privacy_Framework_for_RFID_Applications_v2.pdf

481 *Ibid*.

482 OECD Policy Guidance on Radio Frequency Identification (2008), p. 53.

HIMs can also be integrated with other technologies. For instance, RFID implants and RFID readers can enhance the capabilities of CCTV surveillance systems. RFID readers attached to or located nearby CCTV cameras could potentially combine visual surveillance with database-linked surveillance capabilities, thereby enabling CCTV camera operators to identify and follow the individual they wish to observe. However, while this may be more practical than using face recognition software, extensive co-ordination between the relevant data controllers is required. RFID implants could also be potentially interfaced with Wi-Fi technology. VeriChip already began the process of interfacing their RFID implants with Wi-Fi, in order "to achieve an even higher level of system integration that collects location-based information".[483]

Generally, tags read events (TREs) can be anonymous at first, but can later be converted into personally identifiable location information. For example, the unique ID number of RFID implants can automatically be coupled with a debit or credit card when an implantee makes a purchase in a shop that contains RFID readers. Such information could later be used to identify and track the implantee and target personalized, real-time, location-based advertisements, either via nearby screens or via mobile phones, as the person passes by any RFID reader associated with the same shop or company.

Linking HIMs to the implantee's bank account, debit card or credit card number could also enable the use of HIMs to make cashless transactions,[484] which is perhaps why some correlate HIMs with the 'Mark of the Beast' as prophesized in the Bible.[485] When an implantee's right arm or hand is scanned, followed by the entering of a PIN, the transaction can be executed.[486] HIMs can, therefore, also enhance the ability of retailers and marketers to meticulously record the consumer habits of individuals.

---

483 see VeriChip Corp.'s 10-K Annual Report for the fiscal year ended 31 December 2007, p. 16, available at: http://www.sec.gov/Archives/edgar/data/1347022/000136231008001657/c72788e10vk.htm

484 ADS revealed at the ID World 2003 International Congress in Paris, France, the company's subdermal RFID solution called VeriPay, which allows the implant to be used to make payments. see McCullagh, Declan."Chip implant gets cash under your skin" (CNET News, 25 November 2003), available at: http://news.cnet.com/2100-1041-5111637.html

485 "He causes all, both small and great, rich and poor, free and slave, to receive a mark on their right hand or on their foreheads, and that no one may buy or sell except one who has the mark or the name of the beast, or the number of his name". (Revelation 13:16).

486 VISA and MasterCard have already developed and deployed contactless smartcards, which make use of RFID, such as MasterCard's PayPass card. Other examples include Exxon Mobil's SpeedPass. In an article, published by TIME Magazine in 1998, entitled "The Big Bank Theory" Joshua Cooper Ramo, et al., proclaimed, "Your daughter can store the money any way she wants--on her laptop, on a debit card, even (in the not too distant future) on a chip implanted under her skin". The question is will this prove true within the next ten years?

However, the concern over remotely tracking people's movements does not only pertain to RFID and/or GPS implants. Although HIMs are the ultimate person-locating device or generator/transmitter of location information, GPS enabled hand-held devices or smartphones and even traditional mobile phones are already capable of being used to track or locate users.[487] The risk is so high that the Secret Service strongly advocated that US President Barack Obama give up his Blackberry for security purposes, since there was a high risk that his location could be determined. Even the Bluetooth signal emitted from mobile phones can be used to track users, as demonstrated by Bath University's Cityware project.[488]

Moreover, RFID tags can be embedded in practically anything people buy or wear, from clothes, watches and shoes to items in a woman's purse such as lipstick, and, similar to RFID implants, can be used to track and identify persons (Albrecht and McIntyre, 2005). People throughout the day normally carry these items. RFID tags are already being embedded in a number of consumer goods. Equally, personally identifiable information (or personal data) can be linked to the unique numbers of the RFID tags embedded in these items when they are purchased using a credit or debit card.[489] As Linda D. Koontz, Director of Information Management Issues at the US Government Accountability Office (GAO), testified, "once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile of the individual".[490]

7.3.2 Location information

HIMs can generate practically limitless amounts of location information on individuals. Here, location information, however, is not limited to where an individual lives or

---

487 The location of traditional cell phones can also be determined or "triangulated", albeit less accurately.

488 The discontinued Cityware project tracked mobile phone users at various locations to study patterns of how people move around cities. The participating users required a Facebook account and the Cityware application and needed to register the Bluetooth ID of their mobile phone. The researchers had set up nodes around the UK and in the US, which constantly scanned for Bluetooth-enabled devices in a given area, and then relayed information to servers, which compared the IDs of the devices with the enabled Facebook profiles. see "Bluetooth helps Facebook friends", (BBC News, 16 August 2007), available at: http://news.bbc.co.uk/2/hi/6949473.stm

489 see FTC staff report on RFID, p. 14.

490 Testimony Before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives, PRIVACY: Key Challenges Facing Federal Agencies, Statement of Linda D. Koontz, Director of Information Management Issues, 17 May 2006, GAO-06-777T, p. 16, available at: http://www.gao.gov/new.items/d06777t.pdf

works and the street addresses thereof, but rather pertains to either information on their daily movements tracked and stored over a prolonged period of time ('mobility data') and/or their accurate, real-time, physical location at any given moment. For the purposes of this dissertation, location information includes, in addition to ordinary street addresses, both geographic coordinates and TREs.

Location information should be considered a category of personal information when it is personally identifiable or can later potentially be construed as such. Location information/data, as the EU's 'ePrivacy Directive' distinguishes in Article 2, is not identical to traffic data processed for the purpose of carrying out a transmission on an electronic communications network or for the billing thereof, but rather is data which indicates the geographic position of the terminal equipment of a user of a publicly available electronic communications service in order to provide a 'value added service' (or location-based service).[491]

The intrinsic market value of the location information generated by HIMs in the so-called 'information age' could potentially result in HIM service providers and/or data controllers succumbing to lucrative temptations and disclosing their customer's location information to a variety of third parties, such as insurance companies, retailers, marketers, data brokers and even law enforcement agencies. As Masters and Michael argue, "[t]he main temptation will be in the value of the data and how it can be used not only to sell value-added services but separate service-sets that rely on location information" (2006, p. 32). Under a 'surveillance-for-profit' scheme, locations, for example, where one travels, eats and shops on a daily basis are just a few examples of information that is very valuable to retailers and marketers (Karim, 2004, p. 495). Location information can, for example, enable location-based advertising (LBA) in real-time. Thus, location information has a huge potential of becoming a key asset within the 'knowledge-based economy' of tomorrow's 'ubiquitous information society'. The location information generated by smartphones has already begun to be provided to marketers to target advertisements based on a person's real-time location and travel patterns,[492] and TechnoCom Corporation, for example, has launched SpotOn GPS, a LBA platform for mobile phones.

However, personally-identifiable location information, as a whole, is considerably more privacy-intrusive than simply revealing the places where a person, on a daily ba-

---

[491] The ePrivacy Directive explicitly regulates 'location data', requiring that the use of non-anonymous location data is particularly restricted to the extent necessary to provide the value added service, and clarifies the scope of the required informed consent (Article 9), and the scope of use without informed consent.

[492] see Clifford, Stephanie. "Advertisers Get a Trove of Clues in Smartphones" (The New York Times, 11 March 2009), available at: http://www.nytimes.com/2009/03/11/business/media/11target.html

sis, shops or eats. As emphasized by the EU's Article 29 Working Party, the processing of location information is a particularly sensitive matter.[493]

7.3.3 Social and privacy implications

Indeed, location information can reveal not just where an individual travels, but potentially more sensitive information associated with where he/she has been, including a person's consumer habits and more private or personal affairs and activities. For example, as Jack Dempsey, currently Vice President for Public Policy at the Center for Democracy and Technology, inquires,

> What if your insurer finds out you're into rock climbing or late-night carousing in the red-light district? What if your employer knows you're being treated for a sexually transmitted disease at a local clinic? The potential is there for inferences to be drawn about you based on knowledge of your whereabouts.[494]

An experiment, carried out by Michael et al. (2006), demonstrated the sensitivity of location information. This study involved a participant who had their daily movements tracked for just two weeks. Each day during the two-week study, the participant carried a Magellan Meridian Gold handheld device either in a bag he carried around or in his pocket. The GPS device was setup to collect location data every three seconds. At the end of each day this data was uploaded into the GIS software "DiscoverAus Streets & Tracks". The study showed that tracking a person's movements over a period of time is relatively easy and can create a detailed profile of that person, including where he/she lives, works and engages in social activities, simply based on his/her daily travel routines (see Michael et al., 2006). As partly demonstrated in a more recent study, involving mobile phone users,[495] a person's movements tracked over a specific period of time

---

493 Article 29 Working Party, Opinion on the use of location data with a view to providing value-added services, November 2005 (WP 115), available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

494 Romero, Simon. "Location Devices' Use Rises, Prompting Privacy Concerns" (New York Times, 4 March 2001), available at: http://query.nytimes.com/gst/fullpage.html?res=9E04E1DC123BF937A35750C0A9679C8B63&sec=&spon=&pagewanted=print

495 The whereabouts of more than 100,000 mobile phone users were tracked in an attempt to build a comprehensive picture of human movements. see Fildes, Jonathan. "Mobile phones expose human habits" (BBC News, 4 June 2008), available at: http://news.bbc.co.uk/2/hi/science/nature/7433128.stm

can be used to construct a profile of that person. These profiles, for example, can be used by the private sector for conducting market research and categorizing people and can also be useful for law enforcement agencies. Nevertheless, the privacy implications of tracking a person's movements and/or disclosing a person's location information also depend, to a certain point, on the type of activities that person engages in.

The ability of HIMs (or simply RFID tags) to identify/track individuals can thus lead to the development of profiles based on their movements and whereabouts. These studies have also shown that location information can be used for analyzing an individual's past movements in order to potentially determine a person's future movements. Even an individual's social interactions/social relationships can be potentially determined.[496] Location information, as a result, significantly further adds to the capability of creating "digital dossiers" on every person (Solove, 2004) in possession of a mobile phone/smartphone or implanted with a HIM.

Furthermore, since implantees will essentially not know when their RFID implant has been read and by whom, they must then bear an even greater risk of losing control of their personal data, if the relevant safeguards are not implemented to prevent this from happening.

The widespread deployment and use of RFID implants (or RFID tags) and RFID readers, whereby the implants/tags become a critical element in the granting or denying of physical access or the granting or denying of certain advantages, could also potentially add to the "digital divide"[497] and broaden discrimination in the digital age, as the non-implanted are faced with increasing disadvantages in a ubiquitous information society. However, since the digital divide is mostly an issue, at present, of not being able to afford the technology, in addition to not knowing how to use it, and RFID technology in general is rapidly becoming cheaper and is very easy to use, RFID implants will not necessarily add to the digital divide. But, if the people who refuse to be implanted are increasingly disadvantaged and discriminated against, and the law does nothing about it, then RFID implants will indeed rapidly add to the digital divide.

---

496 *Ibid.*

497 There is little consensus over the overall definition of the term "digital divide", but it essentially refers to the growing gap between those who have access to ICT and those who do not or the difference between the "haves" and the "have-nots" of ICT (see Hilbert, 2011, p. 5). Hilbert (2011) argues that the "[d]ifferences in definitions arise because scholars distinguish between (1) the kinds of Information and Communication Technology (ICT) in question; (2) the choice of subject; (3) diverse attributes of the chosen subjects; and (4) levels of adoption, going from plain access to effective usage with real impact" (p. 2). see Hilbert, Martin. *The end justifies the definition: the manifold outlooks on the digital divide and their practical usefulness for policy-making* (Telecommunications Policy, Volume 35, Issue 8, 2011), pp. 715-736, available at: http://martinhilbert.net/ManifoldDigitalDivide_Hilbert_AAM.pdf

While there are already valid concerns over the privacy threats of RFID, there are lots of unknowns. The need for further validating these threats can only come from the deployment of RFID applications. However, applying the *precautionary principle* here would imply that any potential widespread deployment of RFID implants should be put on hold, even before there is hard evidence concerning their tracking capabilities, until we are certain of all the privacy and social implications and the means and preconditions for addressing or preventing them.

7.3.4 A means of control

Human identification and tracking goes beyond privacy, serving as a powerful means of control. As Mark Weiser asserts, in referring to ubiquitous computing, "the problem, while often couched in terms of privacy, is really one of control".[498] If left unchecked, HIMs could pose a serious threat not just to privacy, but also to liberty and human dignity, as the European Group on Ethics in Science and New Technologies (EGE) equally points out.[499] As Melvin Gutterman further asserts:

> [t]he ability to move about freely without constant supervision by the government is an important source of individual liberty that must be addressed. A fear of systematic observation, even in public places, destroys this sense of freedom (1988, p. 706).

HIMs, or RFID technology in general, could have a 'chilling effect' on the freedom of movement, whereby people, concerned that their movements could be tracked and recorded, self-impose limitations on where they actually travel. Even worse, RFID implants could lead to controlled or restricted movement. For example, if RFID implants are used as travel passes for mass public transportation, a person could easily be electronically and remotely denied access. Contactless smart cards are already widely used and could similarly be used to restrict access to mass public transportation. RFID implants (or RFID embedded ID cards/passports) could also have a 'chilling effect' on the freedom of association, since government agents could potentially use RFID

---

498 Weiser, Mark. T*he Computer for the Twentieth-First Century* (Scientific American, Vol. 265, No. 3, September 1991), pp. 94-104.

499 OPINION OF THE EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES TO THE EUROPEAN COMMISSION, Opinion No. 20, Adopted on 16/03/2005.

readers to deliberately determine who is present at a demonstration. Unfortunately, however, these potential threats to personal freedom, posed by RFID and GPS, are being ignored, for the most part, by human rights and civil rights organizations and within human rights reports.

HIMs could serve as a powerful tool of mass control and mass management. For Dobson and Fisher (2003), electronically tracking people's movements and generating location information can lead to a "new form of slavery characterized by location control" or what they term "geoslavery".[500] Herbert (2006) similarly links human tracking to "geoslavery" and further associates the mandatory implantation of identification and tracking devices to slavery control mechanisms, such as branding.[501] Whether or not HIMs (or any other personal location-tracking device) will lead to "geoslavery", their widespread deployment could certainly bring about mass categorization.

In essence, if left unchecked, HIMs could be the last drop in the bucket needed to give rise to an age where omnipresent scrutiny and continuous, real-time surveillance is commonplace and limitless, a society where there will in effect be truly *nowhere to hide* in a global, automated, digital information surveillance-tracking grid that will become increasingly impossible to escape.[502]

7.3.5 Internet of Persons

Proponents of RFID and major investors behind its development and deployment envision the integration or 'bridging', so to speak, of the physical and virtual/digital world in what is now commonly known as the "Internet of Things" (IoT).[503] The IoT is defined as a "network of interconnected objects, from books to cars, from electrical appliances to food".[504] In a full-blown deployment of IoT, billions of physical objects are embed-

---

500 see Dobson, Jerome E. and Fisher, Peter F. *Geoslavery* (IEEE Technology and Society Magazine, 2003).

501 In linking mandatory RFID/GPS implants to a form of slavery, Herbert (2006) also argues that the Thirteenth Amendment of the US Constitution could serve as a basis of prohibiting any mandatory implantation.

502 see e.g. O'Harrow, Robert. *No place to hide* (Free Press, 2005).

503 see the First International Conference on the Internet of Things, Adjunct Proceedings, available at: http://www.iot2008.org/adjunctproceedings.pdf

504 COM(2009) 278 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Internet of Things – An action plan for Europe, p. 2.

ded with RFID tags and assigned, for instance, Electronic Product Codes (EPCs),[505] allowing these objects to be identified and tracked in real-time either in a closed or open network.[506] When an RFID reader reads or interrogates an RFID tag embedded in an object, the EPC number is communicated to computers or mobile devices running relevant middleware, which can then use EPCglobal's Object Name Service (ONS), an automated networking service based on the Domain Name Service (DNS), which directs objects (instead of computers) to websites/web-based databases, in order to identify and track the object and enable access to the stored information on the object.[507] This information can include, in addition to other general product information, its location history or TREs based on the last occasions where the object's embedded RFID tag was read. Specific locations, such as a warehouse, shop or even a store shelf, can also be electronically identified using a Global Location Number (GLN), giving rise to the so-called "Internet of Places".[508] As pointed out in the OECD paper on "RFID: Drivers, Challenges and Public Policy Considerations", "the information infrastructures associated with RFID, in particular with UHF [ultra high frequency] RFID, will increasingly be accessed across IP networks, private intranets and the public Internet".[509]

Essentially, the data from RFID tags can be captured by RFID readers and wirelessly transmitted to computer databases over a network, stored on a server and made accessible anywhere in the world via the Internet, using a web-based application or even a search engine. The objects could then potentially be converted into what Bruce Sterling refers to as "spimes", objects that are location-aware, self-registering and uniquely

---

505 EPCs, first developed by MIT's AutoID Center, are basically standardized codes for RFID tags. If RFID tags indeed eventually replace bar codes completely, as RFID technology advances and becomes cheaper to reproduce, then, as generally purported, EPCs could one day replace Universal Product Codes (UPCs). see Grossman, Lisa. "New RFID Tag Could Mean the End of Bar Codes" (Wired, 26 March 2010), available at: http://www.wired.com/wiredscience/2010/03/rfid/

506 The assigning of IP addresses to objects has called into question the feasibility or rationale of considering IP addresses as personal data.

507 For further explanation, see "Object Name Service (ONS), Version 1.0", EPCglobal Ratified Specification, October 4, 2005, available at: http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_1_0-standard-20051004.pdf

508 An "Internet of Places" is "where information specific to places can be readily picked up by devices and users in specific locations". see Cooper, Joshua and Anne James. *Challenges for Database Management in the Internet of Things* (IETE Technical Review, Vol. 26, Issue No. 5, August 2009), available at: http://tr.ietejournals.org/text.asp?2009/26/5/320/55275

509 OECD (2006), "Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations", OECD Digital Economy Papers, No. 110, OECD Publishing, p. 18.

identifiable, and thus traceable in space and time.[510] With the gradual transition from IPv4 at 32 bits to IPv6 at 128 bits, there will be more than enough IP addresses for practically every single object and human on Earth.[511] On the whole, such a scheme could bring about 'ubiquitous positioning' or an "everyware" world.[512]

IoT is considered an integral part of the so-called "Future Internet" and is widely supported by industry stakeholders and other actors. IoT is also receiving public funding and widespread deployment is expected within the next several years. The IP for Smart Objects Alliance (IPSO Alliance), whose members include Cisco, Google and Intel, is a testament to the backing of the ICT industry's major players towards IoT and using IP as the network for the connection of personal and household 'smart' objects/devices.[513] Interesting enough, CIA Director David Petraeus discussed about the emergence of the IoT and the transformational ability of these smart devices to help the CIA execute their clandestine activities and gather immense quantities of geolocation data on individuals. Petraeus explained that "items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters – all connected to the next-generation internet using abundant, low-cost, and high-power computing".[514]

While the deployment of RFID is spreading and the industry is growing, IoT is still, nonetheless, a promising vision and currently not a reality.[515] It will also require a vast amount of additional data storage space, which is already an issue.[516] In spite of this, IoT

---

510 Sterling, Bruce. *Shaping Things* (MIT Press, 2005).

511 For further explanation see *Embedded, Everywhere: A Research Agenda for Network Systems of Embedded Computers*, Report from the Committee on Networked Systems of Embedded Computers, Computer Science and Telecommunications Board, National Research Council (National Academic Press, Washington, DC, 2001).

512 see Greenfield, Adam. *Everyware: The Dawning Age of Ubiquitous Computing* (New Riders Publishing, 2006).

513 "Smart objects" are essentially objects that are location-aware, possess processing capabilities and are able to 'communicate' with other objects.

514 Ackerman, Spencer. "CIA Chief: We'll Spy on You Through Your Dishwasher" (Wired blogs, Danger Room, 15 March 2012), available at: http://www.wired.com/dangerroom/page/2/

515 For instance, according to a survey in 2009 conducted by Eurostat, only 3% of enterprises in the EU27 use RFID technology. see Eurostat news release at: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-19012010-BP/EN/4-19012010-BP-EN.PDF

516 see a special report on managing information from the Economist, titled "Data, data everywhere", Feb. 2010.

has already called into question the adequacy of the current legal framework in the US and the EU and the potential need for new legislation and/or a new governance model.[517]

But, we are now witnessing just the beginning of this location-aware revolution. As the ultimate vehicles of LBS and location awareness, HIMs could take us to the next level – an 'Internet of Persons'. In the same way RFID tags will usher in IoT, RFID implants will carry on the evolution of the Internet, and could ultimately bring about an "Internet of Persons" (see Figure 1), giving a whole new meaning to being inter-connected to one another or to 'networked individuals' or 'social networking' in tomorrow's ubiquitous information society. This evolution is arguably only a natural development with the growing trend of increasing mobility, ubiquity, traceability, identifiability and heterogeneity of components of the information society, and the growing enterprise for achieving unlimited storage space, bandwidth and Internet access points.

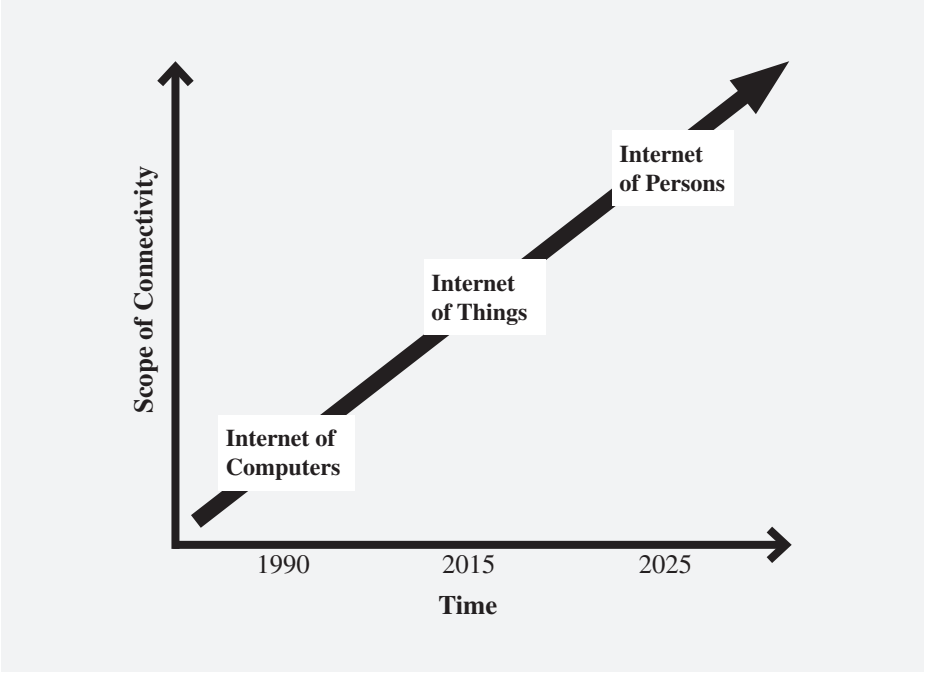

Figure 1: Potential evolution of the Internet

[517] see, for further discussion, for example: Weber, Rolf H. I*nternet of things – Need for a new legal environment?* (Computer Law & Security Review, Volume 25, Issue 6, November 2009), pp. 522-527.

RFID implants, assigned IP addresses and interfaced with the Internet, could in actuality link implantees with the virtual space, breaking the boundaries between the biological and the digital, and indirectly between each other.[518] The "Internet of Persons", for instance, could be based on the EarthSearch Communications' AutoSearchRFID unique solution, which combines data from RFID readers with GPS transmitters' real-time, location-reporting capabilities. While the system was developed for tracking goods or assets, a similar system could be used for RFID implantees. In any case, the TREs, together with the location information of the RFID readers, could be communicated to servers and made available via the Internet (see Figure 2).

As RFID or GPS implantees are transformed into two-way transmitters of information, both emitting as well as receiving data, and active generators of information, rather than passive receivers, "there is no more *we* as in we human beings, the "we" is an information space like any other" (van Kranenburg, 2008, p. 18). Implantees will become one with the global information space and part of the Internet, changing the nature of the human body. This would potentially mark the beginnings of "Internet-enabled people", a concept Vinton Cerf[519] envisaged more than a decade ago,[520] which could enhance the "web presence" of people, meaning that people will become accessible via the Internet through the automatic correlation between a web resource and their physical location, as envisaged by the Hewlett Packard's Internet and Mobile Systems Laboratory.[521] Already, an individual in the US has become the first person to be implanted with a pacemaker connected wirelessly to the Internet that can transmit

---

518 Already, in Japan, cattle have their own IPv6 addresses, enabling farmers to identify and track the cattle throughout the entire production lifecycle.

519 Vinton Cerf, often called "the father of the Internet", was instrumental in the creation of email, the development of TC/IP technology and the founding of the Internet Corporation for Assigned Names and Numbers (ICANN), which he chaired for seven years. At present, Cerf is Google's Chief Internet Evangelist.

520 Cerf, Vinton. "What Will Replace The Internet?" (TIME Magazine, 19 June, 2000), available at: http://www.time.com/time/magazine/article/0,9171,997263,00.html
(In the same article, Cerf gives the following example of the conception of Internet-enabled people. "The speech processor used today in cochlear implants for the hearing impaired could easily be connected to the Internet; listening to Internet radio could soon be a direct computer-to-brain experience!").

521 see Kindberg, Tim., et al. *People, Places, Things: Web Presence for the Real World* (Internet and Mobile Systems Laboratory, HP Laboratories Palo Alto, HPL-2000-16, February, 2000), available at: http://www.hpl.hp.com/techreports/2001/HPL-2001-279.pdf

information to her doctor.[522] RFID implants and the corresponding infrastructure could change not just our relationship and interaction with objects, electronic devices, public or private infrastructure and with each other, but also how we view ourselves and our bodies, now merged in a networked 'intelligent' environment. RFID implants, as technologies of human enhancement,[523] could thus eventually play a significant early role in the transhumanism movement.[524]

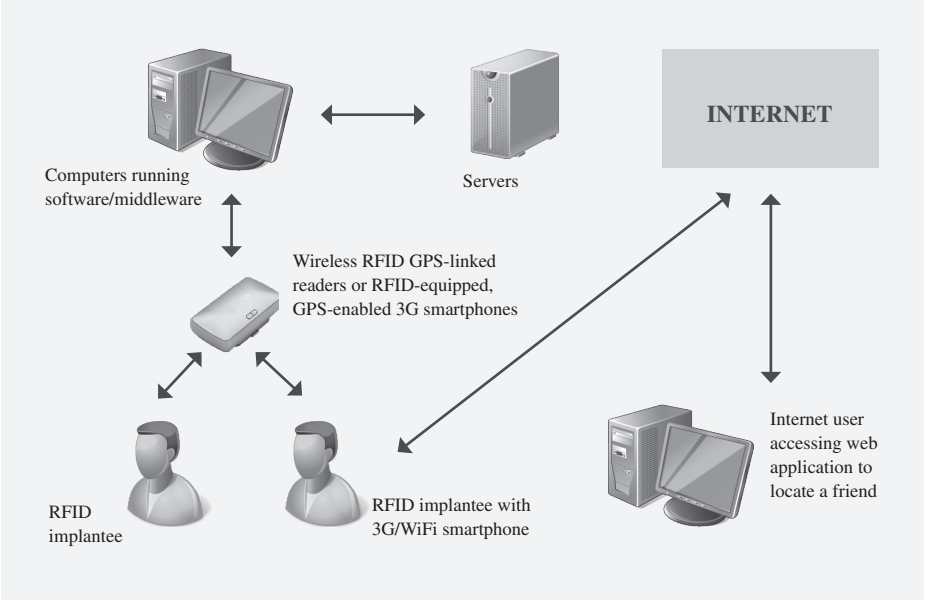

Figure 2: Internet of Persons

522 Gruber, Ben. "First Wi-Fi Pacemaker in the US gives patient freedom" (Reuters, 10 August 2009), available at: http://www.reuters.com/article/idUSTRE5790AK20090810
Such a move is yet another example of the trend of increasing convergence of ICT and life sciences. see Weber, Karsten. *The Next Step: Privacy Invasions by Biometrics and ICT Implants* (Ubiquity, Vol. 7, Issue 45, 2005), available at: www.acm.org/ubiquity/views/pf/v7i45_weber.pdf

523 The human enhancement abilities include, for example, the ability of implantees to automatically open doors and to pay for items.

524 Transhumanism refers to the potential future merger of man and machine, what Ray Kurzwell and others refer to as "singularity", which also describes the era when artificial intelligence is equal to that of human intelligence. Transhumanism aims to augment human capabilities. HIMs are merely just the beginning.

Since HIMs can be interfaced with the Internet, there is the possibility of implantees being able to choose via a web application to automatically have their real-time location information posted on their social networking webpage or blog or even perhaps sent via services such as Twitter,[525] which would mean that a person's location information could be publicly available to anyone with access to the Internet. This information could thus also potentially be searchable on a search engine, such as Google. This would lead to what the Royal Academy of Engineering terms "Google spacetime",[526] whereby the location of a specified individual at some particular time and date can be searched on Google or another search engine, essentially again converting people into Sterling's "spimes" (2005). Even more, similar to Alcatel-Lucent's touchatag solutions (formerly known as Tikitag) and the concept of 'augmented reality', when a RFID implant is read by an RFID-enabled smartphone, for instance, the relevant implantee's personal website or social networking webpage could be launched on a smartphone, tablet PC or other MCD.[527]

While RFID implants can move us beyond today's Internet and past IoT, GPS implants can propel us beyond today's location-aware applications. GPS implants can improve the ability of being automatically notified of the location of a friend if and when he or she is within a certain distance nearby or being able to look up a friend's real-time location, regardless if RFID readers are present, via the Internet using, for instance, a smartphone.

7.3.6 Nearly there

The path towards the ultimate location-aware world that HIMs promise has already been initiated. A continuous wave of GPS-equipped smartphones and tablet PCs and a multitude of GPS tracking devices or personal locating devices (PLDs)[528] and servic-

---

525 Foursquare, a location-based social application, already enables users to automatically integrate their location "check-ins" with their tweets on Twitter.

526 *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (The Royal Academy of Engineering, London, 2007), available at: http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf

527 Already, the Astonishing Tribe, a Swedish mobile software developer, has developed software, which runs on camera-equipped smartphones, that can recognize a person's face and then launch links to that person's social networking websites on a smartphone/mobile device. The system integrates facial recognition, augmented reality and social networking. This development has been dubbed "augmented ID". For more info, see http://www.tat.se

528 see section 7.7 for an outline of the multitude of GPS tracking devices and PLDs (and corresponding services), which have recently hit the market and may serve as an alternative to GPS implants.

es[529] have hit the market over the past couple years, and the LBS market is also growing at a remarkable rate. In addition, the location-aware and processing capabilities of the microchips for smartphones are continuously advancing.[530]

As a result, millions of people are walking around with a device (i.e. a smartphone), albeit not implanted, but rather carried around in their pocket or purse, that can accurately pinpoint, track and transmit where they are at all times and, with a location-aware application, use that location information, in combination with web-based data, to find out what and who is nearby or provide other LBS.[531] The iPhone and Google's Android smartphones have a multitude of applications that tap into the available location information generated via GPS or the available cell phone data.[532] Even applications, such as games, that do not require location information to serve their purpose collect location information. Likewise, the Palm Pre smartphone, for example, transmits the user's location information back to Palm's servers without the user's permission and even when no location-aware application has been activated on the Pre, as programmer Joey Hess discovered.[533] The same was also later discovered about Google's Android smartphones and Apple's iPhone.[534]

Google has already launched an "Add Location" feature, which automatically adds location information to the sender's signature in Gmail, but this is based on the sender's device IP address as opposed to geographic coordinates derived from GPS. Develop-

---

529 Personal locating services include, for example, OnStar's "Family Link" service, which allows for vehicles equipped with OnStar to be tracked and authorized individuals to monitor the vehicle movements via the OnStar's website.

530 For instance, Broadcom has began to market the 4752 microchip for smartphones that can pinpoint the phone's location with ultimate precision, potentially within a few centimeters both outdoors and indoors, by receiving GPS, cell-phone and Wi-Fi signals and also input from gyroscopes, altimeters, etc. For further information, see Mims, Christopher. "A new microchip knows just where you are, indoors and out" (MIT: Technology Review, 9, April 2012), available at: http://www.technologyreview.com/communications/40075/?p1=A1

531 see Honan, Mathew. "I Am Here: One Man's Experiment With the Location-Aware Lifestyle" (Wired Magazine, 19 January 2008), available at: http://www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig

532 The Garmin-Asus' Nüvifone G60, for instance, had also planned to put location-awareness as an integral part of its capabilities, whereby location information provided by GPS is integrated into everything, from emails, text messages and photos to social networking and even gaming

533 see Joey Hess' explanation, available at: http://kitenet.net/~joey/blog/entry/Palm_Pre_privacy/

534 The security analyst Samy Kamkar recently discovered that Google's HTC Android smartphone collected its location every few seconds and directly transmitted the location data, including a unique phone identifier, to Google several times an hour. see Angwin, Julia., Jennifer Valentino-Devries. "Apple, Google Collect User Data" (Wall Street Journal, Technology, 22 April 2011).

ers of web browsers are now more and more ensuring that their software supports both location-aware web-based applications and location-aware web browsing. Mozilla's Firefox now enables web applications to automatically know where the user is located, which will, for example, provide local search results without the need to include a post-code in the search query.

People are more and more revealing what they are currently doing via Twitter, what is currently on their mind via Facebook, and what they are currently working on via LinkedIn. Now, letting people, or the world for that matter, know where you are precisely continuously in real-time is increasingly becoming popular. This popularity will likely only increase, since Twitter has integrated location data into 'tweets' through geo-tagging, whereby location information can automatically be annotated to a person's tweets, and Facebook has also announced that it plans to integrate location-based features.

There are already now a multitude of dedicated location-aware applications, which enable users to reveal exactly where they are in real-time. These applications, which operate on GPS-equipped smartphones and tablet PCs, are changing our daily lives. As Mathew Honan explains, "[t]his one input – our coordinates – has the potential to change all the outputs. Where we shop, who we talk to, what we read, what we search for, where we go – they all change once we merge location and the Web".[535] In addition to the LBS available on smartphones, there are other services, systems or devices that are capable of collecting and subsequently retaining location information, such as intelligent transportation systems (ITS) and automatic license plate recognition (ALPR) or automotive number plate recognition (ANPR) systems. However, while many of the location-aware applications on smartphones, for example, simply enable location-relevant searches, such as nearby restaurants and venues,[536] a number of these applications are in fact focused on keeping track of the movements of individuals.

LifeAware not only tracks you via your smartphone, it also allows you to connect with other people running the application on their smartphones, showing you their current location.[537] *Loopt* provides a service, whereby users can discover where their friends are located and even what they are doing via detailed, interactive maps on their

---

[535] see Honan, Mathew. "I Am Here: One Man's Experiment With the Location-Aware Lifestyle" (Wired Magazine, 19 January 2008), available at: http://www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig

[536] see Biba, Erin. "Inside the GPS Revolution: 10 Applications That Make the Most of Location" (Wired Magazine, 19 January 2008), available at: http://www.wired.com/gadgets/wireless/magazine/17-02/lp_10coolapps?currentPage=3

[537] LifeAware, available at: http://www.lifeaware.net/

smartphones.[538] *Highlig.ht* and *Ban.jo* alert users when their (Facebook) friends are nearby. *Sonar*[539] also determines if any friends (or friends of friends) are close by based on a user's Facebook networks. *Sniff* lets users instantly locate their friends anywhere in real-time using their smartphone. *Glancee* even lets you know when other people with similar interests are nearby. *WhosHere also* enables users to locate people in real-time that match their profile anywhere in the world. Other location-based services include *Foursquare* and the location-based social network websites *Whrrl*[540] *and BrightKite.*[541] Another smartphone application called *Glympse* enables users to broadcast where they are in real-time. GTX Corp. has developed an iPhone application called *LOCiMe*, which converts the smartphone into a 2-way GPS receiver, allowing users to locate their friends and transmit their location to others.

Google has also launched *Latitude*, free software that enables people to always keep track of each other using their smartphones. *Latitude* could potentially be used as a tool, for example, by parents to keep tabs on their children's' location. However, it can be used by anyone to find anyone else, assuming permission is given.[542] On the other hand, *Latitude,* like *Loopt,* apparently does not keep a log of the real-time location data. On the other hand, *Latitude* is set by default as a website with authorization to Gmail accounts. The latest addition to Google's *Latitude* is the "Public Location Badge", which enables users to share their location on their blog or website, but without the ability to limit who will be able to access this location information, since it will be publicly available to everyone with access to the Internet.

Furthermore, Sprint launched the Business Mobility Framework,[543] which allows employers to track employees, and other companies have also launched similar systems. It is already common for GPS to be used to track certain categories of employees in their vehicles, such as taxi drivers[544] and contractors, whether they like it or not, and

---

538 Loopt, available at: http://www.loopt.com/

539 Sonar, available at: http://sonar.me

540 Whrrl, available at: http://www.whrrl.com/

541 Brightkite, available at: http://brightkite.com/

542 Google Mobile, available at: http://googlemobile.blogspot.com/2009/02/locate-your-friends-in-real-time-with.html

543 Sprint, available at: http://www.sprint.com/business/products/products/bmf.html

544 see Karni, Annie. "GPS Concerns Taxi Drivers" (New York Sun, 5 January 2007), available at: http://www.nysun.com/new-york/gps-concerns-taxi-drivers/46133/

the law does little to prohibit this activity. RFID is also already increasingly being used to register the comings and goings of employees at their place of work.

However, unlike the LBS or location-aware applications available on smartphones, the location information generated by HIMs, at present, may be more difficult for implantees to manage. For example, HIMs make it impossible to falsify one's location and smartphones do not normally broadcast an individual's identity, unlike RFID implants. Smartphones can simply be left at home or the LBS on smartphones can be deactivated. In addition, most smartphones, at least for now, normally do not constantly transmit their location.

7.4 POTENTIAL SECURITY AND WELL-BEING BENEFITS

The common good of public security and security of critical infrastructure, in addition to the other benefits, which HIMs could help to enhance, is perhaps why people might be open to their widespread deployment. There are indeed various legitimate non-medical uses of HIMs, ranging from identifying employees at secure facilities to locating a missing child and tracking criminals.

The occurrence of child abductions every year in the US is disturbing,[545] while the number of involuntary missing children is daunting.[546] This has led some parents and RFID/GPS profiteers, such as VeriChip/ADS, to suggest implanting HIMs in children. Indeed, if an abducted child had been implanted with a RFID implant, his or her

---

[545] On the other hand, Frank Furedi argues that the fear of parents over their child being kidnapped is not justified by the figures and that this fear is mostly hyped by the media (2006, p. 32). However, according to a 2002 report by the U.S. Department of Justice, in 1999 there were an estimated 33,000 nonfamily child abductions and 115 child abductions of the stereotypical type in the US. "A nonfamily abduction occurs when a nonfamily perpetrator takes a child by the use of physical force or threat of bodily harm or detains a child for at least 1 hour in an isolated place by the use of physical force or threat of bodily harm without lawful authority or parental permission; or when a child who is younger than 15 years old or is mentally incompetent, without lawful authority or parental permission, is taken or detained by or voluntarily accompanies a nonfamily perpetrator who conceals the child's whereabouts, demands ransom, or expresses the intention to keep the child permanently." "Stereotypical kidnappings are the particular type of nonfamily abduction that receives the most media attention and involves a stranger or slight acquaintance who detains the child overnight, transports the child at least 50 miles, holds the child for ransom, abducts the child with intent to keep the child permanently, or kills the child. They represent an extremely small portion of all missing children". see Sedlak, Andrea J., et al. "National Estimates of Missing Children: An Overview" in *National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children*. (Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice, October 2002), pp. 4-7, available at: http://www.ncjrs.gov/pdffiles1/ojjdp/196465.pdf

[546] However, nearly a third of all missing children have benign explanations, but account for many of the reported cases to the police. see Ibid., p. 6.

location could be determined if the child comes near to a RFID reader linked to the Internet.[547] However, RFID implants could be potentially destroyed using microwaves or obstructed by covering the implantee's arm with metal. In extreme cases, the implantee's arm or hand could either be cut off or his or her captors could simply carve the HIM out.[548]

On the other hand, if a child implanted with a GPS implant was kidnapped or abducted, his or her exact, real-time location could be provided without delay to the police and enable AMBER Alerts distributed via text messages based on the physical location of subscribers determined via their smartphone or their own HIM, informing people that a child of a certain description has gone missing in their vicinity or is located in their vicinity. This is especially important since experience has shown that an abducted child's chance of survival dramatically decreases after the first day, and so the ability to locate the kidnapped child immediately is crucial. However, since nearly all reported cases of missing children have benign explanations,[549] the ability of parents to immediately and easily locate their children through GPS via the Internet could, in theory, reduce avoidable emergency calls. Additionally, if a child implanted with a GPS implant were to become lost, for example, in a forest, a search and rescue team would effortlessly be able to locate him or her.

But, even the GPS signal received by GPS implants can be 'spoofed', as demonstrated by researchers at Cornell University, who spent more than one year building equipment that can transmit fake GPS signals capable of fooling receivers.[550] This would result in transmitting the wrong signal to the implant and inaccurate location information to the HIM service provider, rendering the GPS implant not very helpful to the implantee if he/she indeed needed to be located as a consequence of being kidnapped or of becoming involuntary lost or missing. GPS signals can also be potentially 'jammed' using commercially available jamming devices.

---

547 Solusat, the Mexican distributor of the VeriChip, is marketing the device as an emergency ID tag called VeriKid. see Scheeres, Julia. "Tracking Junior With a Microchip" (Wired News, 10 October 2003), available at: http://www.wired.com/science/discoveries/news/2003/10/60771

548 Perhaps, even a child wearing something which states, "I have an implant" could have the similar deterrent effect that signs placed in homes stating "Beware of Dog" or other home security warning stickers may have.

549 see Sedlak, Andrea J., et al. "National Estimates of Missing Children: An Overview" in *National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children*. (Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice, October 2002), available at: http://www.ncjrs.gov/pdffiles1/ojjdp/196465.pdf

550 Ju, Anne. "Researchers raise uncomfortable questions by showing how GPS navigation devices can be duped" (Cornell Chronicle, 19 September 2008), available at: http://www.news.cornell.edu/stories/Sept08/GPSSpoofing.aj.html

HIMs can also provide a secure form of identification, but this is debatable (see Section 7.5 for further discussion). Unlike conventional forms of identification, such as ID cards or passports, HIMs cannot be lost or stolen. RFID implants, for example, could be used to verify the identity of a person before granting their entry into secure sites, such as nuclear facilities. RFID implants and the strategic deployment of fixed and mobile RFID readers can theoretically provide companies or government agencies with the ability to both unmistakably identify employees and track their comings and goings and other movements. This is especially important in restricted access areas, such as nuclear facilities and luggage sorting halls at airports, where physical access technology plays a crucial role. RFID implants in this context could play a significant role in national security.

HIMs can also provide an extra layer of banking security, whereby an ATM machine or a bank teller can authenticate the identity of a customer by using a RFID reader. As such, if the data stored on HIMs is secure, HIMs can help to prevent fraud and identify theft. Equally, PCs could come equipped with RFID readers which are then able to authenticate a user via his or her implant, adding yet another layer of security to Internet banking or e-commerce. Already, there are computers that come equipped with fingerprint biometric scanners and software.

HIMs could also be used in 'smart gun' technology. In April 2004, ADS announced a partnership with gun manufacturer FN Manufacturing to produce a prototype of a gun that can only be fired if operated by their owner identified with a RFID tag implanted in his or her hand.[551] The concept behind the prototype is that a RFID reader in the gun reads the HIM's unique identification number and sends a digital signal unlocking the trigger so it can be fired. If the person who handles the gun does not have a HIM or the RFID reader does not recognize a HIM's unique ID number, then the gun will remain locked.

Prisoners convicted of violent crimes could be implanted with RFID microchips to actively track their movements within prisons or with GPS implants to immediately locate them if they happen to escape prison. Parolees of violent crimes could also be implanted with RFID/GPS implants to either actively or passively track or monitor their movements and whereabouts, in order for a law enforcement agency to be immediately notified of an offenders' growing proximity to the stored addresses of the victims of their previous crimes.

HIMs implanted into convicted pedophiles/sex offenders could help to better keep track of their location or monitor their movements in real-time, regardless if they are

551 see "No Chip in Arm, No Shot From Gun" (Associated Press, 14 April 2004), available at: http://www.wired.com/science/discoveries/news/2004/04/63066

registered or not in compliance with Megan's Law.[552] An application called Offender Locator, for example, is available on the iPhone, which displays the names, addresses, faces and criminal records of registered sex offenders near the user's location in real-time via the iPhone's GPS capability.

The location information generated by HIMs, let alone smartphones, will surely be useful to the continued development of the Information Sharing Environment (ISE), which aims to combine or "fuse" information controlled by all levels of government, including information held by the private sector, for subsequent analysis in the fight against terrorism.[553] In fact, the Executive Summary of the Fusion Center Guidelines, developed by the Department of Justice, recommends at minimum the attainment of access to location information. Governmental access to location information maintained by the private sector is yet another example of the cooperation between the US Government and the private sector in collecting and storing data within the emerging security-industrial complex that Robert O'Harrow (2005) warns us about in *No Place to Hide*.

Finally, RFID technology, whereby tiny RFID microchips are covertly tagged (or even implanted) onto targeted individuals (terrorists), could also be potentially used to locate and track the targeted individuals for termination by way of UAVs. However, these RFID tags are far more advanced than the current RFID implants discussed here. These capabilities are reportedly being developed and demonstrated by the US military, as part of the GWOT, and are purportedly just one component of the classified "Clandestine Tagging, Tracking, and Locating" (CTTL) program.[554]

7.5 SECURITY RISKS AND DRAWBACKS

While HIMs offer a number of security benefits, even if most are currently hypothetical, many of the security risks and drawbacks of HIMs, and the associated technology of RFID and GPS, are serious and real. The security benefits of HIMs could be compromised, if these security risks and drawbacks are not dealt with accordingly.

---

552 Megan's Law is the name given to the laws in the US requiring law enforcement authorities to make information available to the public regarding registered sex offenders. At the Federal level, the Sexual Offender (Jacob Wetterling) Act of 1994 requires convicted child sex offenders or pedophiles to notify local law enforcement agencies of any change of address after being released from prison. This information is publicly available.

553 The 9/11 Commission Act focused on establishing the Homeland Security Department's fusion center program.

554 see Weinberger, Sharon. "What is Woodward's Secret Weapon in Iraq?" (Wired, 9 September 2008), available at: http://www.wired.com/dangerroom/2008/09/whats-the-milit/

As the Data Privacy and Integrity Advisory Committee of the Department of Homeland Security (DHS) affirmed, "[a]ttempts to improve speed and efficiency through using RFID to track individuals raise important privacy and information security issues".[555] The US GAO observed, with regards to RFID microchips embedded in passports (ePassports) and ID cards, in a report titled *Information Security: Radio Frequency Identification Technology in the Federal Government* [hereinafter called "GAO RFID Report"], that "[w]ithout effective security controls, data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users".[556] Moreover, in a staff report on RFID, the FTC points out, "security concerns are likely to arise in connection with interoperable tags, which can be read by different enterprises sharing information associated with those tags".[557]

IT security experts have been warning about the security risks of RFID tags for some time now, and even have demonstrated those risks. 'Ethical hacker' Chris Paget has famously demonstrated using a low-cost RFID reader that he could surreptitiously read and clone the EPC Generation 2 RFID tags embedded in US passport cards (not to be confused with US ePassports) and Enhanced Driver's Licenses. *The Hacker's Choice*, a group of international experts on computer security, provided an emulator applet for copying ePassports and demonstrated their considerable security loopholes.[558]

The VeriChip RFID implant is based on ISO 11784/85, the same international standard that regulates animal-implantable RFID microchips. However, ISO 11784/85 is not well-known for ensuring the security and integrity of the data held on the microchips. Identity theft via RFID implants is especially a grave (data) security concern.[559]

---

555 The Use of RFID for Human Identification: A Draft Report from DHS Emerging Applications and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee, Version 1.0, p. 3, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf
(This precise statement was removed from the final adopted version of the report)

556 Information Security: Radio Frequency Identification Technology in the Federal Government, The United States Government Accounting Office, May 2005, p. 19, available at: http://www.gao.gov/new.items/d05551.pdf

557 FTC staff report on RFID, p. 16.

558 see *The Hacker's Choice* explanation, available at: http://freeworld.thc.org/thc-epassport/

559 Identity theft is already the most significant consumer complaint. For instance, during 2009, identity theft was by far the number 1 consumer complaint, accounting for 21% of all consumer complaints in the US. see the 2009 Consumer Sentinel Network Data Book, Federal Trade Commission, February 2010.

As demonstrated by Annalee Newitz and Jonathan Westhues,[560] VeriChip's RFID implant, which have no adequate security features, can be 'cloned'.[561] Directions on how to do so were made available on the Internet.[562] Jonathan Westhues also explained on his website about another vulnerability of VeriChip's implant using another type of attack called a "replay attack", which refers to when an attacker replays an earlier transmitted unique identification number.[563] Researchers from John Hopkins University and RSA Laboratories also demonstrated that the data on an RFID tag can be stolen by reading the tag's signal, then 'cracking' the tag's encryption key and creating a 'clone' of the RFID tag. The tag used even had a 40-bit encryption key.[564] A group of doctors from the American Medical Informatics Association equally recognized that VeriChip's RFID implant is vulnerable to attacks.[565] Thus, RFID implants are currently vulnerable because the microchips can be cloned or spoofed, especially if the implant is based on inadequate standards.

The hosts of *Mythbusters,* a popular TV show produced by the Discovery Channel, wanted to demonstrate in an episode segment "how hackable, how reliable, how trackable" are RFID microchips. VISA, MasterCard and American Express, which all have a certain interest in using RFID for contactless payment, apparently pressured the Discovery Channel to refrain from airing this episode.[566] In the end, the show pursued a different topic during their episode on RFID.

Furthermore, a group of computer experts from Vrije Universiteit demonstrated that it is also possible to transmit a virus or malware software onto RFID tags, causing

---

560 Fulton, Nic. "High-tech cloning" (Reuters, 22 July 2006), available at: http://blogs.reuters.com/blog/2006/07/22/high-tech-cloning/

561 The act of 'cloning' a RFID tag, also known as 'spoofing', is similar to the way credit cards can be copied, known as 'skimming', whereby an account number and other data needed to clone a credit card is covertly copied. But, RFID tags do not need to be physically taken, in order to be copied.

562 see Jonathan Westhues' website, available at: http://cq.cx/verichip.pl

563 *Ibid.*

564 see Bono, Steve., et al. *Security analysis of a cryptographically-enabled RFID device*, USENIX Security Symposium Proceedings of the 14th conference on USENIX Security Symposium, Volume 14, 2005.

565 see Halamka, John., et al. The Security Implications of VeriChip Cloning (Journal of the American Medical Informatics Association, Volume 13, Issue 6, 2006), pp. 601-607.

566 see Leyden, John. "*Mythbusters* RFID episode axed after 'pressure' from credit card firms", The Register, 3 September 2008, available at: http://www.theregister.co.uk/2008/09/03/mythbusters_gagged/

unwanted actions to occur and jeopardizing the databases linked to the tags.[567] Any RFID system, which transmits information over the Internet, is equally subject to cyber attacks, and many of the same security dilemmas of RFID microchips are, accordingly, relevant to RFID implants. Therefore, RFID implants and the creation of an 'Internet of Persons' could add a new dimension to cybercrime or hi-tech crime, now one of the leading criminal activities, whereby human bodies themselves, as opposed to just computers, become the target of cybercriminals and vulnerable to a cyber attack. As a result, it is conceivable that HIMs and, therefore, human beings themselves, in a way, could be infected with a virus or malware software and that a computer virus pandemic caused by RFID implants is a possibility.[568] Indeed, Mark Gasson, a scientist at the University of Reading, became the first human to be infected with a computer virus by infecting his RFID implant. Gasson is also currently researching the potential risks associated with other electronic devices implanted into humans, in addition to RFID implants, such as cochlear implants and pacemakers.[569] Sandler et al. (2010) have equally raised their concerns over the security vulnerabilities of the software code of (wireless) implantable medical devices.[570]

The RFID microchips, however, are not the only vulnerability of the system. The middleware/software and associated databases are also subject to security risks. The Food and Drug Administration (FDA) cites, one of the potential risks associated with the VeriChip's RFID implant, are "compromised information security".[571] Although an implant's ID number is essentially just a number and basically inconsequential without additional access to the integrated database(s), there is the threat that a hacker or an unauthorized third party, other than the implantee or authorized data controller, could indeed gain access to the associated data. Therefore, another major security threat to the implantee is the potential for unauthorized access to his/her electronic health data,

---

567 Rieback, M.R., et al. *RFID Viruses and Worms* (Department of Computer Science, Vrije Universiteit Amsterdam, 2006), available at: http://www.rfidvirus.org

568 Interestingly, I wrote about this possibility at least a year before the news broke on unique Mark Gasson's research project.

569 see Palmer, Maija. "Scientist 'infects himself" with computer virus", (Financial Times, 26 May, 2010), available at: http://www.ft.com/cms/s/0/2e2f5ea4-68b5-11df-96f1-00144feab49a.html

570 Equally, any software-controlled, wireless medical device could be vulnerable.
see, e.g., Darlene, Storm. "Feds pressed to protect wireless medical devices from hackers" (ComputerWorld, 11 April 2012), available at: http://blogs.computerworld.com/20015/feds_pressed_to_protect_wireless_medical_devices_from_hackers?source=rss_blogs

571 Federal Register, Volume 69, Number 237, 10 December 2004, pp. 71702-71704.

location information or any other personal information associated with the HIM and stored on the multiple associated databases.

Other security concerns pertain to the contactless nature and non-direct line-of-sight capability of RFID technology. As a result, RFID normally operates unnoticeably, making it difficult if not impossible for people to know when they are being identified and/or tracked.[572] Without strong security standards, the information contained on HIMs can therefore be read without the implantee's knowledge or consent, leaving RFID implantees considerably deprived of the ability to control the information others may know about them.

With regards to the security drawbacks of prospective GPS implants, relying too much on GPS to track and monitor the movements of parolees of violent crimes and sex offenders could result in providing a false sense of security for society as a whole, as some have pointed out.[573] GPS tracking is certainly not a silver bullet for preventing crime, as was shown with the murder of 13-year-old Alycia Nipp by a sex offender who was under monitoring via a GPS bracelet.[574] But, this particular sex offender was under passive monitoring, as opposed to active monitoring. Nevertheless, the sex offender or parolee could simply become unconcerned that he is being monitored and commit another crime regardless.

Paradoxically, as easily as an implantee can be found by law enforcement agencies, if he or she were to be kidnapped or was to become lost, criminals could also intentionally locate an implantee. The availability of location information, for instance, could lead to a stalker somehow accessing that information, if adequate safeguards are not put in place. As the National Network to End Domestic Violence (NNEDV) warns, RFID can be used by abusers to track or stalk their victims.[575] The same is obviously true and even worse for GPS and just about any location-based service.

---

572 see The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

573 see McLaughlin, Eliott C. and Patrick Oppmann. "Sex offender kills teen while under GPS monitoring, police say" (CNN.com, 12 March 2009) available at: http://edition.cnn.com/2009/CRIME/03/12/sex.offender.gps/index.html

574 *Ibid.*

575 see a paper prepared by the NNEDV, available at: http://www.aclunc.org/issues/technology/asset_upload_file364_7757.pdf

7.6 SCOPE OF DEPLOYMENT

7.6.1 Actual deployment in the US

The research that led to the development of RFID occurred decades ago, however, the innovation steps that have translated the research and development into various marketable products and solutions, such as access control cards and identity cards, and services for supply chain management, is relatively recent. HIMs are just one of the latest innovation concepts developed using RFID technology.

HIMs are not theoretical or science fiction, they are real and here. The concerns over the deployment of HIMs are not premature. The deployment of HIMs is indeed spreading, however, just not as much as some proponents may like.

VeriChip's[576] previously publicly stated goals of implanting millions of Americans with their implantable RFID tags, has so far not been successful. As of 17 March 2008, 616 people have had VeriChip's RFID implant implanted.[577] But, this number is likely higher when including those who have been implanted outside the US. Moreover, this number does not include the number of people who have implanted an implantable RFID tag/microchip independent of VeriChip (see below for further explanation).

VeriChip had focused on targeting people with medical conditions, such as diabetes and Alzheimer's disease or dementia, and senior citizens. As part of a study on the VeriMed Patient Identification System, VeriChip implanted their RFID implants in 200 individuals suffering from Alzheimer's disease and other forms of dementia, as well as their caregivers.[578] A number of diabetics have also been implanted. In addition, VeriChip equipped a large bus as a mobile "chipping station", also known as the

---

[576] In 2009, VeriChip Corporation changed its name to PositiveID Corporation after completing its acquisition of Steel Vault Corporation. Throughout this dissertation, however, the company will still be known as VeriChip to avoid confusion. Nevertheless, the new company still markets their RFID implant (VeriChip), but has also now taken the "capabilities of RFID implantable microchips beyond simple identification" to create the "GlucoChip", which "combines an embedded bio-sensor system on an implanted RFID microchip". "One potential application of this bio-sensor system is an implantable, bio-sensing RFID microchip that measures glucose levels in the body in real time". Further information is available at: http://www.positiveidcorp.com/products_glucochip.html

[577] see VeriChip Corp.'s 10-K Annual Report for the fiscal year ended 31 December 2007, p. 13, available at: http://www.sec.gov/Archives/edgar/data/1347022/000136231008001657/c72788e10vk.htm

[578] see VeriChip Corp., Press Release, 22 February 2003, "VeriChip Corporation Partners with Alzheimer's Community Care to Conduct Study of VeriMed Patient Identification System", available at: http://www.verichipcorp.com/news/1172151146

"chip mobile".[579] As of 31 December 2007, more than 200 hospitals and other medical facilities have adopted the VeriMed Patient Identification System protocol in their emergency rooms and have become a part of the network.[580]

During the Hurricane Katrina disaster relief, US Disaster Mortuary Operational Response Team (DMORT) and health officials in Mississippi's Harrison County implanted RFID implants, donated by VeriChip, to speed up or facilitate the process of identifying corpses.[581] The system is now marketed as VeriTrace. In 2007, VeriChip reportedly managed to convince the State of Georgia to buy a package of the company's VeriTrace system which consisted of 500 RFID implants, 5 customized Ricoh 500SE digital cameras capable of receiving both RFID and GPS data wirelessly and adding geographical identification metadata (or GPS coordinates) to the image (known as geotagging), 5 VeriTrace Bluetooth handheld readers, and a web-enabled database. The system can identify, track and automatically record each implant's ID number along with the GPS coordinates captured by the Ricoh cameras embedded in the images, which enables the precise cataloging of all data and images related to human remains after a disaster.[582]

In February 2006, RFID implants were also infamously implanted in employees at CityWatcher.com, a company in Cincinnati, Ohio, with the help of Six Sigma Security, to establish an access control system at the company's secure data center.[583] Although it was not exactly a condition of employment, it would have been difficult for some employees to work there meaningfully without a HIM.

Nevertheless, the objective of privacy advocates to put VeriChip Corp. out of business might in fact one day materialize. VeriChip Corp.'s implant business has yet to generate a viable profit for the company (as of 2009), while the company's future is

---

579 see VeriChip's FAQ webpage, available at: http://www.verichipcorp.com/content/company/corporatefaq

580 see VeriChip Corp.'s 10-K Annual Report for the fiscal year ended 31 December 2007, p. 13, available at: http://www.sec.gov/Archives/edgar/data/1347022/000136231008001657/c72788e10vk.htm

581 see Kanellos, Michael. "RFID chips used to track dead after Katrina" (*CNET News*, 16 September 2005), available at: http://www.news.com/RFID-chips-used-to-track-dead-after-Katrina/2100-11390_3-5869708.html?tag=nw.2;
RFID implants were also implanted in the bodies of victims of the Tsunami in Thailand. see Meyer, H.J., et al. *Implantation of radio frequency identification device (RFID) microchip in disaster victim identification (DVI)*. (Forensic Science International, Volume 157, Issue 2, 2006), pp. 168-71.

582 see VeriChip Corp., Press Release, available at: http://www.businesswire.com/news/google/20070509005155/en

583 see "US group implants electronic tags in workers" (Financial Times, 12 February 2006), available at: http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html

still in doubt. But, the potential privacy threat of HIMs will persist, regardless of the existence of VeriChip Corp.

Although VeriChip Corp. is the only official or FDA approved provider of human implantable RFID tags, going through VeriChip Corp. is not the only way of getting a HIM implanted. VeriChip Corp. does not have a patent or monopoly on glass encapsulated RFID tags. There are a number of other glass encapsulated RFID tag manufacturers and distributors, such as Trovan, Destron Fearing (a subsidiary of Digital Angel[584]) and Philips. Only that these glass encapsulated RFID tags are not marketed, promoted or approved for human implantation, but rather for implantation in animals. Nonetheless, any small, glass encapsulated RFID tag could easily be bought and used for human implantation.

This is indeed what is actually occurring. These so-called "guerrilla taggers" are the latest pioneers of a "brave new world", having RFID implants implanted in the less conventional way. Amal Graafstra is one of the more well-known. He chose not to go through VeriChip because it uses a proprietary system and he also did not want to sign up for the global VeriChip subscriber registry. He has two RFID implants, one in each hand. His left hand contains a 3mm x 13mm EM4102 type glass RFID Ampoule tag that was implanted by a cosmetic surgeon. His right hand contains a 2mm x 12mm Philips HITAG 2048 S implant with crypto-security features and 255 bytes of read-write memory storage space. It was implanted by a family doctor using an Avid injector kit just like the ones used on pets. Graafstra's development is an example of user-driven innovation (UDI). He has developed the means to access his front door, car door, and log into his computer using his RFID implants, and has written a book called *RFID Toys*, which details how to develop these and other RFID-enabled projects. Explanations, pictures and videos can be downloaded from his website.[585] There are numerous other guerrilla taggers (perhaps hundreds) around the world who have also engaged in do-it-yourself RFID implantation. Nancy Nisbet, a Canadian artist, is another well-known guerrilla tagger. Of course, they are all copycats of Kevin Warwick, the renown Professor of Cybernetics at the University of Reading and author of *I Cyborg*,[586] who had a RFID chip implanted in 1998 (later removed) allowing him to automatically open doors

---

584 The current President and CEO of Digital Angel Corporation, Joseph J. Grillo, has extensive experience in identification and tracking technology. He was formerly the President and CEO of the Global Technologies Division of Assa Abloy, and before that managed the Identification Technology business unit of Assa Abloy. Before that, he was President of HID.

585 see Amal Graafstra's website, available at: http://amal.net/rfid.html

586 Warwick, Kevin. I *Cyborg* (Century, 2002).

and turn on lights, and four years later a micro electrode array surgically implanted into the median nerve fibers of his left arm allowing him to be connected to the Internet and control a robotic arm from afar.

The development of the GPS implant, on the other hand, is still most likely in its near final stages of development and miniaturization, according to ADS, which apparently had successfully tested a working prototype several years ago,[587] consistent with the company's previous public statements made repeatedly that it intended on developing a HIM with GPS tracking capabilities. ADS/Digital Angel, formerly the largest shareholder of VeriChip Corp., is the most notable company publicly involved in the R&D of GPS implants and acquired the rights to U.S. Patent No. 5,629,678 in 1999.[588] But, a GPS implant has yet to hit the consumer market, and ADS/Digital Angel has since removed this information from the Internet and altered its website and apparently its business plan.[589] A patent application for a GPS implant for animals was filed with the U.S. Patent Office.[590] The patent application cites the technology used in the GPS implant apparently developed by ADS/Digital Angel.[591] Nonetheless, it is perhaps not incredibly farfetched to assume that national intelligence agencies or secret government-funded research projects are or were also working to develop GPS implants or may have already done so. Though, there is no publicly available proof to this statement.

Nevertheless, the technology, however, is not really the obstacle to the widespread deployment of HIMs, whether RFID or GPS-based, and nor is the law for that matter. The difficulties VeriChip Corp. and ADS have faced, for instance, and the obstacles to the

---

587 see Applied Digital Solutions Inc., Press Release, 13 May 2003, "Applied Digital Solutions Announces Working Prototype of Subdermal GPS Personal Location Device", available at: http://findarticles.com/p/articles/mi_m0EIN/is_2003_May_13/ai_101629083

588 see Applied Digital Solutions, Inc., Press Release, 15 December 1999, "APPLIED DIGITAL SOLUTIONS ACQUIRES RIGHTS TO WORLD'S FIRST DIGITAL DEVICE - IMPLANTABLE IN HUMANS - WITH APPLICATIONS IN E-BUSINESS TO BUSINESS SECURITY, HEALTH CARE AND CRIMINAL JUSTICE" (retrieved through Internet Archive's Wayback Machine), available at: http://web.archive.org/web/20000511001424/www.digitalangel.net/pr_12_15_99.htm

589 This information, nonetheless, can also be retrieved through the use of Internet Archive's Wayback Machine. see, for instance, Digital Angel's website dated July 11, 2000, available at: http://web.archive.org/web/20000711033923/http://www.digitalangel.net/

590 see U.S. Patent Application No. 20090009388, filed by Carole A. Wangrud on 8 January 2009, which claims to be a system for monitoring and tracking the location of animals comprising of a GPS implant designed to be transplanted subcutaneously.

591 *Ibid.*, para. 0025.

widespread deployment of HIMs pertain rather to the uneasiness of the public towards HIMs. As VeriChip Corp. notes in its 2007 10-K report, privacy concerns and negative media coverage are significant risks to its business, acknowledging that people may not be willing to be implanted and that physicians may be reluctant to recommend the procedure.[592] Other obstacles include the fact that VeriChip's RFID implant costs around $200 and is not covered by private healthcare insurance companies or by Medicare/Medicaid.

The perception of the public towards HIMs and their effects might slowly change. We are already seeing the general acceptance of the deployment of numerous other tracking technologies, devices, applications and schemes, many of which have similar effects (see sections 7.3.6 and 7.7). HIMs are arguably just the next step.

7.6.2 Potential deployment

The potential greater (or perhaps widespread) deployment of HIMs is arguably not farfetched. On the basis that the implantation of HIMs is cheap and quick and that the technology is already in place, the futurist Matthew Sollenberger predicted in 2007 that "[t]here is at least a low probability of chipping becoming widespread within 10 years".[593] Wolfgang Grulke, a former IBM executive, winner of the prestigious IBM Outstanding Innovation Award and Chairman of FutureWorld International, has equally predicted that HIMs will be common in a decade or so. As a report of the consortium of the SWAMI project[594] agrees,

> [i]ndeed, it is not impossible to imagine a day when almost everyone will have implantable devices, not only for tracking their whereabouts, but also for monitoring their physiological condition. At the same time, there may be considerable social pressure, perhaps even legal requirements, for individuals to bear

---

592 see VeriChip Corp.'s 10-K Annual Report for the fiscal year ended 31 December 2007, pp. 34-35, available at: http://www.sec.gov/Archives/edgar/data/1347022/000136231008001657/c72788e10vk.htm

593 Sollenberger, Matthew. "Chipping People" (Social Technologies, 12 November 2007), available at: http://www.socialtechnologies.com/FileView.aspx?fileName=PressRelease11122007.pdf

594 The SWAMI (Safeguards in a World of Ambient Intelligence) project aimed to provide an overview of the key social, legal and ethical implications of ambient intelligence and highlight the privacy threats.

> such implants as a security measure. One could further foresee such implants interacting with the "intelligence"-embedded, networked environment too.[595]

More recently, in a roadmap on current and future trends, Richard Watson included as a possibility that by 2025-2035 all babies born will be implanted with GPS and ID chips.[596]

Kevin Haggerty, an expert on surveillance and Professor of Sociology, wrote an article in the Toronto Star explaining evocatively how this could develop in the US.[597] Haggerty describes a scenario whereby the Government starts off implanting stigmatized groups, such as pedophiles or sex offenders and criminals, and then suggests that illegal aliens and soldiers be implanted, until eventually a majority of Americans become implanted for one reason or another. As Haggerty asserts, it is "[b]est to contemplate these dystopian potentials before we proffer the tender forearms of our sons and daughters".[598]

In other words, there is a likelihood that the mandatory implantation of HIMs for sex offenders and parolees of violent crimes for public security purposes will not cause most people to speak up in protest. Then, the mandatory implantation of HIMs in soldiers for their safety will likely not cause uproar from private citizens. Then, the mandatory implantation of HIMs in employees at secure facilities, such as nuclear power plants, again for the sake of public security, will likely make sense to many people, especially those who do not work at these facilities. As the mandatory implantation progresses with additional justifications, more and more people will be implanted with a HIM until there are few categories of people leftover that do not meet the requirements for mandatory implantation.[599]

---

595 Friedewald, M., R. Lindner & D. Wright (eds.), "Policy Options to Counteract Threats and Vulnerabilities in Ambient Intelligence", SWAMI Deliverable D3: A report of the SWAMI consortium to the European Commission under contract 006507, June 2006, (Draft version), p. 37, available at: http://www.isi.fhg.de/publ/downloads/isi06b24/SWAMI_D3_030706.pdf

596 see Trends & Technology Timeline 2010+ , available at: http://nowandnext.com/PDF/trends_and_technology_timeline_2010.pdf

597 see Haggerty, Kevin. "One generation is all they need" (The Star, 10 December 2006), available at: http://www.thestar.com/sciencetech/article/136744

598 *Ibid*.

599 *Ibid.*

Therefore, the famous words of Friedrich Gustav Emil Martin Niemöller may be relevant here for the potential deployment of HIMs. In speeches and in a poem, referring to the Nazis, the German pastor and theologian famously states:

> In Germany, they first came for the communists, and I didn't speak up because I wasn't a communist. Then they came for the Jews, and I didn't speak up because I wasn't a Jew. Then they came for the trade unionists, and I didn't speak up because I wasn't a trade unionist. Then they came for the Catholics and I didn't speak up because I wasn't a Catholic. Then they came for me – and by that time there was nobody left to speak up.

If RFID does become the primary method of identification, human beings will then commonly be electronically identified for verification purposes. For reasons of homeland security, RFID tags are already being embedded in US passports, enhanced state driver's licenses and ID cards, and in the Western Hemisphere Travel Initiative (WHTI) cards. RFID implants are naturally the next step in electronic identification (eID). Dr. Richard Seelig, formerly VP for Medical Affairs at VeriChip, similarly advocated that RFID implants "could function as a theft-proof, counterfeit-proof ID, like having a driver's license embedded under your skin".[600] RFID implants could thus potentially serve as a significant component of a 'universal identification system', whether desirable or not.

In line with these plans perhaps, VeriChip acquired Steel Vault Corporation, a credit reporting and identity security service provider, to form a combined company called PositiveID. As VeriChip (now known as PositiveID) noted, in its quarterly 10-Q report, "[b]eginning in the fourth quarter of 2009, with the acquisition of Steel Vault, the Company intends to pursue its strategy to offer identification tools and technologies for consumers and businesses".[601] Perhaps, the acquisition of Steel Vault could also be linked to the possible long-term intention of linking HIMs to financial information or credit card data.

RFID implants could also replace ordinary keys or RFID security clearance badges/contactless cards as the means of opening doors or gaining access to secure areas. Already, for example, there was talk in Texas and in the US Congress on whether or not

---

600 Grossman, Lev. "Meet the Chipsons" (Time Magazine, 11 March 2002), available at: http://www.time.com/time/magazine/article/0,9171,1001972-2,00.html

601 Positive ID Corporation, Form 10-Q for the quarterly period ended September 30, 2009.

airport employees should be mandated to have a microchip implanted.[602] Employees themselves could essentially become their entrance or security pass. Since RFID is already used immensely in the form of contactless cards for physical access control at places of business, replacing RFID cards with RFID implants will not require a great deal of further investment. However, in addition to keeping track of employees' comings and goings for time registration, HIMs (like RFID-embedded access cards) could also keep track of their movements within the workplace or office space and not just when entering or exiting the building.

There have been escalating calls for HIMs to be implanted into convicted pedophiles/sex offenders, violent criminals and even into HIV carriers. For example, in Oklahoma legislators debated whether to authorize HIMs in prisoners convicted of violent crimes.[603] With the overcrowding of prisons in the US, particularly in California, and a nationwide prison population now at over two million and growing, GPS implants could be used to relieve overcrowded prisons and rising costs by freeing people accused of non-violent crimes or could even be used as an alternative to prison for certain non-violent crimes. In the US, like in the UK, electronic monitoring in the form of GPS bracelets has been commonly introduced as a condition of being granted bail, an early release or parole. There are already tens of thousands of electronically tracked offenders in the US.[604] GPS bracelets are essentially just one step behind GPS implants and, according to Steve Aninye, President of Omnilink Systems, "the [US] justice system is interested in an implantable [GPS] device".[605] RFID implants could also be implanted into prisoners convicted of violent crimes and still in prison, which is equally just one step ahead of the RFID bracelets, developed by Alanco Technologies, being worn by thousands of inmates within several prisons across the US.

HIMs could be implanted in immigrants when they enter the US and used to track their movements and to locate them once their work visa has expired. Scott R. Silverman, the Chief Executive Officer of VeriChip, and largest shareholder, similarly proposed implanting HIMs in immigrants and guest workers during an interview on

---

602 see a *KENS 5* Eyewitness News broadcast video on 14 May 2007 available on YouTube, at: http://www.youtube.com/watch?v=Keo2TR1Zouw

603 Talley, Tim. "House rejects microchip implants for violent criminals" (Associated Press, 25 May 2007), available at: http://www.examiner-enterprise.com/articles/2007/05/24/news/state/news440.txt

604 see Hunt, V. Daniel., Albert Puglia, and Mike Puglia. *RFID-A Guideline to Radio Frequency Identification* (Wiley, 2007), p. 81.

605 Cozzens, Tracy. "Implant Issues More than Skin Deep" (GPS World, 1 June 2006), available at: http://uc.gpsworld.com/gpsuc/article/articleDetail.jsp?id=364980

"Fox & Friends", a program on FoxNews, adding that "We [VeriChip] have talked to many people in Washington about using it...."[606] HIMs could also be used to track border crossings of US citizens. Already, RFID smart cards have been tested at the US-Mexico border and Washington State and the DHS are testing licenses with embedded RFID microchips.

RFID implants could be implanted in soldiers as a means of identifying their corpses, while GPS implants could monitor individual troop movements in a battlefield. GPS, after all, was apparently developed in the first place to monitor the movements of troops and equipment. VeriChip has already lobbied the Pentagon to replace military dog tags with HIMs,[607] and the RFID bracelets, developed by Precision Dynamics Corporation and Texas Instruments, have been deployed in Iraq to track the location and status of wounded soldiers.[608] In addition, police officers could also be required to have a RFID implant implanted in order to deploy 'smart guns', or a GPS implant in order to instantly determine the closest officer to dispatch to a crime scene.

HIMs could even be implanted in children in order to tackle poor attendance or tardiness and record the entering and exiting on school buses. As a pre-requisite to fully-fledged GPS implants, school buses could instead be fitted with GPS devices to enable parents to know the bus's current location by logging onto a secure website. There have already been calls for mandating that children wear RFID tags or to attach them to their school bags[609] and pilot programs to test the effectiveness of such schemes.[610]

There is even a potentially strong market for HIMs in sports, based on their capability for tracking the performance of athletes. Already, RFID tags were used in the 2007 Boston Marathon.[611]

---

606 "Verichip Injects Itself Into Immigration Debate" (Spy Chips, 18 May 2006), available at: http://www.spychips.com/press-releases/verichip-immigration.html

607 see Francis, David and Myers, Bill. "Company trying to get under soldiers' skin" (The Examiner, 21 August 2006), available at: http://www.examiner.com/a-232630~Company_trying_to_get_under_soldiers__skin.html

608 Precision Dynamics Corp., Press Release, 20 May 2003, available at: http://www.pdcorp.com/en-us/company/pr2003-pdc-rfid-navy-use.html

609 Leff, L. "Students ordered to wear tracking tags" (Associated Press, 9 February 2005), available at: http://www.msnbc.msn.com/id/6942751/

610 Gutierrez, David. "U.S. School District to Begin Microchipping Students" (Natural News, 16 June 2008), available at: http://www.naturalnews.com/023445.html

611 see O'Connor, Fred. "RFID helps the Boston Marathon run" (PC World, 9 April 2007), available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/04/09/AR2007040901011.html

The increase in web-based digital or electronic medical/health records or 'health IT', as part of the greater movement towards e-Health, may coincide with the increased implantation of HIMs, particularly if Medicare or private insurance companies cover the costs (Spivey, 2009). During the beginning of 2009, US President Barack Obama announced his plan to computerize the entire country's health records within five years.[612] Companies with a vested interest in the technology, such as Philips, and lobbying organizations, such as the Center for Health Transformation, are promoting RFID technology as the main component of electronic health records (EHR). RFID technology has already been significantly deployed within the healthcare sector in the US (Cannataci, 2011).

This would be consistent with the strong potential for RFID implants to become a carrier of the Unique Health Identifier (UHID), as Spivey (2009) asserts.[613] The UHID is a number composed of 28 numeric digits, which will eventually serve to facilitate the nationwide electronic availability of personally identifiable health/medical information.[614]

The American Recovery and Reinvestment Act of 2009 allocated the billions of dollars needed to bring about the widespread digitization of medical records.[615] The bill also extensively provides the necessary provisions for EHRs and sets a goal for the creation and utilization of an EHR for each US citizen by 2014,[616] i.e. within five years, as President Obama earlier announced. Of course, (web-based) EHRs present additional data security and serious privacy concerns for personal health data that this dissertation will not go into.

RFID implants and associated web-based databases, such as those of VeriChip, fit in perfectly with the American Recovery and Reinvestment Act's definition of "health information technology" as the "hardware, software, integrated technologies or related

---

612 see Goldman, David. "Obama's big idea: Digital health records" (CNN, 12 January, 2009), available at: http://money.cnn.com/2009/01/12/technology/stimulus_health_care/index.htm

613 see Spivey, Crystal. *Breathing New Life Into HIPAA's UHID – Is The FDA's Green Light To The VeriChip™ The Prince Charming Sleeping Beauty Has Been Waiting For?* (9 DePaul Journal of Health Care Law, 2005-06), pp. 1317-1342.

614 Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
However, as widely recognized among privacy law experts, the problem is that the Health Insurance Portability and Accountability Act 1996 (HIPAA), the federal medical privacy bill, does not cover web-based medical records.

615 Incorporating new and unrelated legislation into spending bills is not unheard of. For example, the Real ID Act 2005 was astonishingly attached to a spending bill. See Division B of H.R.1268, An act making Emergency Supplemental Appropriations for Defense, the Global War on Terror, and Tsunami Relief, for the fiscal year ending September 30, 2005.

616 American Recovery and Reinvestment Act of 2009, Sec. 3001, (3)(A)(ii).

licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by healthcare entities or patients for the electronic creation, maintenance, access, or exchange of health information".[617]

Already, manufacturers of implantable medical devices sold in the US are required by the Food and Drug Administration Amendments Act of 2007 to ensure that implantable medical devices are identifiable and trackable via a 'unique device identifier' (UDI). RFID technology is increasingly being used to electronically track medical devices. An implantable medical device with an embedded RFID microchip could potentially have similar identification and tracking capabilities to RFID implants.

Perhaps, the next step would be for the US Government to request health insurance providers to cover the costs of the RFID implant procedure. Medicare could also eventually cover the costs. In 2008, the American Medical Directors Association (AMDA) initiated a clinical study to evaluate whether VeriChip's VeriMed Patient Identification System can improve patient outcomes. The study is meant to involve up to 10 facilities and 100 participants. Upon completion of the study, VeriChip intends to use the results to seek reimbursement approval from insurance companies and the Centers for Medicare & Medicaid Services.[618]

A hospital in New Jersey (US) and the major health insurance provider Horizon Blue Cross Blue Shield began recruiting volunteers in 2006 to have a RFID implant implanted in a two-year trial to determine if the implants reduce healthcare costs.[619] Already, US President Obama has advocated that EHRs could create jobs and reduce healthcare costs in the long-term. As a result, there is perhaps a possibility that RFID implants could become more common, if they are viewed as a means of reducing healthcare costs in conjunction with EHRs.

Moreover, VeriChip, the exclusive provider of RFID implants authorized for human implantation, announced that it has obtained exclusive licenses for two additional patents, which will help the company to develop implantable virus detection systems in humans. The patents, held by VeriChip partner Receptors LLC, relate to biosensors that can detect the H1N1 virus and other viruses, and biological threats. The technology will reportedly combine with VeriChip's RFID implant technology to develop a 'triage detection system'.

---

617 *Ibid.*, Sec. 3000 (5).

618 see VeriChip Corp., Press Release, available at: http://www.reuters.com/article/pressRelease/idUS137195+08-Jan-2008+BW20080108

619 see M.L. Baker. "Insurers Study Implanting RFID Chips in Patients", *eWeek.com*, 19 July 2006, available at: http://www.eweek.com/c/a/Health-Care-IT/Insurers-Study-Implanting-RFID-Chips-in-Patients/

While the ongoing economic crisis and existing health legislation is ripe for RFID implants, even global warming (or climate change), can be used as an excuse to track the movements of people and generate a carbon footprint report or 'green report card' for each and every person.[620] This can already be done with GPS-equipped smartphones using the application *Ecorio*, which uses GPS to track every movement and uses the data to generate a personalized carbon footprint report,[621] or via GPS devices in vehicles to levy a road tax by kilometer/mile, which was proposed in the Netherlands. Although this report would be incomplete, governments could one day perhaps use this information to tax each person according to the results of their report or to monitor the use of their personal 'carbon allowance'.[622]

For now, HIMs are implanted voluntarily. Under the National Animal Identification System (NAIS), RFID ear tags or injectable RFID tags are being used to identify and track millions of livestock animals to enable the US Government to respond quickly to disease. The animals are each identified by a 15-digit Animal Identification Number (AIN). Some critics of the plan have already voiced their concerns that animals could be the forerunner of a similar system for humans.[623] There is, however, no evidence that there are plans for HIMs to be mandated for individuals.

On the other hand, as Ramesh (1997) argues, "[a] national identification system via microchip implants could be achieved in two stages. Upon introduction as a voluntary system, the microchip implantation will appear to be palatable. After there is a familiarity with the procedure and knowledge of its benefits, implantation would be mandatory".[624] Indeed, history has demonstrated that something voluntary today can become mandatory tomorrow, or at least indirectly mandatory, since its possession could later become necessary to carry out ordinary daily activities. This is already the case today with ID cards in the US, and the same may potentially also prove true for

---

620 see Ecorio, available at: http://www.ecorio.org

621 This concept is gaining traction. During the post-i2010 Public Hearing on "Priorities for a new strategy for European Information Society" held 23 September 2009 in Brussels, a representative from the mobile phone carrier Orange expressed interest in the potential of mobile phones to be used to collect data.

622 The idea for personal 'carbon allowances' for individuals was proposed by the Chairman of the UK's Environment Agency, Lord Smith.

623 see Gumpert, David E. "Animal Tags for People?" (Business Week, 11 January 2007), available at: http://www.businessweek.com/smallbiz/content/jan2007/sb20070111_186325.htm?chan=smallbiz_smallbiz+index+page_today's+top+stories

624 Ramesh, Elaine M. Time Enough? Consequences of Human Microchip Implantation, Franklin Pierce Law Center (1997), available at: http://www.fplc.edu/risk/vol8/fall/ramesh.htm.

HIMs. Moreover, once the coerced implantation of HIMs in parolees and in convicted pedophiles or other convicted criminals is put into effect and the public accepts the potential security benefits, other coerced implantations could similarly materialize.

However, HIMs do not necessarily have to be something that governments enforce upon us. Mandatory implantation may not be required as consumers begin to want HIMs anyhow or are enticed to want one on the basis of security, personal safety, consumer and medical benefits. The ongoing proliferation of tracking technologies and of LBS on smartphones implies that consumers already accept location-aware applications and the amenities that location-awareness provides. If many people are already willingly, some quite enthusiastically, to broadcast their location, it is likely that these people will begin to accept or even desire RFID or GPS implants, particularly as digital inclusion (or e-Inclusion) increasingly becomes a means of social inclusion, or as digital exclusion (e-Exclusion) more and more translates into social exclusion.

HIMs could even become a status symbol or made to look fashionable, with the increasing array of hypothetical scenarios depicted in popular culture to familiarize society with HIMs and to condition or program people's acceptance through mainstream media and commercials.[625] As Aarts and de Ruyter (2009) question "how long will it be before we accept the implantation of chips for non-medical reasons?" Further adding, "[a]ttitudes to the body are already changing. Body piercing, tattoos and cosmetic surgery are much more common than a generation ago" (2009, p. 12).

Still, fear, above all else, and not the lure of fashion or the satisfaction of a desire, nor the struggle for efficiency or progress, will likely be the main catalyst for HIMs. Just like other tragic disasters and crises have led to negative effects on freedom and privacy, the threat of terrorism, the ever-increasing crime rate and apparently worsening global environmental crisis could lead to further tracking of people's movements.

---

[625] There are numerous examples in mainstream media. The relevant clips that depict HIMs can be found on YouTube. In the film, *Casino Royal* (2006), the British spy James Bond 007, and in the film, *Demolition Man*, the character John Spartan are both implanted with a microchip in order to track their movements. In the television series *Heroes* (Series 3, Episode 14), one of the characters is even implanted with a "GPS implant". In the BBC drama *The Last Enemy* (2008), a plot to implant everyone with a RFID tag is revealed. RFID implants are remarkably described as an "ID that can't be lost, forged or stolen…Its content and function can be adapted to suit my needs. It can be my credit card. It can be door key, my car keys. I'll never lose them again. Eventually it will become universal. Starting at school age, a tag for life". In *CSI Miami* (episode 305), a murdered teenager's VeriChip is removed and scanned to reveal her associated information on a computer screen, which later helps in the investigation. In *Mission: Impossible 2* (2000) a transponder chip is implanted into a main character. More recently, in the film *Hunger Games*, children are implanted with microchips to track their movements. In an IBM televised commercial several years ago on e-Business of the future, a supermarket shopper is shown stuffing RFID-tagged items under his coat and then automatically paying for the items by simply walking through a RFID gateway and without using a credit/debit card or mobile phone, which likely implies he had a RFID implant.

Fear of global warming, fear of a terrorist attack, fear of being kidnapped or murdered and the fear of one's child either being kidnapped or sexually offended are just a few examples. HIMs could slowly just become as ordinary as having an ID number or an RFID-embedded ID card or wearing clothing or carrying items with embedded RFID tags or carrying around GPS-equipped smartphones – all of which exist today.

Nonetheless, any widespread deployment and realization of the diverse practical applications of RFID will require not just interoperability and the necessary infrastructure, but also additional available space in the radio spectrum for the transmission of data over longer distances. This could be accommodated for through the complete switchover from analog to digital TV, which is occurring in the US and gradually in the EU.

7.6.3 Actual and potential international deployment

Kevin Haggerty also foresees that the escalation of HIMs will start in countries at the periphery of the Western world.[626] Remarkably, his prediction is already gaining traction.

In the Indonesian province of Papua, it was reported that carriers of HIV are to be implanted with microchips under a bill backed by the provincial parliament to track and punish anyone who deliberately infects others.[627] In Mexico, the country's Attorney General (former), Rafael Macedo, and members of his staff were reportedly implanted with RFID implants as a means of controlling access to a sensitive records room. Other people in Mexico are getting HIMs implanted, like the one developed by Xega, to counter the threat of being kidnapped. In addition, the Congressional Record shows that Colombian President Álvaro Uribe told (former) US Senator Arlen Specter (D-Pa) "he would consider having Colombian workers have microchips implanted into their bodies before they are permitted to enter the United States to work on a seasonal basis".[628]

HIMs are also slowly spreading beyond America's borders into the Western world. In Barcelona, Spain and in Rotterdam, the Netherlands, the Baja Beach nightclubs infamously began to implant HIMs in those wanting to jump entrance lines, open doors to VIP lounges and pay for drinks without cash or debit/credit cards. However, much of this is just a publicity stunt of the nightclub's owner. The parents of Danielle Duval,

---

626 Haggerty, Kevin. "One generation is all they need" (The Star, 10 December 2006) available at: http://www.thestar.com/sciencetech/article/136744

627 see "Indonesian AIDS patients face microchip monitoring" (Associated Press, 24 November 2008), available at: http://www.guardian.co.uk/world/2008/nov/24/indonesia-aids

628 Trip to Colombia, Peru, Brazil and Dominican Republic, U.S. Senate, 25 April 2006, p. S3495.

an 11 year-old girl, reportedly took the extraordinary step of having their daughter implanted with a transponder microchip so that her movements could be traced if she were to be abducted. They decided to do so after the abduction and murder of the schoolgirls Holly Wells and Jessica Chapman.[629] The issue came up again in the wake of the disappearance of the British child Madeleine McCann in Portugal. The Times published an article asking whether children should be implanted.[630] Even more controversial, a leaked British policy review document revealed that the British Government even considered implanting RFID implants in the mentally ill.[631]

7.7 ALTERNATIVES TO HIMs

There are indeed alternative systems and/or devices to RFID and GPS implants on the market or in development that can fulfill, to a certain degree, the same goals.

Direct competition for VeriChip's human-implantable RFID tags for medical purposes include the non-RFID, low-tech alternative of MedicAlert's jewelry bracelets that are engraved with the wearer's primary medical conditions and an ID number. However, MedicAlert's bracelet is not linked to hospital databases and can easily be removed. Another potential alternative is "medical tattoos", which can include basic information on a person's chronic diseases or allergies. Other non-RFID alternatives for medical purposes include: smart chip cards, which can be used to both access the medical history of patients at hospitals and store medical history; the CARE Memory Band, which can be connected to a computer by medical personnel to access medical data stored on the wrist bracelet; and simple bar-code wristbands. However, since RFID is a type of 'over-the-air' technology it does not require direct line-of-sight and can be read through non-metallic materials, unlike bar codes. RFID microchips also have a larger memory storage capacity than bar codes. The advantages of RFID tags have led to the belief that they will eventually replace bar codes in general, but this has yet to happen.

SmartWear Technologies produces wearable RFID devices that can equally be used to provide medical information to paramedics. Other RFID alternatives for medical

---

629 Wilson, Jamie. "Girl to get tracker implant to ease parents' fears" (The Guardian, 3 September), available at: http://www.guardian.co.uk/uk/2002/sep/03/schools.childprotection2

630 Midgley, Carol. "Would an implanted chip help to keep my child safe?" (Times Online, 15 May 2007), available at: http://women.timesonline.co.uk/tol/life_and_style/women/families/article1788169.ece

631 Jones, George. "Microchips for mentally ill planned in shake-up" (The Telegraph, 18 January 2007), available at: http://www.telegraph.co.uk/news/uknews/1539716/Microchips-for-mentally-ill-planned-in-shake-up.html

purposes include Precision Dynamics Corp.'s Smart Band RFID wristbands and GenTag's RFID wireless skin patches, which can be used to identify patients and capture and verify data before delivering medication or conducting surgery. However, both the Smart Band and GenTag's RFID wireless skin patches are designed for use after being admitted within hospitals and are disposable. The Smart Band is also marketed for use as a means of cashless purchases, keyless hotel entry and access control, while GenTag also markets its RFID wireless skin patches for use in entrance control, child ID and location tracking at amusement parks and for cashless payment transactions at hotels and casinos. Ident Technologies has developed a system named Skinplex®, which is composed of small signal generators worn closely on the body that transmit coded data to one or more receivers to identify and/or track the person concerned.

The TSI PRISM system, developed by Alanco Technologies, Inc. for use in correctional facilities, uses a RFID-enabled wrist bracelet to monitor the location of prison inmates in real-time.[632] To track children's movements while in the park, Legoland in Denmark uses a combination of RFID tags in bracelets and Wi-Fi.[633]

Once again, instead of implanting RFID microchips into the human body for identification purposes, the microchips can instead be embedded in ID cards or state driver's licenses, a method, which is currently being piloted in the US.

Alternatives to GPS implants, include GPS bracelets developed by Pro Tech or the GPS bracelets developed by Omnilink Systems that are combined with cellular technology. GPS bracelets are already being attached to parolees and sex offenders to create "mobile exclusion zones".[634] RemoteMDx Inc. delivers a similar monitoring system to keep track of offenders no matter where they may be. Also on the market include Fujitsu's Tag Locator V2, which uses GPS to detect its location and RFID to send that data along with its unique ID number to a reader, and Lego-James, a multi-faceted bracelet that allows parents to track the location of their children through 3G technology and the use of a GPS receiver. BlackBox GPS' personal locators, which resemble a pager, allows users to know where the wearer is located at all times anywhere in the world.[635] TRACKiT is a similar GPS device and service that locates the object or person

---

632 TSI Prism, at http://www.tsiprism.com; see Sofge, Erik. "High-Tech Lockup: Inside 4 Next-Gen Prison Security Systems" (PopularMechanics, 12 February 2008), available at: http://www.popularmechanics.com/technology/military_law/4248844.html?page=2

633 Collins, Jonathan. "Lost and Found in Legoland" (RFID Journal, 28 April 2004), available at: http://www.rfidjournal.com/article/view/921/1/1

634 Omnilink, at http://www.omnilinksystems.com/solutions_domestic_violence_monitoring.php

635 BlackBox GPS, available at: http://www.blackboxgps.com/cms/

the device is attached to and enables the user(s) to view the location on the Internet and receive sends text messages or emails if the tracked object or person ventures outside an invisible, customizable perimeter, also known as a 'geo-fence'. XACT|TRAX and the Little Buddy Child Tracker are other similar devices. Lok8u produces Num8, an inexpensive device, which resembles a wristwatch, that can be used by parents to locate and track their children at all times via the Internet and via text messages on a cell phone. GTX Corp. has developed a "GPS smart shoe", which has an embedded GPS chip and enables the wearer to view their location data in real-time on a Google map via a smartphone or PDA. Other less popular or less likely alternatives to GPS implants include wearable computers such as Eurotech's Zypad WL 1000, which is a wrist-worn touch screen computer with GPS and Wi-Fi connectivity.

Alternatives for implantable military dog tags include the Defense Advanced Research Projects Agency's (DARPA) personal radio beacons, which are worn on the soldier's uniform and can provide location data without the use of GPS, and Thales' MILTRAK, which is a device similar to a cell phone and also capable of transmitting and receiving location data.

However, none of these alternatives entirely possess the benefits and attributes of a HIM. The fact that HIMs essentially cannot be easily lost, removed or tampered with is what might make them more appealing to parents, corporations, the medical industry and governments. HIMs are everlasting, convenient and cannot be forgotten. For consumers, HIMs could be appealing because they are not uncomfortable to wear.

7.8 LAWS, CODES, DECISIONS AND OTHER LEGAL/POLICY INSTRUMENTS OF SPECIAL RELEVANCE IN THE US

7.8.1 Constitutionally protected rights

The Fourth Amendment of the US Constitution, which protects individuals from "unreasonable searches and seizures", conducted by the US Government and serves as the basis of the right to privacy in the US, reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment is invoked when the US Government infringes upon a person's 'reasonable expectation' of privacy.

Also relevant is the Fifth Amendment, which states that no individual "shall be compelled in any criminal case to be a witness against himself". In other words, individuals cannot forcibly incriminate themselves. However, only written or spoken words are considered self-incriminating and covered by the Fifth Amendment, while elements, such as blood samples or DNA samples, are not. In Schmerber v. California, for example, a case concerning whether or not blood forcibly withdrawn from Armando Schmerber while in hospital recovering from a traffic accident could be used to prove intoxication, the US Supreme Court affirmed, "blood test evidence, although an incriminating product of compulsion, was neither petitioner's testimony nor evidence relating to some communicative act or writing by the petitioner, it was not inadmissible on privilege grounds".[636]

7.8.2 Federal statutory laws

Telecommunication companies have the capacity to collect vast amounts of information on their customers when they use a telecommunication service. The Telecommunications Act of 1996 (hereinafter called the "Telecom Act") terms this information Customer Proprietary Network Information (CPNI) and regulates when and how telecom companies may use and disclose CPNI to third parties.[637]

The Federal Communications Commission (FCC) adopted formal rules, later codified in Federal regulations, requiring cell phones to be location-capable and wireless service providers to develop the capability for providing precise location information of wireless emergency callers, known as Enhanced 911 (E911) capabilities.[638]

Accordingly, the definition of CPNI[639] was amended by the Wireless Communications and Public Safety Act of 1999[640] to include "location" and subsection (f) was added to Section 222 of Title 47 U.S.C. Chapter 5, Subchapter II, Part I, explicitly

---

636 *Schmerber v. California*, 384 U.S. 757, 765 (1966).

637 see Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 222.

638 see Title 47 C.F.R. Ch. I, § 20.18.

639 see Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 222 (h)(1)(A).

640 Public Law 106-81, 113 Stat. 1286 (1999).

mandating, with certain exceptions, that "express prior authorization of the customer" is required to disclose, use or access call location information.[641]

The growing use of mobile phones, or other wireless/digital communication technologies, also brought about the need for new legislation to ensure that the use of pen registers and trap and trace devices by law enforcement agencies is still effective, in order to preserve their ability to intercept communications and obtain "call-identifying information". The Communications Assistance for Law Enforcement Act of 1994 (CALEA)[642] provides that telecommunications carriers and manufacturers of telecommunications equipment ensure their equipment, facilities, and services are capable of being used by law enforcement for surveillance purposes.[643] However, as CALEA specifies, "call-identifying information shall not include any information that may disclose the physical location of the subscriber" when "acquired solely pursuant to the authority for pen registers and trap and trace devices".[644]

The Electronic Communications Privacy Act 1986 (ECPA) regulates government access to private/stored electronic communications.[645] Government entities require a court order for access, which may be issued if the government entity "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation".[646]

With regards to the laws specifically relevant to RFID implants, the US Congress is paving the way forward for a national ID card embedded with an RFID microchip. The REAL ID Act of 2005 mandates that all state driver's licenses and ID cards conform to certain standards.[647] While ID cards are voluntary in the US, they are nonetheless required for a wide variety of everyday purposes. Although the REAL ID Act does not specifically require that driver's licenses contain RFID, the REAL ID Act mandates that

---

641 Exceptions to this rule include, for example, when there is a need to provide the location information of the caller to a public safety answering point, emergency medical service provider, public safety, fire service, or law enforcement official, etc., in order to respond to the caller's emergency. see Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 222(d)(4)(A).

642 Public Law No. 103-414, 108 Stat. 4279.

643 Title 47 U.S.C. Chapter 9, Subchapter I, § 1002 (a).

644 *Ibid.*, § 1002 (2) (B).

645 Public Law No. 99-508, 100 Stat. 1848 (1986).

646 Title 18 U.S.C Part I, Chapter 121 § 2703(d).

647 see Real ID Act of 2005, Public Law No. 109-13, § 201-207.

all state driver's licenses and ID cards include machine-readable technology, among other requirements, and gives the Secretary of Homeland Security the authority to do so.[648] RFID is a type of machine-readable technology and, as already mentioned, RFID microchips are indeed being embedded in state driver's licenses and in US passports.[649] However, few US states have implemented the REAL ID Act and even a number of US states have passed legislation rejecting the REAL ID Act. Since then, S. 1261, titled "Providing for Additional Security in States' Identification Act of 2009" or the "Pass ID Act", which is similar to the REAL ID Act, was proposed in the US Senate, possibly to replace the failed attempt by the REAL ID Act.

The Identity Theft and Assumption Deterrence Act of 1998 criminalizes the intentional transfer, possession or use, without lawful authority, a "means of identification" of another person. A means of identification may include, in addition to any name, social security number, etc., a unique electronic identification number.[650] Therefore, regardless whether or not a RFID implant is linked to personally identifiable information, the unique ID number of a RFID implant alone should qualify as personal identifiable information under US statutory law, since it legally constitutes a means of identification.

The printout of location information, generated by both GPS and RFID implants, could be considered originals and thus admissible as evidence in a court of law. As the Federal Rules of Legal Evidence confirms:

> An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".[651]

Once again, however, wrongfully obtained evidence, in violation of the Fourth Amendment, may be excluded from criminal proceedings in a court of law,[652] known as the "exclusionary rule". As Rule 402 states:

> All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other

---

[648] *Ibid*. § 205(a).

[649] RFID tags are also being embedded in passports around the world, notably in EU Member States, to comply with US demands and international standards.

[650] see Public Law No. 105-318, 112 Stat. 3007, codified at Title 18, U.S.C. Part I, Chapter 47, § 1028 (d)(7).

[651] Federal Rules of Legal Evidence, Article X, Rule 1001(3).

[652] see *Weeks v. United States,* 232 U.S. 383 (1914); Mapp v. Ohio, 367 U.S. 643, 655 (1961).

rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible.

7.8.3 Tort law

Tort law is relevant for the private use of the location information generated by HIMs. There are four invasion of privacy torts, of which one or more are recognized by courts in practically all states in the US, albeit to some extent and sometimes tentatively (McClurg, 1995). The Restatement (Second) of Torts reads:

> (1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
> (2) The right of privacy is invaded by:
> (a) unreasonable intrusion upon the seclusion of another, as stated in 652B; or
> (b) appropriation of the other's name or likeness, as stated in 652C; or
> (c) unreasonable publicity given to the other's private life, as stated in 652D; or
> (d) publicity that unreasonably places the other in a false light before the public, as stated in 652E.[653]

The most potentially relevant of the four torts for the unauthorized collection and disclosure of location information is the tort of "unreasonable intrusion upon the seclusion of another" (McClurg, 1995), which is defined as:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[654]

7.8.4 Case law

There is judicial precedent in the US regarding the use of tracking (or location-detecting) devices by law enforcement agencies, which is relevant to the tracking capabilities of both GPS and RFID implants.

---

653 Restatement (Second) of Torts, § 652A (1977).

654 *Ibid.,* § 652B.

In *United States v. Knotts*, law enforcement agents placed a RF tracking device on a chloroform bottle that one of the defendants purchased and then followed him to what was later suspected to be a drug laboratory. The US Supreme Court held that the driver in his automobile had "no reasonable expectation of privacy in his movements from one place to another" while in public.[655] The US Supreme Court also held:

> The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of [Darryl] Petschen's automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.[656]

Around a year later, in *United States v. Karo*, the US Supreme Court held that no showing of evidence or probable cause is required to observe information conveyed in areas observable to the public.[657] Similarly, in *Oliver v. United States,* the US Supreme Court also held that there is no reasonable expectation of privacy in 'open fields'.[658] Nevertheless, while *United States v. Karo* reaffirmed that an individual has no reasonable expectation of privacy of his movements in public, the US Supreme Court recognized that Fourth Amendment protections are applicable when the RF device moves out of a public place and into a private space.[659]

Moreover, in *Katz v. United States*, the US Supreme Court earlier on held that whatever a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected"[660] (emphasis added), as long as the person concerned exhibits first "an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable".[661] This is commonly known as the *Katz* test.

---

655 *United States v. Knotts*, 460 U.S. 276, 281 (1983).

656 *Ibid.*, at 282.

657 see *United States v. Karo*, 468 U.S. 705 (1984).

658 see *Oliver v. United States*, 466 U.S. 170 (1984).

659 see 468 U.S., at 714.

660 *Katz v. United States*, 389 U.S. 347, 351 (1967).

661 *Ibid.*, at 361. Concurring opinion of Justice Harlan.

In *Kyllo v. United States*, the US Supreme Court infuses into the interpretation of the Fourth Amendment the notion that law enforcement does not engage in a search under the Fourth Amendment when it uses a technology or device that is in general public use.[662] However, more recently, in *United States v. Jones,* the US Supreme Court ruled that the installation and use of a GPS tracking device to monitor vehicle movements constitutes a search under the Fourth Amendment.

With regards to the legality of forced implantation, case law in the US has long recognized that individuals have the right to physically or bodily integrity and the protection from bodily intrusions. As Justice Cardozo asserts, "[e]very human being of adult years and sound mind has a right to determine what shall be done with his own body".[663] There are certain exceptions in light of the needs of society. For example, mandatory random drug tests for certain lines of work have been upheld. In *Skinner v. Railway Labor Executives Association*, the US Supreme Court ruled that drug and alcohol testing of railroad employees, engaged in tasks that pose a threat to public safety if errors are to occur, was justified,[664] and, in *National Treasury Employees Union v. Von Raab*, the US Supreme Court held that random drug testing of employees who carry firearms is equally justified.[665]

With regards to the right to refuse to be identified, in *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*, the US Supreme Court upheld that individuals are not permitted to refuse to identify themselves to a law enforcement officer during the conduct of an investigation.[666]

---

662 *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

663 *Schloendorff v. Society of the N.Y. Hosp*., 211 N.Y. 125, 129 (1914).

664 *Skinner v. Railway Labor Executives Association*, 489 U.S. 602 (1989)

665 *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989)

666 *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*, 542 U.S. 177 (2004).

7.8.5 State statutory laws

Although there are no federal statutory laws pertaining to HIMs, there are a number of relevant state legislative acts that have been signed into law. For example, North Dakota Senate Bill 2415 (2007) prohibits anyone from requiring another person to have a HIM implanted. Wisconsin has a similar law, which requires that "[n]o person may require an individual to undergo the implanting of a microchip".[667] California Senate Bill 362 provides that no person may "require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device".[668] Washington criminalized the unauthorized reading of an RFID identification device "for the purpose of fraud, identity theft, or for any other illegal purpose" as a class C felony".[669] In Pennsylvania, H.B. 2374 prohibits anyone from requiring another person to undergo the subcutaneous implanting of an identification device. The bill passed Pennsylvania's House of Representatives. Other state legislatures have also passed legislation prohibiting the involuntary implantation of HIMs. It is important, however, to point out here that these state laws have not banned HIMs, but have rather prohibited their forced implantation. A number of other states have introduced legislation relating to the use of RFID, but most address the use of RFID tags/microchips embedded in retail products.

Some legislative proposals pertaining to the use of RFID for tracking purposes have also failed to become law. In Rhode Island, H.B. 5929, which attempted to prohibit the state's Government from tracking the movement or identity of an employee, student or client as a condition of obtaining a benefit or services, actually made it to the state governor's desk, but was strangely vetoed. The Identity Information Protection Act of 2005, among other security and privacy guarantees, attempted to make it a crime in California to "skim" (i.e. to scan in an unauthorized manner) an individual's RFID-enabled identification document in order to obtain personal data without the knowledge of that individual.[670] However, this balanced and thoughtful bill was vetoed.[671]

---

667 see Wisconsin Statute 146.25.

668 see California Civil Code, Section 52.7 (a).

669 see Title 19, Chapter 19.300, § 19.300.020.

670 California Senate Bill 768.

671 The (former) Governor of California, Arnold Schwarzenegger, explained that he vetoed the legislation because it "may inhibit various state agencies from procuring technology that could enhance and streamline operations, reduce expenses and improve customer service to the public and may unnecessarily restrict state agencies" and "may unduly burden the numerous beneficial new applications of contactless technology". see A Letter from the Governor of California to Members of the California State Senate, available at: http://gov.ca.gov/pdf/press/sb_768_veto.pdf

A second attempt[672] was also vetoed, but finally California Senate Bill 31 (2007) was signed into law, which makes skimming of RFID-enabled identification documents a crime punishable with imprisonment. In Maryland, H.B. 1401, which aimed to prohibit an employer from requiring or compelling an employee to undergo the subcutaneous implantation of a RFID tag, was not even put to a vote.

Existing laws, which address stalking and cyberstalking or electronic stalking, could be relevant to the tracking capabilities of HIMs. All 50 states, the District of Columbia and the US Government have enacted various laws making the act of stalking a felony (Miller, 2001, p. 36). Federal law is applicable in inter-state stalking.[673] Cyberstalking or electronic stalking is essentially the use of the Internet or a telecommunications or electronic communications device to threaten, harass or annoy another person. Federal law prohibits inter-state or foreign electronic stalking[674] and a number of states have also prohibited electronic stalking.

Moreover, nearly all states have similar laws requiring convicted sex offenders and/or certain individuals convicted of a felony to wear a GPS tracking device (GPS bracelet), in order for police to track their movements. Important differences, however, are whether or not the decision to do so is based on individual based assessments (Hinson, 2008). For example, Massachusetts Senate Bill No. 1351 provides for an individualized 'dangerousness assessment', while Florida's Jessica Lunford Act does not, as pointed out by Hinson (2008).[675] There is, however, at present, no equivalent federal law on the electronic monitoring of convicted sex offenders.

7.8.6 Administrative decisions

In 2004, the FDA approved the use of RFID implants as a Class II medical device.[676] This serves as the single most important official administrative decision regarding RFID implants (i.e. HIMs).

---

672 California Senate Bill 30 (Identity Information Protection Act of 2007).

673 Title *18 U.S.C. Part I, Chapter 110A, § 2261A;* see Miller, Neal. *Stalking Laws and Implementation Practices: A National Review for Policymakers and Practitioners* (2001), p. 36, available at: http://www.ncjrs.gov/pdffiles1/nij/grants/197066.pdf

674 Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 223.

675 see Hinson, Zoila. *GPS monitoring and constitutional rights* (43 Harvard Civil Rights-Civil Liberties Law Review, 2008), pp. 285-288.

676 Federal Register, Volume 69, Number 237, 10 December 2004, pp. 71702-71704.

7.8.7 Standards, guidelines and self-regulations (soft laws)

The privacy policy of VeriChip Corp. was first declared in a 'Six Point Privacy Statement', which read as follows:

1. VeriChip should be voluntary and voluntary only. No person, no employer, no government should force anyone to get "chipped."
2. Privacy must be a priority at the highest levels of our organization and as such we will have a Chief Privacy Officer who, with privacy experts, will be charged with addressing the day-to-day global evolution of this technology.
3. We will immediately address privacy and patients' rights in all consumer, distributor and medical documents related to VeriChip
4. VeriChip subscribers are able have their chip removed and discontinued at any time.
5. Privacy means different things to different people, so only the VeriChip customer should designate the groups that may have access to his or her data base information.
6. We pledge to thoughtfully, openly and considerately engage government, privacy groups, the industry and consumers to assure that the adoption of VeriChip and RFID technology is through education and unity rather than isolation and division.

Since then, VeriChip's full privacy policy has changed, and is no longer available on the company's new website after changing its name to PositiveID.

The Federal Trade Commission Act (FTC Act) prohibits unfair, deceptive or misrepresented corporate practices. Unfair practices include, for instance, a failure to implement a minimal level of security of personal information, while deceptive practices include a company's failure to actually implement its own registered privacy policies/codes of conduct. The FTC has the authority to enforce the promises companies make as a result of their privacy policies/codes of conduct regarding how they collect, use and secure personal information[677] and the FTC has used this authority on numerous occasions to challenge the data processing practices and policies of companies that cause harm to consumers.

Since doctors are meant to administer the implantation of HIMs, the American Medical Association (AMA), the largest professional organization of physicians and

[677] Title 15 U.S.C. § 41-58, as amended, Section 5 of the FTC Act.

patients in the US, established guidelines to protect patients receiving RFID implants,[678] which are a part of the AMA's medical code of ethics. In the report, titled "Radio Frequency ID Devices in Humans", the AMA acknowledges the important ethical, legal and social issues raised by HIMs and advocates for a greater role of doctors regarding the non-medical uses of the technology.[679]

The National Institute of Standards and Technology (NIST) issued its Guidelines for Securing Radio Frequency Identification (RFID) Systems. The NIST elaborates how to address the privacy concerns of RFID in the context of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). In addition, the OECD Policy Principles on Radio Frequency Identification were also finalized in 2008.

In recognition of the threats to privacy posed by GIS, the Urban and Regional Information Systems Association (URISA) adopted the GIS Code of Ethics, advocating for the protection of individual privacy and the careful handling of new information discovered about individuals through GIS-based manipulations.

The Cellular Telecommunications and Internet Association (CTIA) adopted the Best Practices and Guidelines for Location Based Services, essentially highlighting the necessity of gaining a user's consent before disclosing his/her location information. In addition, the World Wide Web Consortium (W3C) formed a Geolocation Working Group to develop a set of standards for handling users' location information that ensures both interoperability and privacy.

---

678 Report of the Council on Ethical and Judicial Affairs, CEJA Report 5-A-07, available at: http://www.ama-assn.org/ama1/pub/upload/mm/467/ceja5a07.doc

679 *Ibid.*

7.9 DEFICIENCIES AND DILEMMAS OF THE US LEGAL FRAMEWORK

Based on the principles of privacy and the criteria for determining the adequacy of a legal framework, as outlined in Chapter 3, significant legal deficiencies and dilemmas within US statutory laws, tort law and the 'reasonable' expectation of privacy standard (as adopted by US courts) become clear. The ineffectiveness of the US legal framework in upholding the right to privacy against the intrusive capabilities of HIMs is, in this dissertation's analysis, quite substantial.

First and foremost, in light of the US Supreme Court's decisions in *United States v. Knotts*, *United States v. Karo* and *Oliver v. United States*, implantees may not have a reasonable expectation of privacy of the location information generated by their HIMs as they move about in public. Location information collected by law enforcement agencies via the scanning of RFID implants or monitoring of GPS implants is, at present, not protected under the Fourth Amendment.

The case law also fails to uphold the general legal ***principle of proportionality*** or ensure that the scanning and/or monitoring of HIMs is proportionate to their purported legitimate aim(s). Given that there is essentially no reasonable expectation of privacy in public, as the law stands now, mass public surveillance and the tracking and recording of people's movements out in public by the US Government, without any justification whatsoever, could be potentially lawful. Nevertheless, unwarranted mass public surveillance should be considered disproportionate, unreasonable and inappropriate in a free and democratic society.

Although the US Supreme Court, in *Katz v. United States*, held that whatever a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected",[680] if that person does not take extraordinary steps or affirmative measures to protect his or her privacy, as both Paton-Simpson (2000) and Kearns (1998) separately point out, he or she has no reasonable or subjective expectation of privacy.[681] This is essentially consistent with the findings of the 9th Circuit Court of Appeals in *US v. Kyllo*.[682] "Thus the viewpoint is well established that anyone who does not behave as a 'reasonable paranoid' has waived any right to privacy" (Paton-Simpson, 2000, p.

---

680 *Katz v. United States*, 389 U.S. 347 (1967).

681 see Kearns, Thomas B. T*echnology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns* (7 William & Mary Bill of Rights Journal, 1998), pp. 975-1011, at 1005; Paton-Simpson, Elizabeth. *Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places* (50 University of Toronto Law Journal 305, 2000), pp. 305-346, at 306.

682 *US v. Kyllo*. 190 F.3d 1041 (9th Circuit, 1999).

306). This interpretation may especially hold true for those who have decided to have a HIM voluntarily implanted.

The "reasonable expectation" of privacy is additionally problematic, since it is presently defined by the privacy-intrusive capabilities of the latest technologies, their availability and the scope and manner of their deployment and use. For instance, consistent with *Kyllo v. United States,*[683] the mass deployment and widespread public use of RFID and GPS technology and GPS tracking devices, as the technologies become more and more readily available, without the appropriate safeguards in place, would surely diminish our privacy expectation level, both meaningfully and legally. As David Wood, in the *Report on the Surveillance Society,* argues, the reasonable expectation of privacy will surely be depressed if people "get used to" increasingly more surveillance.[684] Likewise, as Dr. Peter Zhou, ADS' chief scientist at the time, similarly proclaimed, "[b]efore there may have been resistance, but not anymore. People are *getting used* to implants. New century, new trend"[685] (emphasis added). In addition, as Minert (2006) points out, the problem is that the reasonable expectation could become just an echo of the government's expectation of privacy (2006, pp. 1653-54). Moreover, the relatively widespread voluntary implantation of HIMs could also potentially indicate that people value privacy far less (or it could be interpreted as such) and, as Noah Feldman (Harvard law professor) argues, "the less we value it [privacy], the less our judicial institutions will protect it for us".[686]

Although the ECPA regulates government access to stored electronic communications, communications from a tracking device is exempted from being included in electronic communications.[687] A "tracking device" is defined as "an electronic or mechanical device, which permits the tracking of the movement of a person or object".[688] Both RFID and GPS implants are indeed types of tracking devices and, thus, may be explicitly excluded from the ECPA.

---

683 see *Kyllo v. United States*, 533 US 27, 34.

684 see Wood, David Murakami (ed.). A *Report on the Surveillance Society* (2006), p. 80.

685 Gossett, Sherrie. "Implantable-chip company in financial straits" (WorldNetDaily, 4 March 2003), available at: http://www.wnd.com/news/article.asp?ARTICLE_ID=31353

686 Feldman, Noah. "Strip-Search Case Reflects Death of American Privacy" (Bloomberg, 9 April 2012), available at: http://www.bloomberg.com/news/2012-04-08/strip-search-case-reflects-death-of-american-privacy.html

687 Title 18 U.S.C. Part I, Chapter 119, § 2510(12)(c).

688 Title 18 U.S.C. Part II, Chapter 205, § 3117(b).

In addition, relevant ***case law is not grounded on statutory law*** and the legal framework fails to provide adequate ***clarity*** and ***consistency***. While Rule 41 of the Federal Rules of Criminal Procedure requires that if law enforcement agents want to use or install a tracking device, they must obtain a warrant based on probable cause to do so, "[t]he traditional statutory framework governing electronic surveillance does not provide law enforcement with clear-cut guidance" (Clark, 2006, p. 25). The law does not clearly delineate whether or not probable cause or simply reasonable suspicion under Title 18 U.S.C Part I, Chapter 121 § 2703(d) is required for a warrant or court order requesting telecommunication companies to hand over cell-site information, whether historical, real-time or 'prospective', to government entities. Federal agencies are routinely asking US courts to order telecommunication companies to provide historical or real-time tracking/location data[689] and the basis of the decision to do so is at the discretion of judges (*Ibid*.), rather than based on explicit provisions in statutory law. The US Justice Department recommends that Federal prosecutors seek warrants based on probable cause, in order to access location information.[690] However, Federal judges differ as to whether the government actually requires probable cause to obtain a warrant to access the cell-site (location) information. Some judges have been granting warrants based not on probable cause, but rather based on considerable lower standards of suspicion (*Ibid*.). Local police officials are now also routinely using cell phones as a tracking tool "with little or no court oversight".[691]

Essentially, there is general disagreement whether or not location data gathered/obtained from cell phones/GPS-enabled smartphones/GPS tracking devices is protected by the Fourth Amendment and uncertainty about the procedures/requirements that law enforcement agencies must satisfy to access/use the location data, which has often enabled law enforcement agencies to access/use this data without probable cause or a warrant.

---

689 As most recently revealed by the privacy activist Christopher Soghoian on his blog, Sprint Nextel provided law enforcement agencies with customer location data more than 8 million times between September 2008 and October 2009 made available through a web application developed by Sprint to handle the large volume of requests, according to a manager of the company, who disclosed the information at a non-public conference, available at: http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html

690 Nakashima, Ellen. "Cell phone Tracking Powers on Request: Secret Warrants Granted Without Probable Cause" (Washington Post, 23 November 2007), available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/11/22/AR2007112201444.html

691 see Lichtblau, Eric. "Police Are Using Phone Tracking as a Routine Tool" (New York Times, 31 March 2012), available at: http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html?_r=2&partner=MYWAY&ei=5065

Arguably, the US legal framework requires little or no evidence or degree of suspicion when tracking is destined to occur only in public places. As US Magistrate Judge James K. Bredar recognized, "[i]f acquisition of real-time cell site information is equivalent to a tracking device, it would seem the Government is not constitutionally required to obtain a warrant provided the phone remains in a public place where visual surveillance would be available".[692] Moreover, as US Magistrate Judge Gabriel Gorenstein pointed out, there is a difference between cell phones voluntarily carried and the Government's covert placement and use of tracking devices. HIMs are voluntarily implanted, at least for now. When an individual has chosen to voluntarily carry a device and permit the transmission of its information to a third party, the Fourth Amendment is not implicated.[693]

The same legal reasoning for cell phones and cell site information could apply to the use of GPS implants (and other GPS tracking devices) for law enforcement surveillance purposes when the implantee (or end-user) is in public (Ganz, 2005).[694] Equally, warrantless RFID tracking within public areas could also be considered lawful.

Already, a number of Federal courts that have deliberated on GPS tracking have extended the legal reasoning of the US Supreme Court in *United States v. Knotts* and *United States v. Karo* to the use of GPS tracking devices.[695] The 7th Circuit US Court of Appeals in *United States v. Garcia*, basing its decision on *Knotts*, upheld warrantless GPS tracking in public areas, denying that the use of a GPS tracking device constituted a search,[696] by incorrectly comparing the use of GPS satellites for vehicle tracking to the use of satellite imaging or CCTV cameras for observing a vehicle's route.[697] The 9th Circuit US Court of Appeals in *United States v. Pineda-Moreno* equally upheld that the use of a GPS tracking device by law enforcement agencies to monitor a person's

---

692 In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers and the Production of Real Time Cell Site Information, United States District Court for the District of Maryland, Memorandum Opinion, 28 November 2005, p. 13.

693 see In Re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, United States District Court for the Southern District of New York, Opinion and Order, United States Magistrate Judge, Gabriel W. Gorenstein, 20 December 2005, p. 25.
The opinion is consistent with *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

694 see Ganz, John S. I*t's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Tracking Devices* (95 The Journal of Criminal Law and Criminology, 2005).

695 see, e.g., United States v. Moran, 349 F.Supp.2d 425 (NDNY, 2005).

696 *United States v. Garcia*, 474 F.3d 994 (7th Circuit, 2007).

697 *Ibid.*, at 997.

movements in public is not considered a search under the Fourth Amendment and thus does not require a warrant.[698]

There are also a few State courts in the US that have clearly concluded that GPS tracking in public is not a search under the Fourth Amendment. For instance, the District IV Wisconsin Court of Appeals ruled that police are permitted to conduct warrantless GPS tracking, since the tracking does not constitute a search, as the law currently stands.[699] Interesting enough, the law's deficiency even caused the Wisconsin court to urge the state legislature to regulate police and private use of GPS tracking technology. In 2005, the Connecticut Appellate Court in *Turner v. American Car Rental, Inc* dismissed the intrusion upon seclusion tort claim, concluding that it was unaware of any legal precedent establishing that the installation of a GPS tracking device on a vehicle violates the privacy rights of the driver or that a driver has an expectation of privacy on a public highway.[700]

On the other hand, certainly not every US court agrees. The District of Columbia Circuit Court of Appeals in *United States v. Maynard*[701] reversed the drug conviction of Antoine Jones, which was significantly based on the location information gathered from a GPS tracking device installed on his vehicle without a warrant. The District of Columbia Circuit Court of Appeals held that warrantless GPS tracking violated the Fourth Amendment and that the location information obtained from the GPS tracking device was not public, concluding that Antoine Jones had a reasonable expectation of privacy of his movements. After the District of Columbia Circuit Court of Appeals overturned Jones' conviction, the Obama Administration petitioned the District of Columbia Circuit Court of Appeals to rehear the case *en banc*. The petition was denied.[702]

Some State courts have also ruled that GPS tracking requires a warrant. But, these decisions are premised on the respective State laws and State constitutions and not explicitly on Federal law or the Fourth Amendment,[703] and there were also compelling dissenting opinions.

---

698 *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Circuit, 2010).

699 *State v. Michael A. Sveum*, 769 N.W.2d 53, 59 (District IV Wisconsin Court of Appeals, 2009).

700 *Turner v. American Car Rental*, 884 A.2d 7 (Conn. App. Ct., 2005).

701 *United States v. Maynard*, 615 F.3d 544 (D.C. Circuit, 2010).

702 United States v. Jones, 625 F.3d 766 (D.C. Circuit, 2010).

703 see, e.g., *People v. Scott C. Weaver*, 12 N.Y. 3d 433, 435 (New York Court of Appeals, 2009); Washington v. Jackson, 150 Wash. 2d 251, 76 P3d 217 (2003).

However, since there are conflicting decisions in the US among the circuit courts concerning the constitutionality of warrantless GPS tracking under the Fourth Amendment, at the request of the US Government,[704] the US Supreme Court indeed granted a writ of certiorari in the case *US v. Jones* to potentially resolve and clarify the issue.[705]

It is important to point out that in *United States v. Knotts* the US Supreme Court ruled on RF tracking devices capable of enhancing the ability of law enforcement agents to conduct visual and physical surveillance, but the Court did not rule on GPS tracking capable of substituting or removing the need for visual or physical surveillance altogether, as both the EFF and ACLU highlight in their *amicus curiae* brief,[706] in support of the appellant in *US v. Jones* in the District of Columbia Circuit Court of Appeals.[707]

Moreover, the US Supreme Court also indicated in *United States v. Knotts* that other methods of more sophisticated electronic surveillance (i.e. GPS tracking) may require a different judgment[708] and in *Dow Chem. Co. v. United States* judged that satellite imaging may constitute a search under the Fourth Amendment, since it practically replaces, rather than enhances, the senses of law enforcement agents.[709] Indeed, using GPS devices to constantly track a person's movements for a prolonged period of time, replacing the need for law enforcement agents in the field, can divulge far greater amounts of data than using simple RF devices to assist law enforcement agents in the field when observing a person's movements for a limited period of time.

Furthermore, the District of Columbia Circuit Court of Appeals in *United States v. Maynard*[710] convincingly held that Antoine Jones' movements were actually not exposed to the public, since "the likelihood a stranger would observe all those movements is not just remote, it is essentially nil".[711] Indeed, the District of Columbia Circuit Court

---

704 Petition for a Writ of Certiorari, *United States v. Jones*, No. 10-1259 (April 15, 2011).

705 *US v. Jones*, USSC No. 10-1259, certiorari granted 6/27/11.

706 *Amicus curiae* literally means "friend of the court". According to Rule 37(1) of the Rules of the *Supreme Court of the United States (adopted 17 July 2007), an amicus curiae* brief "brings to the attention of the Court relevant matter not already brought to its attention by the parties may be of considerable help to the Court".

707 see Brief of *Amici Curiae* Electronic Frontier Foundation and American Civil Liberties Union of the National Capital Area in Support of Appellant Jones, 3 March 2009.

708 *United States v. Knotts*, 460 U.S. 276, 283-284 (1983).

709 *Dow Chem. Co. v. United States*, 476 U.S. 227, 238-239 (1986).

710 *United States v. Maynard*, 615 F.3d 544 (D.C. Circuit, 2010).

711 *Ibid*., at 560.

of Appeals made a strong argument in differentiating between the tracking of a vehicle's single journey and the prolonged, non-stop tracking of a vehicle. Emmett (2011) agrees with this argument.[712]

But, as the US Government contends, the US Supreme Court in *Knotts* did not make this distinction.[713] In addition, as the US Government also points out, the US Supreme Court in *United States v. Karo* did not judge that the length of time or duration was a factor in determining whether or not electronic tracking constituted a search under the Fourth Amendment.[714]

Up until 2011, the US Supreme Court had not yet had an occasion to deliberate on the legal questions concerning GPS tracking or to judge whether or not the installation and use of GPS tracking devices constitutes a search under the Fourth Amendment. Since the US Supreme Court has granted a writ of certiorari in the case *US v. Jones*,[715] this occasion finally arrived.

The US Supreme Court, in *United States v. Jones*, ended up ruling against the US Government (and some previous circuit court decisions), judging that the installation and use of a GPS tracking device to monitor the movements of a vehicle constitutes a search within the meaning of the Fourth Amendment (i.e. concurring with the District of Columbia Circuit Court of Appeals). But, as earlier predicted (see, e.g., Ganz, 2005), the Court did not explicitly rule that GPS tracking requires a warrant. Although, the minority concluded in their separate opinions that prolonged GPS tracking/monitoring could amount to a search requiring a warrant, the majority declined to decide whether or not the search in this specific case required a warrant. The Court argued that it was not required, in this particular case, to clarify whether or not electronic monitoring (i.e. GPS tracking/monitoring) for prolonged periods of time is an unconstitutional invasion of privacy or to judge whether this type of search was reasonable or unreasonable. As a result of procedural rules, the majority considered that argument *forfeited*.

712 For example, Emmett (2011) argues: "Close consideration of both the duration of the electronic monitoring and the GPS technology that enabled the surveillance would have revealed that law enforcement obtained information of a type that was not available to the public through simple
(or even technologically enhanced) visual surveillance" (Emmett, Caitlin. *United States v. Pineda-Moreno, Tracking Down Individuals' Reasonable Expectation of Privacy in the Information Age* (41 Golden Gate University Law Review, 2011), p. 26.

713 Petition for a Writ of Certiorari, *United States v. Jones*, No. 10-1259 (U.S. Apr. 15, 2011), p. 14.

714 *Ibid*., p. 15.

715 *US v. Jones*, USSC No. 10-1259, certiorari granted 6/27/11.

Given the conservative majority of the current US Supreme Court,[716] the Court, as a result, neither contradicted *United States v. Karo*, which held that evidence or probable cause is not required to observe information conveyed in areas observable to the public,[717] nor backpedaled on a landmark decision with regards to RF tracking in *United States v. Knotts*. On the contrary, these decisions were essentially reaffirmed.

Moreover, in light of the US Supreme Court's decision in *Kyllo v. United States*, which judged that the greater availability and more widespread the deployment and adoption of a particular technology the less reasonable expectation of privacy the public enjoys with respect to its use,[718] the widespread availability of GPS tracking devices and the widespread use of GPS technology has significantly reduced the reasonable expectation of privacy of one's movements in public. Now that GPS tracking has already become a common practice in criminal investigations, this legal interpretation has only been amplified.

Therefore, the legal matter is still not closed and the conflicting decisions among the circuit courts are not fully settled. There is, as a result, no compelling way to foresee how the US Supreme Court, or other US courts, will rule on future warrantless GPS (or RFID) tracking cases. Essentially, the law, as it stands now, arguably still fails to provide ***foreseeability, consistency*** and ***clarity***, regarding the use of tracking technologies by law enforcement agencies.

Unless significant changes manifest in the near future, in light of the relevant case law, the vacuum of law, the US Government's warrantless wiretapping controversy, the increasing abuse of the National Security Letters process, the revealed "President's Surveillance Program" [referring to former US President George W. Bush], the PATRIOT Act, the Protect America Act of 2007, which amended the Foreign Intelligence Surveillance Act (FISA) and removed the warrant requirement for government surveillance of international electronic communications, the increasing use of cell phones for real-time tracking and the increasing availability and widespread use of GPS technology, the signs are there that warrantless GPS tracking will only further develop as a common practice. Accordingly, there is still increasing pressure from the US Government to allow for warrantless GPS tracking.

---

716 For further discussion and analysis on the increasingly conservative judgments of the US Supreme Court, see Chemerinsky, Erwin. T*he Conservative Assault on the Constitution* (Simon & Schuster, 2010).

717 *United States v. Karo*, 468 U.S. 705 (1984).

718 see *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

In short, as a consequence of the legal deficiencies and dilemmas outlined above, the examination by law enforcement agencies of the location information generated by both RFID and GPS implants is, at present, not granted Fourth Amendment protections.

Moreover, in light of the recent *Hiibel v. Sixth Judicial District Court of Nevada,* 542 U.S. 177 (2004) decision, which held that police may oblige a person to provide identification upon request when conducting an investigation, the reading of a person's RFID implant, which constitutes a form of identification, may also arguably not constitute a search under the current legal framework (Herbert, 2006).

Furthermore, since the printouts of location information generated by GPS and RFID tracking may be considered originals and due to the interpretation of the Fifth Amendment, as it stands now, the location information pertaining to HIMs could be used as potentially incriminating evidence in a court of law. The apparent ***lack of foreseeability*** and ***clarity*** of Fourth Amendment interpretations of electronic tracking in public, or the lack of specific Federal statutory rules concerning the use of or access to location information generated by RFID/GPS implants, may also quash the possibility of resorting to the 'exclusionary rule'.

When it comes to the private sector, tort law is equally not applicable to the location information generated by HIMs, as the current US legal framework stands, since it is generally accepted by courts in the US that "there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye", as elaborated in the comments of the Restatement (Second) of Torts.[719] Hence, as McClurg (1995) rightfully points out, the problem is not so much with the definition of the tort of intrusion, but rather the Restatement comments pertaining to that definition. As McClurg (1995) further points out, the adherence of US courts to the outmoded rule and viewpoint that privacy and seclusion, for the most part, cannot be intruded upon in public places exhibits a deficient understanding of the purpose of privacy and the other civil liberties it is meant to defend. An additional problem with tort of intrusion of privacy, as Schwartz (2000) points out, is that the intrusion must be "highly offensive" [720] and that case law has shown that most stealthy intrusions are unlikely to be found sufficiently "objectionable" (Schwartz, 2000, p. 778).

Significantly, the US legal framework is ***not up to date*** with the current technology. While there is no explicit Federal law that regulates the privacy implications of RFID or

---

[719] Restatement (Second) of Torts, § 652D, comment b (1977). see, e.g., *Hartman v. Meredith Corp.*, 638 F. Supp. 1015, 1018 (D. Kan. 1986) ("The plaintiffs must show that there has been some aspect of their private affairs which has been intruded upon and does not apply to matters which occur in a public place or place otherwise open to the public eye").

[720] Restatement (Second) of Torts, § 652B.

the information collected and stored as a result of RFID technology, there are equally no specific statutes or regulations that sufficiently address the privacy implications of GPS tracking. Although Federal law regulates the disclosure of location information generated by cell phones (as part of CPNI), and also regulates governmental access to private/stored electronic communications, the law, however, does not apply to the location information generated by RFID or GPS implants. As Reneger points out, the Telecom Act "offers no protection for people whose privacy is violated through non-cell-phone-based collections of location information" (Reneger, 2002, p. 562). Herbert similarly agrees that while cell phone users may have a reasonable expectation of privacy of their call location information, "non-cellular forms of wireless products containing GPS technology are not currently protected by any statutory location privacy protections" (Herbert, 2006, p. 445). Moreover, the meaning of location information is explicitly restricted to "call location information concerning the user of a commercial mobile service",[721] and therefore does not cover the more extensive location information generated by HIMs or other similar PLDs. Consequently, with the exception to the CPNI of cell phones, as the law stands now, location information generated by devices other than cell phones is not afforded adequate privacy protection. This deficiency may be partly the result of the US piecemeal legal approach to protecting privacy, which is particularly sectoral rather than all-inclusive or comprehensive.

Under the US legal framework, "telecommunications carriers" are defined as "any provider of telecommunications services".[722] RFID or GPS implants could only come into the scope of the Telecom Act if companies like Digital Angel, ADS or VeriChip Corp. (now known as PositiveID), for example, were considered telecommunications carriers, commercial mobile service providers or joint venture partners. However, none of these companies are considered as any of these types of entities. As a result, there are arguably little or no legal barriers, at present, that prevent companies, like ADS or Digital Angel, from selling location information generated by HIMs to third parties.

One of the other main dilemmas is that the US legal framework does not have comprehensive, cross-sectoral privacy legislation equivalent to the EU's Data Protection Directive,[723] which is binding on both private entities and public authorities (except

---

721 Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 222(f).

722 Title 47 U.S.C. Chapter 5, Subchapter I, § 153(44). "Telecommunications" are defined as the "transmission, between or among points specified by the use, of information of the user's choosing without change in the form or content of the information sent and received". Title 47 U.S.C. Chapter 5, Subchapter I, § 153(43).

723 Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

for law enforcement agencies). The EU's Data Protection Directive even affects entities without activities or operations in the EU, since the Directive regulates the transfer of personal data from EU Member States to any third party outside the EU. Article 25 requires that personal data from the EU must not be transferred to any country outside the EU unless that country has "adequate" privacy protections. A conflict between the US and EU over whether or not privacy laws in the US were adequate or up to par with the EU's Data Protection Directive may have arguably resulted in the US-EU 'Safe Harbor' arrangement, in order to alleviate some of the differences, whereby US companies voluntarily self-certify their adherence to the safe harbor requirements or participate in a self-regulatory organization that adheres to the requirements. However, the need for the 'safe harbor' agreement in the first place only revealed an agreement that the US legal framework, in terms of privacy protection, is relatively weak and inadequate in comparison to the EU legal framework.

Instead of comprehensive privacy legislation, the US relies on a hodgepodge of a number of statutory laws covering separately different sectors or themes. But, as Reidenberg argues, "sectoral regulations are reactive and inconsistent" and the "gap-filling approach also leaves many areas of information processing untouched and runs counter to the cross-sectoral nature of modern data processing" (Reidenberg, 2000). Indeed, none of the US sectoral laws, for instance, can be applied adequately to RFID applications.

On the other hand, the EU's Data Protection Directive (Directive 95/46/EC) does apply to the processing of personal data by RFID technology.[724] Nevertheless, even though the EU has far superior privacy law, the EC has recognized that there are indeed difficulties in applying the Data Protection Directive to new technologies, even if the Directive is meant to be technologically neutral or independent. The EC has further recognized that it may be necessary to develop additional specific provisions or new legislation to defend against the new threats posed by RFID and other technological developments.[725] The EU plans to replace the Data Protection Directive with a General Data Protection Regulation, and is considering the formulation of specific legislation or *lex specialis*, with respect to

[724] The EU's Article 29 Working Party on data protection has established that the Data Protection Directive strictly applies to the personal data collected through RFID and that the data protection principles should be implemented within RFID technology. see Article 29 Working Party, Working document on data protection issues related to RFID technology, January 2005 (WP 105).

[725] see Com (2007) 87 final, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive.

the Data Protection Directive, to address the special privacy issues surrounding RFID.[726] The EC also felt that there was a need to specify that the 'ePrivacy Directive'[727] explicitly applies to RFID.[728] The EC has also adopted a set of recommendations to ensure the protection of privacy and personal data in applications supported by RFID technology,[729] but the recommendations are more focused on RFID applications used in retail trade activities.[730]

---

[726] see Commission Staff Working Document, Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Future networks and the Internet: Early Challenges regarding the "Internet of Things", p. 8; COM(2007) 96 Final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy Framework, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/dir_citizens_rights_en.pdf

[727] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[728] see COM(2007) 698 final. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, p. 19, para. 28; see Directive 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009, recital 56. Accordingly, Article 3 of the ePrivacy Directive, which defines the scope of the directive, was revised to include "*public communications networks supporting data collection and identification devices*". The amendments ensure that the EU's data protection legal framework covers RFID. For further discussion, see Cannataci, Joseph A. *Recent developments in privacy and healthcare: Different paths for RFID in Europe and North America?* (International Journal of RF Technologies, Volume 2, 2010/2011), pp. 173–187.

[729] C(2009) 3200 final, Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.
The recommendation calls for a PIA framework for RFID. The European Commission will later analyze the impact of the recommendation on companies, public entities and citizens (Cannataci, 2011). If the impact is adequate, then perhaps specific rule-making for RFID applications may be put aside (Cannataci, 2011).

[730] I attended the 3rd closed meeting of the RFID Recommendation Implementation Informal Working Group at the EC. Present at the meeting were industry associations, standardization bodies, public authorities and a representative from the Article 29 Working Party. The first goal of the group was to establish an agreed upon generic pan-European PIA Framework for RFID applications (RFID PIA) with the endorsement of the Article 29 Working Party. This was accomplished in February 2011. The ultimate seal of approval came in April 2011, when the RFID PIA was officially signed by the European Commission Vice President (Neelie Kroes), the Chairman of the Article 29 Working Party (Jacob Kohnstamm), the Executive Director of the European Network and Information Security Agency (Udo Helmbrecht) and various retail and RFID industry representatives, including GS1 and the European Retail Round Table (For further information/explanation, see Cannataci, 2011). The RFID PIA framework is the first of its kind in Europe, and supplementary templates and checklists are to be developed for specific RFID applications. It is important to point out that while the RFID PIA framework is a step in the right direction, the main problem is that it will only be applicable to RFID application service providers, and not to the developers of RFID infrastructures/systems. This is, unfortunately, consistent with the Data Protection Directive.

In addition, the EC has also recognized the opinion of the European Group on Ethics (EGE) that "non-medical ICT implants [HIMs] in the human body are not explicitly covered by existing legislation, particularly in terms of privacy and data protection".[731] The EGE recommended that the EC initiate legislation on HIMs.[732] Surely, without equally comprehensive privacy legislation, the US legal framework is in far worse shape and, above all, requires specific legislation on RFID, let alone for HIMs.

Since there is no Federal law yet on RFID technology whatsoever, there is also essentially a lack of legal consistency concerning RFID in the US, as the relatively few existing State laws on RFID vary considerably in substance, scope and purpose. Most of the State laws address the use of RFID tags embedded in retail products or identity documents. Moreover, some of the State laws that address RFID technology are insufficient and are not without their own flaws. For example, in Washington, the State law criminalizes the unauthorized reading of an RFID identification device, "for the purpose of fraud, identity theft, or for any other illegal purpose", as a class C felony.[733] Thus, this law only prohibits reading an individual's RFID identification when it is done so for illegal purposes and does not prohibit the reading for identification and tracking purposes alone. Nevertheless, as EPIC Executive Director Marc Rotenberg pointed out in a prepared testimony before the House of Representatives Oversight Committee's Information Policy, Census and National Archives Subcommittee, the US Government typically acts only after the identity theft has occurred.[734]

However, while there is no Federal statutory law clearly regulating the use of GPS tracking devices, some states, such as California, have statutory laws regulating the activity. California Penal Code Section 637.7 (a) mandates: "No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person". But, this law is clearly only applicable to persons in vehicles, and therefore does not explicitly cover GPS tracking via smartphones or GPS implants. For instance, Subsection (b) states: "This section shall not apply when the registered owner, lesser, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle". Moreover, Subsection (d) defines an "electronic tracking device"

---

731 Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, Opinion No. 20, Adopted on 16/03/2005, Section 6.5.4.

732 *Ibid.*

733 see Title 19, Chapter 19.300, § 19.300.020.

734 see Marc Rotenberg's prepared testimony, available at: http://informationpolicy.oversight.house.gov/documents/20090617111417.pdf

as "any device attached to a vehicle or other movable thing that reveals its location or movement by transmission of electronic signals".

Moreover, although state legislatures in the US have also enacted breach notification laws concerning personal data, there is no Federal law yet,[735] which would be ideal for any nationwide breach and for establishing common notification standards. Instead, state laws can vary somewhat on the process behind the notification of breaches.

The DHS claims that the Privacy Act 1974 regulates the data collected through RFID, stating the following:

> When RFID is used for human tracking, the data collected will undoubtedly comprise a "system of records" under the Privacy Act of 1974. People should have at least the rights accorded them by that law when they are identified using RFID. Systems using RFID technology are, of course, also subject to the E-Government Act's Privacy Impact Assessment [PIA] requirements[736] (emphasis added).

The Privacy Act 1974 does not restrict the content of a "record" to education, financial transactions, medical history and criminal or employment history and may indeed be applicable to data collected through RFID technology. However, in accordance with the current legal standpoint of jurisprudence in the US, concerning the absence of privacy while in public, and the lack of legal clarity concerning the privacy of location information, the Privacy Act 1974 arguably may not be applicable to the location information collected via RFID implants/microchips and RFID readers in public spaces. If the US legal

---

735 Senator Patrick Leahy recently introduced S.1490, entitled "the Personal Data Privacy and Security Act of 2009", which could have provided for a national standard for data breach notification. More recently, the Secure and Fortify Electronic Data Act (the "SAFE Data Act") was proposed in the US House of Representatives, which aims to establish Federal (i.e. nationwide) breach notification requirements, overriding all existing state breach notification laws. With the recently adopted EU Telecom Package and revision of the 'ePrivacy' Directive, the EU has already passed laws requiring communications service providers to notify consumers of security/data breaches. see Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

736 The Use of RFID for Human Identification: A Draft Report from DHS Emerging Applications and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee, Version 1.0, p. 4, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf
This statement was partially amended in the final version. Instead of writing "when RFID is used for human tracking", the final version writes "when an RFID-enabled system is used to collect data about individuals". see The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, p. 4, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

framework does not prohibit the use of location information obtained by law enforcement agencies via GPS tracking devices without a warrant, it would be hard to imagine how the US legal framework would effectively regulate or prohibit the use of location information generated and transmitted to third parties via HIMs voluntarily implanted.

Nevertheless, even if the Privacy Act 1974 is somehow interpreted to be applicable in regulating the storage/processing of location information collected through RFID readers placed in the public space, this is only possible for the location information collected, stored and used by the US Government. The Privacy Act 1974 is only applicable to agencies and the term "agency" is specifically defined as:

> any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.[737]

Therefore, the Privacy Act 1974 is in no way applicable to HIM service providers, which may store the location information generated by HIMs, or any other private data controller for that matter. Moreover, the Privacy Act 1974 does not prohibit the US Government from buying vast quantities of personal information from commercial data brokers, which is in fact an ongoing trend.

Privacy Impact Assessments (PIAs)[738] may be required to evaluate how personal information in identifiable form will be collected, maintained and disseminated using RFID, however, this is also only applicable to personal information held (and technologies/systems used) by the US Government (i.e. Federal public agencies). A PIA was in fact conducted regarding RFID technology, but this specifically pertained to RFID tags embedded in government documents, and not the general use of RFID technology for other applications. Moreover, as Cannataci highlights, PIAs in the US are not being used to induce the implementation of technical measures to safeguard privacy (2011, p. 182).

In addition, the US legal framework, pertaining to privacy protection, ***relies primarily on private sector self-regulations*** (privacy policies, voluntary standards or codes of conduct), whereby self-regulations and internal self-reporting are often preferred over

---

737 Title 5 U.S.C. Part I, Chapter 5, Subchapter II, § 552(f).

738 In US law, a PIA is described as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks" (E-Government Act of 2002, Section 208).

'hard' laws and (external) scrutiny. Moreover, the US approach to privacy protection generally promotes the view that self-regulations are friendlier towards the freedom of information and commerce and the promotion of innovation. The rationale behind this may be based on the laissez-faire economic theory, whereby the belief is that the market usually ends up regulating itself. While there are indeed a number of examples of this rationale proving true, such as the controversy surrounding the unveiling of Intel Corporation's Pentium III microchip in January 1999 (Werner, 2008),[739] there are plenty of more examples proving it to be untrue.

Self-regulations or codes of conduct, without the existence of binding 'hard' laws to establish the minimum standards as their basis, can barely be considered reliable. Consumers/citizens especially cannot depend on self-regulations/codes of conduct when the self-regulations are themselves insufficient and stagnant and cater to the self-interests and requests of major industry players. The over-reliance solely on self-regulations may result in requirements guided by the "invisible hand", not requirements imposed by transparent, binding laws. This approach raises concerns of ***the lack of accountability*** and supervision. The same mistake of over-relying on investment banks and other financial institutions to self-regulate the risky financial derivatives market was made over the last decade and we have now witnessed the enormous negative consequences of that system. This approach is not relied upon or trusted for regulating product safety or the use of chemicals, and there is also little reason it should be relied upon or trusted for safeguarding privacy.

Self-regulations have proved to be insufficient to address threats to privacy. For instance, Schwartz (1999) rightfully argued early on that industry self-regulations are inadequate to regulate online privacy. As EPIC later showed, self-regulations indeed have seriously failed to provide online privacy and regulate the use of cookies.[740] Self-regulations have also failed to ensure the appropriate content and availability of privacy policies for social networking websites.[741] The World Privacy Forum has also highlighted that self-regulation initiatives (e.g. the Networking Advertising Initiative) have been

---

739 The original design for Intel's processor microchip had a serial number embedded within the hardware code that could enable online marketers to identify and track Internet users. Consumer boycott threats led to Intel removing the identification system. see Clausing, Jeri. "Intel Alters Plan Said to Undermine PC User's Privacy" (New York Times, 26 January 1999), p. Al; Werner, Matthew. Google and Ye Shall Be Found: Privacy, Search Queries, and the Recognition of a Qualified Privilege (34 Rutgers Computer & Technology Law Journal 313, 2008).

740 Jay Hoofnagle, Chris. *Privacy Self Regulation: A Decade of Disappointment*, EPIC, 4 March 2005, available at: http://epic.org/reports/decadedisappoint.pdf

741 see Bonneau, Joseph and Sören Preibusch. *The Privacy Jungle: On the market for data protection in social networks* (WEISS, 2009).

inadequate to defend consumer's privacy against online targeted behavioral advertising technologies.[742] As a result of the failures, EPIC recommended that the FTC "should abandon its faith in self-regulation", concluding that "[s]elf-regulatory systems have served to stall Congress while anesthetizing the public to increasingly invasive business practices".[743]

Unfortunately, however, with regards to RFID, the US Government regrettably believes, for now at least, that self-regulations are sufficient to regulate RFID. Some at the FTC have concluded that "technology-specific privacy legislation is unnecessary at this juncture" regarding RFID.[744] But, self-regulations are obviously only effective to the extent to which companies comply. While, in the US, Better Business Bureaus can be leveraged to help put into effect self-regulations, this approach relies on voluntary compliance. Moreover, while the FTC has the authority to enforce a company's privacy policy/code of conduct, no rights of private legal action are available under the FTC Act. Therefore, it may also be unrealistic to claim that the current approach adequately satisfies the ***principle of enforcement/redress***.

Without comprehensive privacy legislation in the US or Federal statutory laws that explicitly regulate HIMs and protect or restrict access to location information generated by them, we are left to rely on the self-regulations and good will of companies like ADS/Digital Angel and VeriChip Corp. However, companies, such as Digital Angel or VeriChip Corp., can gain considerably from selling location information. Moreover, the privacy policy of VeriChip Corp., like with other US companies, is subject to changes.[745] As VeriChip Corp. themselves previously declared, "[w]e reserve the right

---

742 World Privacy Forum, "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation", November 2007.
But, this did not at all prevent the FTC from doubling down on its self-regulation policies, which later published the FTC Staff Report, "Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology" (February 2009).
Hirsch has equally highlighted that the reliance on self-regulations and the Network Advertising Initiative to control the use of online targeted advertising has been largely unsuccessful or ineffective. see Hirsch, Dennis. *Law and Policy of Online Privacy: Regulation, Self-Regulation or Co-Regulation* (Seattle University Law Review, Vol. 34, Issue 2, 2011), pp. 439-480.
The industry association, Digital Advertising Alliance, also adopted in 2010 a "Self-Regulatory Program for Online Behavioral Advertising", but its success is equally questionable.

743 Jay Hoofnagle, Chris. *Privacy Self Regulation: A Decade of Disappointment*, EPIC, 4 March 2005, available at: http://epic.org/reports/decadedisappoint.pdf

744 FTC staff report on RFID, p. 20.

745 For instance, Facebook is constantly changing its privacy policies.

to change our Privacy Policy".[746] Although ADS/Digital Angel proclaims their policy now is not to release the data they collect to third parties, their policy was different before. As Edmundson (2005) reveals, the privacy policy of Digital Angel (formerly a major shareholder of VeriChip Corp.), which was previously available on their corporate website, actually stated, in contrary, that "[w]e [Digital Angel] may, from time to time, share, sell or rent some of your personal information with third parties with who we have a business relationship […]".[747]

The AMA's Code of Ethics, the GIS Code of Ethics, the proposed creation of geolocation standards by W3C, and other self-regulations or industry guidelines, as significant as they may be, are not a valid replacement for legally binding 'hard' laws enforceable in a court. Other privacy guidelines on RFID, such as CTIA's Best Practices and Guidelines for Location Based Services, do not cover RFID technology, and the RFID Privacy Guidelines developed by the Center for Democracy and Technology do not even mention human-implantable RFID microchips.

Although the FDA determined that VeriChip's RFID implants are regulated medical devices, in accordance with the Section 201 (h)(2) of the Federal Food, Drug and Cosmetic Act (FD&C Act), "when marketed [intended] to provide information to assist in the diagnosis or treatment of injury or illness",[748] they are *not* regulated medical devices with regards to their intended uses for security, financial and personal identification purposes.[749]

Essentially, without a federal law specifically stipulating otherwise, the legal framework may be potentially inadequate to ensure that HIMs are only implanted voluntarily and, therefore, may fail to uphold the ***principle of consent***. Indeed, RFID implants are implanted into the body using a syringe and, therefore, forced implantation should naturally be considered a violation of the right to bodily integrity, as Ramesh (1997) rightfully points out.[750] The Fourth Amendment, Fifth Amendment and even potentially the Thirteenth Amendment of the US Constitution, as Herbert argues, including the Equal Protection Clause and Due Process Clause, should also put a stop to forced im-

---

746 see VeriChip Corp., available at: http://www.verichipcorp.com/content/company/privacy

747 Edmundson, Kristen E. *Global Positioning System Implants: Must Consumer Privacy Be Lost in order for People to be Found* (38 Indiana Law Review 207, 2005), pp. 207-238, at: 215-216.

748 see a letter written by David E. Troy, Chief Counsel for the FDA, to Jeffrey N. Gibbs, a lawyer representing ADS, in 17 October 2002, available at: http://www.fda.gov/ohrms/dockets/dailys/03/dec03/120503/81n-0033p-sup0003-vol86.pdf

749 *Ibid.*

750 see Ramesh, Elaine M. *Time Enough? Consequences of Human Microchip Implantation*, Franklin Pierce Law Center (1997) available at: http://www.fplc.edu/risk/vol8/fall/ramesh.htm.

plantation (Herbert, 2006). Moreover, the liberty-based approach in the US to privacy would also strongly oppose the mandated implantation of HIMs.[751]

However, although the right to bodily integrity is clearly established by the US Constitution and case law, forced vaccinations, termed "countermeasures", are nevertheless considered lawful, in accordance with the Homeland Security Act of 2002, when the US Government issues a declaration asserting that the occurrence of "an actual or potential bioterrorist incident or other actual or potential public health emergency".[752] Already forced flu and pneumococcal vaccinations on young children in New Jersey were previously approved by the state's Public Health Council. With past precedence and the necessary laws enacted, if the H1N1 virus (also known as the "swine flu") does in fact become a genuine pandemic, forced vaccinations nationwide are therefore not farfetched (at least it was previously not farfetched during 2009), especially for nurses, teachers, etc. While travelling to some countries requires travelers to be vaccinated beforehand and some universities in the US (e.g., the University of Alabama) could mandate that students must be vaccinated before being allowed to enroll, this is more of a condition of exercising a privilege, rather than mandatory vaccination.

With numerous other threats to security, the US Government could also possibly invoke the changing standard of what is considered a 'reasonable' infringement of privacy as the potential basis of the mandatory implantation of HIMs for certain categories of people, if, for example, crime reached epic proportions or if there was another major terrorist attack. As Herbert (2006) further argues, in light of legal jurisprudence, while GPS bracelets are less intrusive than HIMs, this does not necessarily mean US courts will rule HIMs to be anymore unreasonable under the Fourth Amendment than GPS bracelets (Herbert, 2006, pp. 442-43).

Moreover, with regards to stalking, the laws in several states, as pointed out by Miller (2001), have provisions that restrict their applicability.[753] In North Carolina, for example, stalking refers only to instances where the stalker follows or is in the physical presence of the victim[754] and in Maryland the State law defines stalking in terms of

---

751 For further discussion, see Whitman, James. *Two Western Cultures of Privacy: Dignity Versus Liberty* (113 Yale Law Journal 1151, 2003).

752 see Public Law 107-296, Section 304.

753 see Miller, Neal. *Stalking Laws and Implementation Practices: A National Review for Policymakers and Practitioners* (2001), p. 36, available at: http://www.ncjrs.gov/pdffiles1/nij/grants/197066.pdf

754 see *N.C. Gen. Stat.*, § *14-277.3*.

approaching or pursuing a person.[755] Since then, state and federal laws have provided for stalking by means of telecommunication devices. However, while federal law now covers cyberstalking or stalking using electronic devices, the law is only applicable when the stalker or perpetrator has threatened, harassed or intentionally annoyed another person (Miller, 2001). Therefore, stalking laws are arguably not applicable to the use of telecommunication/electronic communication devices to purely track or monitor the movements of another person using electronic or digital means (Miller, 2001).

Furthermore, the law, at present, is *neither anticipatory of the further advancement of the technology* in the very near future. Today, a separate legal framework is more or less applied for the information society/virtual world and the physical world. However, as the physical world and virtual world are more and more merged or 'bridged' so to speak, due to the potential of an 'Internet of Things' and an 'Internet of Persons', this separation is deficient and increasingly no longer valid.

In summary, in light of the above legal deficiencies and dilemmas, the law, as it stands now, is unable to adequately protect the privacy and civil liberties of implantees, uphold the Fourth Amendment and Fifth Amendment, ensure privacy against the intrusive capabilities of HIMs or other PLDs, provide for the reasonable privacy of location information in an age of increasing location-awareness, and permanently guarantee the voluntary implantation of HIMs.

7.10 RECOMMENDATIONS ON ENHANCING THE US LEGAL FRAME WORK

As US Vice President Joseph Biden (then US Senator) notably expressed, when listing potential landmark decisions for the 21st Century, during the US Supreme Court confirmation hearings for Justice John Roberts in September 2005:

> Can a microscopic tag be implanted in a person's body to track his every movement? There's actual discussion about that. You will rule on that — mark my words — before your tenure is over.[756]

---

[755] see *Md. Code* Ann., art. 27, §*124.*

[756] "Transcript: Day One of the Roberts Hearings" (Washington Post, 13 September 2005), available at: http://www.washingtonpost.com/wp-dyn/content/linkset/2005/09/14/LI2005091402149.html

However, once again, if we adopt the "originalist" or "textualist" approach to understanding the US Constitution, then entirely new laws should be adopted, when deemed necessary, by elected legislators/representatives. Therefore, instead of relying on the US Supreme Court to judge in the future (sometime in the next 10-15 years) on the legality of HIMs and to finally rule on the legality of prolonged, widespread electronic tracking of individuals or to clarify the definitive standard for the US Government to be permitted to access location information, the US Congress should proactively formulate and adopt comprehensive Federal legislation. Specific laws for HIMs and location information would eliminate the excessive dependence on US courts to fill in the legal vacuum with altering and opposing judicial interpretations. After all, the legislative branch, once again, is meant to create law, as opposed to the judicial branch, which is principally meant to apply it. Besides, as outlined earlier, based on the relevant legal precedent, it may be unfavorable, in this case, to solely rely on the US Supreme Court.

Nevertheless, it will probably take at least 15 years or more and the widespread deployment of HIMs before the US Congress adopts comprehensive legislation regulating HIMs. As Herbert argues, "[t]he lack of substantial legislative movement in the field of tracking technology renders it unlikely that there will be a federal legislative response to human implants in the near future" (2006, p. 443). Moreover, as Herbert further points out, "it is far more probable that a majority in the current [109th] Congress will continue to defer to the marketplace for potential corrective action aimed at avoiding privacy intrusions" (2006, p. 413). This is consistent with the overall US policy and approach to privacy protection, whereby legislation is adopted only after the privacy threat becomes serious. It is also consistent with the arguably mistaken belief that regulations are still premature for RFID applications.

Legislation should establish specific privacy safeguards to counter the serious threats to privacy posed by both RFID and GPS technology, particularly in the wake of HIMs being developed and deployed. Still, such legislation should also be comprehensible and flexible enough, and thus applicable to location information regardless of the technology (system, device, etc.) used, and to all entities and services that generate or require access to location information. With a flexible approach, LBS, location-aware applications and human tracking activities are broadly covered in an increasing location-aware world. Nevertheless, the legal rules for HIMs will need to be particularly more restrictive and precise than, for example, the use of a GPS tracking device by an employer in a company-owned vehicle to track their employees only during working hours (Herbert, 2006) or the use of a tracking device in a rented vehicle.

There have been a number of attempts to pass federal legislation regulating RFID. For instance, in 2004, the Opt Out of ID Chips Act[757] was introduced in the US House of Representatives, but ended up being unsuccessful. Although federal legislation on regulating RFID has suffered strong opposition, there are exceptional supporters within the US Congress.[758] There have also been attempts to pass legislation to regulate and protect the privacy of location information in general.[759]

Specific laws, regulations and adaptations in the legal framework are required to safeguard privacy against the threats posed by HIMs and other location-based services. These laws and regulations will not necessarily thwart innovation or commerce pertaining to RFID and GPS. On the contrary, specific laws and regulations could facilitate further development and deployment, ensuring the consumer confidence and trust necessary to open the market to the array of security and commercial benefits HIMs, and other RFID and GPS applications, can indeed provide.[760] Without specific federal regulations, both the private and public sector will face public opposition from all directions to the widespread deployment of HIMs. As RAND Europe equally asserts, the lack of specific mandates is an obstacle to the further deployment of RFID, suggesting that legislation, supported by public information campaigns, will address the privacy concerns and uncertainties of the general public towards RFID.[761] The uncertainties of the scope of data protection rules and the concept of personal data are also a main cause of regulatory uncertainty for industry players and investors in RFID applications, as revealed by the 2006 RFID public consultation in Europe.[762] Still, there are those who

---

757 H.R. 4673, 108th Congress (2004).

758 US Senator Patrick Leahy, a consistent defender of privacy, has persistently warned that RFID technology must be federally regulated and has called for congressional hearings on the technology. see Remarks of US Senator Leahy, "The Dawn of Micro Monitoring: Its Promise, and Its Challenges to Privacy and Security," Conference On "Video Surveillance: Legal And Technological Challenges", Georgetown University Law Center, 23 March 2004, available at: http://leahy.senate.gov/press/200403/032304.html

759 see S.1164, The Location Privacy Protection Act of 2001, Section 2, introduced unsuccessfully by former US Senator John Edwards during the 107th session of Congress.

760 I sent an email to VeriChip's VP for Investor Relations along those lines and inquired about the company's views and suggestions for potential legislation. Unfortunately, but not surprisingly, I never received a reply.

761 see Anna-Marie Wilamovska, et al. *Study on the requirements and options for RFID applications in healthcare*, RAND Europe (2008), Prepared for the Directorate General Information Society and Media of the European Commission, pp. 54-56.

762 SEC(2007)312, Results of the online consultation on future RFID technology policy.

argue that additional laws could dampen the innovation of new technologies. But, of course this depends on the specific content of those laws.

With the use of RFID and GPS to potentially track and record the movements of people and the consequential threats to privacy in public, the moment is now more than ever to address privacy out in public. As Ramesh (1997) declares, with regards to HIMs, "[t]he time to prevent grievous intrusion into personal privacy by enacting appropriate legislative safeguards is now, rather when it is too late".[763]

Embedding physical objects with RFID tags and the growth of IoT also requires specific legislation, but RFID applications involving individuals, in particular, requires special attention. While state level legislation that addresses RFID/GPS implants and human tracking is a good start, Federal legislation is ideal. Federal laws regulating HIMs and government access to location information would prevent differing state laws. Moreover, the privacy and civil liberty concerns pertaining to HIMs and location information are naturally inter-state issues as people travel across state lines. In any case, as Garfinkel et al. (2005) similarly propose, the law must apply the core principles of privacy protection to RFID systems, which is equally true for both RFID and GPS implants.

7.10.1 Consent

First and foremost, based on the principle of consent, and the general understanding concerning the autonomy of individuals, a Federal law, more comprehensive than the state laws of Wisconsin, North Dakota and California, must explicitly prohibit any private or public entity from mandating or requiring an individual to have a HIM implanted or any other foreseeable tracking or identification mechanism instilled for whatever reason, albeit with certain exceptions. Although consent implies that an individual equally has the right to withdraw his or her consent, the law must also specifically guarantee the right to request the HIM to be temporarily deactivated (if possible) or permanently removed.

The implantation of HIMs should not only at be voluntary (with certain exceptions), but should also never be a condition of exercising another right, including, but not limited to, the right to receive welfare or social security benefits, to work, to vote, to open a bank account, to conduct a commercial transaction, to travel, to take out insurance, to receive medical treatment or to be granted physical access to public or semi-public spaces and, with certain exceptions (see below), government-managed buildings. Hospitals must be prohibited from requiring newly born children to be im-

---

763 see Ramesh, Elaine M. *Time Enough? Consequences of Human Microchip Implantation*, Franklin Pierce Law Center (1997), available at: http://www.fplc.edu/risk/vol8/fall/ramesh.htm

planted. Moreover, any individual who consents to be implanted with a HIM, or any other identification or tracking device, must be at least 18 years of age, as Katherine Albrecht equally advocates.[764] But, parents (or legal guardians) may give their consent for their minor children to be implanted.

No individual should be discriminated against by any entity simply because they refuse to have a HIM implanted (or to be tracked by any other device for that matter) nor favored in any way simply because they consented to have a HIM implanted, as advocated by Katherine Albrecht, the Director of CASPIAN, a consumer privacy organization, in her legislative proposals concerning HIMs.[765] Equally, as Spivey (2005) asserts, insurance companies should be prohibited from offering incentives, such as a price reduction or other advantages, in return for their consent to be implanted with a HIM.[766] Any other incentive, discount, or other program that favors implantees must also be prohibited. On the other hand, individuals should equally not be discriminated against for consenting to have a HIM implanted.

Consent, however, may not always be appropriate or required, and may even be at times contrary to the public good and needs of society. Extremely narrow exceptions may apply to convicted violent criminals and the worst sex offenders, where relevant in the vital interest of public security. These individuals could potentially be compelled by the Government to be implanted with a HIM as a condition of parole, subject to Eighth Amendment considerations regarding the prohibition of cruel and inhuman punishment and due process considerations embodied under the Fourteenth Amendment. While Herbert (2006) argues that the Thirteenth Amendment of the US Constitution, which prohibits slavery or forced servitude, could also serve as a basis for prohibiting any mandatory implantation, by comparing mandatory implantation to slavery, there is indeed an exception for the punishment of a crime. Nonetheless, only courts should decide, in accordance with the law, which violent criminal should be compelled to be implanted with a HIM, and not the police nor any other law enforcement agency. Moreover, the basis of the decision should be strictly based on individualized assessments of danger, as opposed to simply mandating, for example, that all sex offenders be implanted, in order to completely avoid legal challenges, as Hinson (2008) argues with

---

764 see Katherine Albrecht's Bodily Integrity Act, available at: http://www.antichips.com/anti-chipping-bill-v07-numbered.pdf

765 see Katherine Albrecht's Bodily Integrity Act, available at: http://www.antichips.com/anti-chipping-bill-v07-numbered.pdf

766 see Spivey, Crystal. *Breathing New Life Into HIPAA's UHID – Is The FDA's Green Light To The VeriChip™ The Prince Charming Sleeping Beauty Has Been Waiting For?* (9 DePaul Journal of Health Care Law, 2005-06), pp. 1317-1342, at 1340.

regards to GPS bracelets. Once the conditions of parole are fully satisfied, the RFID or GPS implant in a convicted violent criminal or sex offender may be removed, if requested by the qualified parolee and equally approved by a court of law.

In addition, certain government employees, which require the highest-level of security, may perhaps reasonably be compelled to be implanted with a HIM as a condition of employment. However, they too must have the right to request the immediate removal of the HIM, if they have resigned or their employment contract has terminated or they have been dismissed. On the other hand, in no circumstances whatsoever, may private entities compel an individual to be implanted.

Any application that removes or diminishes an individual's anonymity with regards to RFID technology must also be prohibited,[767] unless the person concerned gives his or her express consent. Accordingly, the law must prohibit the coupling of the unique ID number of a HIM or any other RFID microchip to information associated with credit or debit cards and any personal information, including name, address, date of birth, telephone number and social security number, unless the person concerned expressly consents otherwise. Equally, the type of information associated with an RFID implant should be at the discretion of the implantee concerned, but narrow exceptions may apply to certain convicted violent criminals and sex offenders.

A person's consent to collect location information through their HIM may also entail the permission to store it for a certain period of time, since that occurs automatically. However, granting permission to collect and temporarily store location information does not entail the permission to disclose it to third parties, without additional explicit permission/consent to do so. The opt-in standard of consent alone must be mandated for the processing or disclosing of location information, lawfully collected and retained through HIMs, or any other RFID tag and/or PLD and/or location-aware device, on each separate occasion. Opt-in consent will endow implantees an opportunity to decide whether or not to allow their location information to be disclosed, essentially returning, for the most part, their ability to control what others may know about them. The opt-in standard of consent in the US is customary. As the FCC points out, most privacy laws in the US "do not employ an opt-out approach but rather require an individual's explicit consent before private information is disclosed or employed for secondary purposes".[768] HIM service providers, data controllers and any other provider of personal tracking or LBS must maintain a record of the opt-in consent and the details of any disclosure of location information, including the name of the third party and the specific purpose of the disclosure. The opt-

---

[767] see FTC staff report on RFID, p. 20.

[768] Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22, 13 March 2007, p. 26.

in consent must also be explicit and should be invalid if the data subject is not genuinely informed of the purpose(s) of the disclosure (see section 7.10.7).

Similar to the exceptions found in the ECPA, exceptions to the opt-in consent rule, with regards to the disclosing or processing of an implantee's location information, may include the reasonable belief that the disclosure is necessary for emergency response purposes, the fact that the person concerned is knowingly missing or has been kidnapped, the need to execute contractual obligations or the need to comply with lawful requests from law enforcement agencies in possession of a warrant.

7.10.2 Proportionality

The non-consensual based implantation of HIMs must only be permitted if the reasons for doing so are legitimate and proportionate in a democratic and free society. If a less intrusive alternative to HIMs is available, which accomplishes similar objectives and provides similar security benefits, then perhaps that alternative should be used instead. But, as explained earlier, a true alternative to HIMs is not really available at the moment.

Moreover, the quantity and scope of the location information collected and any other personal data associated with HIMs, or any other PLD or location-aware device for that matter, should be in line with the objectives and purposes for which the data was collected in the first place, as specified, for example, in a HIM purpose declaration attached to a standard or tailor-made service provider agreement. No more data than is required to fulfill the specified purposes should be collected and/or linked to the HIM, in accordance with both the *principle of proportionality* and the *principle of data minimization*.

7.10.3 Purpose specification

Those individuals who have consented to have a HIM implanted or have been lawfully compelled to do so, do not simply forfeit their right to privacy and should nonetheless enjoy certain privacy protections and legal safeguards.

The law must prohibit any entity from accessing or monitoring the location information of a person implanted with a HIM, or in any way in possession of a locating/tracking device or embedded RFID tag (i.e. the data subject), outside the designated area and/or scope and specified purpose the same individual has given his/her opt-in consent to have his/her movements to be tracked, such as a secure area or office space, regardless if he/she is traveling in public and especially when he/she is off-duty. Certain exceptions may apply to law enforcement agencies with a proper warrant.

A HIM purpose declaration/end-user agreement/service contract can serve as the legal, as opposed to technological, means of providing not just the opt-in consent, but the basis for any private legal action against a data controller who intentionally collects, monitors or accesses the location information of an implantee beyond the specified and legitimate purposes agreed upon. The purpose declaration can be included in a standard service provider agreement/service contract, binding all relevant data controllers, service providers and any other applicable party, taking into account the relevant laws/regulations. With regards to RFID implantees, the purpose declaration, as the EC similarly recommends for other RFID applications, should specify which data is collected, which association, if any, from the RFID tag to personal data is made, and what the possible privacy risks are.[769]

However, as the EU's Article 29 Working Party points out, "the principle of purpose limitation may be more difficult to apply and to control",[770] without solving the drawbacks of RFID interoperability and ensuring that only authorized readers can read RFID tags.[771] Moreover, if RFID implants are to serve as means of identification for private individuals, then the implants should only respond to trusted RFID readers, in conformity with the "Law of Directed Identity".[772] Where necessary, human-centric RFID systems should provide for mutual authentication, whereby only authorized readers can read the RFID microchips.[773] As proposed by the Article 29 Working Party, one way is to limit the initial query of readers to target only relevant RFID tags in the first place, thereby realizing the collection limitation principle at the protocol level.[774] Similarly, Floerkemeier et al. (2005) proposed that the fair information principles (FIPs) can be incorporated at the "reader-to-tag protocol level", whereby they are implemented

---

769 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification "RFID Privacy, Data Protection and Security Recommendation" {C(2009) 3200 final}.

770 see Working document on data protection issues related to RFID technology, WP 105, 19 January 2005.

771 *Ibid.*

772 The Law of Directed Identity is law number four of the seven Laws of Identity, which were formulated by Kim Cameron, together with other experts online, in order to improve trust in the security and privacy of Internet use. The Laws of Identity are available at: http://www.identityblog.com

773 see Article 29 Working Party, Working document on data protection issues related to RFID technology, WP 105, 19 January, 2005.

774 *Ibid.*, p. 6.

directly at the point of data collection, rather than afterwards,[775] similar to how W3C's Platform for Privacy Preferences Project (P3P) integrated machine readable privacy policies into the browser-to-server protocol, allowing for a user's web browser to automatically read the privacy policy of a website, compare it with the user's preferences, and automatically take action on behalf of the user by either permitting or blocking the transfer of his/her personal data.[776] The incorporation of the FIPs directly into the underlying protocol could also better enable both consumers (data subjects) and data controllers to enforce the corresponding regulations.[777]

In the case of RFID implantees, they could potentially set their privacy preferences, whereby only RFID readers that match these preferences would be allowed to read the RFID implant. As the managers of the RFID Ecosystem[778] proposed with regards to non-implantable RFID tags, RFID implantees could similarly specify rules that describe which TREs should be accessible to which users and which TREs should be deleted automatically (see Rastogi et al., 2007). But, as the managers of the project also point out, this could limit the utility of the system (Ibid.). Juels and Brainard (2004) had earlier suggested a similar idea, which they termed "soft blocking", whereby the data subjects also set their privacy preferences and the RFID readers are designed to comply accordingly. Alternatively, Ayoade et al. (2007) proposed a system called an Authentication Processing Framework (APF) that can potentially authenticate readers before they can access the RFID tag's information in a specific system. The idea is that RFID tags and readers are registered on a database, which then authenticates the readers before being allowed to read the information contained on the registered RFID tags.

The Internet Engineering Task Force (IETF) (see Schulzrinne, H. et al., 2009) has also proposed a protocol-independent model for access to location information. The model includes a Location Generator (LG) that determines location information, a Location Server (LS) that authorizes access to location information, a Location Recipient (LR) that requests and receives location information, and a Rule Maker (RM) that

---

775 see Floerkemeier, Christian., et al. *Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols*, Distributed Systems Group, Swiss Federal Institute of Technology (2005), p. 1, available at: http://www.vs.inf.ethz.ch/res/papers/floerkem2004-rfidprivacy.pdf

776 *Ibid.* p. 2.

777 *Ibid.*

778 The RFID Ecosystem is a building-wide RFID project at the University of Washington using thousands of tags and hundreds of readers. The purpose of the project is to demonstrate the risks, benefits, and challenges of user-centered RFID systems and to propose technological solutions to minimizing privacy loss. see RFID Ecosystem, available at: http://rfid.cs.washington.edu/index.html

writes authorization policies. An authorization policy is a set of rules that regulates an entity's activities with respect to privacy-sensitive information, in this case location information. The rule set allows the user to restrict the retention and to enforce access restrictions on location information, including prohibiting any dissemination to certain individuals, during particular times or when in a specific location. The model can also enable the user to control how long the LR may retain the location information and further distribute it.[779]

The 'Internet of Persons' may equally be based on a system whereby the Internet is leveraged, but access to the location information of any RFID/GPS implantee is restricted to those who are registered for the service, logged-in with a username and password and have explicit permission from the implantee concerned to access that information. Therefore, although the means of finding and sharing location information may be available via the Internet, the actual ability to share that information is managed by the implantee.

In addition, the technological, as opposed to legal, means of restricting the tracking of an individual's movements beyond the area in which they have given consent to be tracked may also consist of setting up a so-called "digital territory".[780] In this case, a "digital territory" is simultaneously applied to both the physical and virtual space (Beslay and Hakala, 2007). With regards to HIMs, once an implantee moves outside the designated "digital territory", for instance, the 'bridge' that merges the physical space with the virtual space (*Ibid*.) is temporarily severed until the implantee re-enters into the designated "digital territory".

While obfuscation and anonymity are somewhat suitable technical solutions for other LBS or location-aware applications, these approaches may not be completely suitable for HIMs, since the purpose of HIMs is to in fact accurately identify and track the implantee, albeit under certain conditions, in accordance with the proposed laws and as specified within the implantee's service provider agreement and/or HIM purpose declaration. However, the location information should be rendered anonymous once it is no longer required for the specified purposes it was collected and retained in the first place. Nonetheless, anonymity may be useful to hide the location of individuals in certain areas or during certain time periods. Moreover, as the EC recommends as an

---

779 see Schulzrinne, H. et al., "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location-Information", The Internet Engineering Task Force, Internet Draft, February 2009, available at: http://www.ietf.org/id/draft-ietf-geopriv-policy-21.txt

780 For further discussion, see, for example, Beslay, Laurent., and H. Hakala. "Digital Territory: bubbles" in Paul T. Kidd (ed.) *European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society* (Cheshire Henbury, 2007).

option, a RFID tag could use pseudonyms, whereby the tag can respond with different ID numbers, but the authorized back-office of the system is able to match the different ID numbers to the same RFID tag, whereas this would be much more difficult for an unauthorized party.[781]

7.10.4 Use limitation

While RFID implants are associated with data controllers, they do not necessarily require a wireless service provider. GPS implants, on the other hand, require a service provider, as a result of the required use of a cellular network and the desired storage of the location information. As a service to the customer (i.e. the GPS implantee or data subject), the location information generated by GPS implants should be stored for a certain period of time, in case law enforcement agencies, for instance, need to locate the implantee if he/she is either kidnapped or goes missing.

However, any location information generated by both RFID and GPS implants should be deleted or at least rendered anonymous once it is no longer required for the specified purposes (for example, after 7 days) or should only be retained, in its identifiable form, for a period of time proportionate to the purposes for which it was collected, unless otherwise authorized to be retained for a greater period of time by the implantees concerned.

In addition, the location information should only be retained as long as the service provider or data controller requires it in order to provide the particular services that the implantees have authorized. As the Data Privacy and Integrity Advisory Committee of the DHS similarly proposes, in order to avoid 'function creep',[782] the data collected by

---

781 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification "RFID Privacy, Data Protection and Security Recommendation" {C(2009) 3200 final}

782 The term "function creep" refers to any additional use of personal data beyond the specified purposes for which the personal data was permitted to be collected in the first place. Function creep occurs when "personal data collected for one specific purpose and in order to fulfill one function, are used for completely different purposes, which are totally unrelated to the ones for which they were initially collected". Tzanou, Maria. *The EU as an Emerging Surveillance Society: The Function Creep Case Study and Challenges to Privacy and Data Protection* (4 Vienna Online Journal on International Constitutional Law, 2010), p. 421. Function creep "constitutes a breach to the purpose limitation principle" (Ibid.)

RFID technology should only be used for the stated objective and kept "for only as long as necessary to meet the original objective for which it was collected".[783]

A number of difficulties may still arise in enforcing a prohibition on reading RFID implants or other RFID tags on a person without the knowledge and/or permission of that person. To serve as an additional deterrent, the law could potentially also mandate that all RFID readers manufactured for sale in the US make a sound audible within several feet from the reader whenever a HIM or other RFID tag is read, in order to better alert individuals that a RFID tag/microchip has been read. It is already common for RFID readers to make a sound when used in access control systems, such as those found at places of business. Such a measure would be similar to the bill introduced by US Congressman Peter King, which aims to require cell phones containing digital cameras to make a sound when a photo is taken using them, in order to inform individuals that a photo has been taken nearby.[784]

The law should also prohibit the use of read-write tags for the manufacture of HIMs and mandate that HIMs remain passive and are manufactured from read-only or WORM tags. In the case of HIMs manufactured from read-only tags, the data stored on the HIMs should be limited to the unique ID number. In the case of HIMs manufactured from WORM tags, the implantee may request additional information, such as date of birth, in addition to the unique ID number, to be stored on the HIM. While there is no real need for the RFID implant to have much more than the unique ID number stored, RFID implantees themselves should alone have the final say. Nevertheless, it is recommended that only the unique ID number be stored on the RFID implant, as any storage of additional personal data would significantly increase the threat to privacy and data security risk.

Furthermore, the law should also regulate the procedure for implanting HIMs. While the law cannot necessarily prohibit someone from implanting a RFID implant by themselves, it can prohibit the business of implanting HIMs at any place other than licensed clinics, including tattoo or piercing parlors. Moreover, there should be an established protocol regulating not just the implantation of HIMs, but also their removal. A standard waiver agreement should also be adopted and used by all the licensed clinics.

---

783 The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, p. 11, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

784 see H.R. 414, entitled "Camera Phone Predator Alert Act", introduced 9 January 2009. The text of this proposal, however, is already outdated since other devices, such as Apple's iPods and iPads, now have integrated cameras. In Japan, camera phones are already required to make a shutter sound when used.

7.10.5 Enforcement, accountability and redress

Any individual who coerces or compels or otherwise requires another individual to be implanted with a HIM, or in any way implants a HIM in a person without that person's consent, should be subject to criminal penalties. Each violation should be considered a felony, rather than a misdemeanor offense, since it is a serious violation of bodily integrity and a form of physical assault.

Anyone implanted with a RFID implant, or in any way in possession of a RFID tag, is still potentially broadcasting their identity to anyone or anything with a RFID reader several centimeters to a couple feet away. The law should, therefore, criminalize the eavesdropping of RFID implants, without that person's explicit consent, unless done so by law enforcement agencies, in accordance with the law. Accordingly, RFID data transmissions concerning individuals should explicitly be deemed a form of electronic communication, thereby causing the ECPA to apply.[785]

Similarly, the monitoring or interception of the signals of a GPS implant (or any other GPD device) without the knowledge and consent of that person, unless done so by law enforcement agents (under certain circumstances), must also be prohibited.

In order to criminalize the unauthorized interception of the radio signals broadcasted from GPS implants, the ECPA needs to be amended to remove the exception concerning tracking devices (Karim, 2004) and/or the broadcasting of location information, in any form or from any (electronic) source, should also be deemed a form of electronic communication.

It is also critical that statutory law explicitly regards GPS tracking (i.e. electronic tracking) as a search and ensures that the protections of the Fourth Amendment apply (Hutchins, 2007).[786] Equally, when law enforcement agents seek to access or monitor the location information stored on the databases of service providers, for example, in order to conduct an investigation/gather criminal intelligence, statutory law should also specify that a warrant is needed, thereby applying the protections of the Fourth Amendment (Hutchins, 2007) and adjusting the Federal Rules of Criminal Procedure.[787] How-

---

[785] see Levary, Reuven R., et al. "RFID, Electronic Eavesdropping and the Law" (RFID Journal, 14 February 2005), available at: http://www.rfidjournal.com/article/articleview/1401/1/128/

[786] see Hutchins, Renee. *Tied Up in Knotts? GPS Technology and the Fourth Amendment* (UCLA Law Review, Vol. 55, No. 1, 2007), pp. 409-465.

[787] see S.1212, titled "Geolocation and Privacy Surveillance (GPS) Act", introduced 15 June 2011 in Senate by Senator Ron Wyden (D-OR), Sec. 2602. The bill failed to become law.

ever, certain exceptions may apply, in line with existing Federal wiretapping laws.[788] Warrants, for example, should not be required if the individual has presumably been kidnapped or has specifically requested assistance.[789] The law must also explicitly clarify, once and for all, that probable cause alone is required to obtain a warrant or court order to track the movements of an individual and/or to gain access to personally-identifiable location information, based on the belief that the concerned person has committed, is committing or will commit a crime.[790] If deemed necessary or helpful at the initial stages, a dedicated and independent oversight committee could supervise the number of such warrants sought after and obtained, while also ensuring the legal requirements are being fulfilled. The statutory laws, however, should not alter existing legislation on the authority of intelligence agencies to conduct electronic surveillance.[791]

With regards to the private sector, the law must also hold HIM service providers and any other provider of personal locating services, or controller/processor of location information, accountable, if they gather and/or disclose an individual's location information to any private third party without the explicit permission of the person concerned and/or in violation of a standard service provider agreement/HIM purpose declaration. The right to private action against the service providers (or private sector data controllers/processors) should, therefore, also be afforded to implantees who have suffered damages as a result of the unlawful collection and/or disclosure or processing activities.

Accordingly, tort law relevant to privacy intrusion must also be re-defined, whereby location information may pertain to one's private affairs and the disclosure of location information may constitute an invasion upon one's seclusion. This will enable an adversely affected individual, whose location information was unlawfully disclosed/processed, to bring private legal action against any violator and to potentially receive compensation. In order to re-define tort law and permit invasions of privacy in public places to be actionable, McClurg (1995) proposes that the tort of seclusion should take into account, among other factors, the "magnitude of the intrusion, including the duration, extent, and the means of intrusion" (McClurg, 1995).

In order to ensure that the service providers/data controllers are not capable of potentially evading US law, the databases and web-servers associated with US-based

---

788 see 18 USC §2511; S.1212, titled "Geolocation and Privacy Surveillance (GPS) Act".

789 S.1212, titled "Geolocation and Privacy Surveillance (GPS) Act", Sec. 2604.

790 see S.854, titled "The Electronic Rights for the 21st Century Act", Sec. 102, introduced in the US Senate by Senator Patrick Leahy in 1999. The bill failed to become law.

791 S.1212, titled "Geolocation and Privacy Surveillance (GPS) Act".

HIM service providers should be prohibited from being placed in locations outside the jurisdiction of the US.

7.10.6 Access and participation

The law must mandate the ability for implantees to request access to all the information lawfully stored in databases associated with their HIM and be able to delete or correct any such information, at least up to the point permitted so by the service provider agreement and HIM purpose declaration, where applicable.

In the case of implantees under the age of 13, in accordance with the Children's Online Privacy Protection Act (COPPA), the parents or guardians must have the right to access all the information associated with their child's HIM.

Implantees should also have the ability to manage and control how their location information is shared and with whom. As the managers of the RFID Ecosystem proposed and later demonstrated, data subjects can use a web interface to control/manage all the location information (and other data) associated with RFID tags.[792] In the case of RFID implants, implantees should also be able to set privacy preferences, as explained previously in section 7.10.3. The sharing of location information associated with GPS implants could equally be managed online using the protocol-independent model proposed by the IETF.[793] A similar system has already been created by Useful Networks and applied to their *sniff* (Social Network Integrated Friend Finder) location-aware application for smartphones.[794]

Another potential technological solution, albeit farfetched, would be to use RFID microchips with an on/off switch for RFID implants, giving greater control to the implantee. The idea is based on the so-called "right to the silence of the chip". However, knowing when the implant is on or off is another matter.[795] Perhaps, an on/off switch

---

[792] see Welbourne, E., et al. *Challenges for Pervasive RFID-based Infrastructure*, PERTEC 2007, Workshop on Pervasive RFID/NFC Technology and Applications, 19 March 2007, available at: http://rfid.cs.washington.edu/images/welbourne-pertec-07.pdf

[793] Schulzrinne, H. et al., "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", The Internet Engineering Task Force, Internet Draft, February 2009, available at: http://www.ietf.org/id/draft-ietf-geopriv-policy-21.txt

[794] Useful Networks, at: http://www.useful-networks.com/site/products/community/

[795] see Paturi, Prasad. "Switching Off Credit Card Fraud" (RFID Journal, 12 September 2005), available at: http://www.rfidjournal.com/article/articleview/1843/1/82/

could equally be used for GPS implants. A more realistic solution, on the other hand, is the RFID Guardian, developed by a group of researchers, coordinated by Melanie Rieback, from Vrije University Amsterdam. The prototype RFID Guardian is battery-powered and performs 2-way RFID communications, acting both like an RFID reader and an RFID tag. The tool could potentially be an implantee's technological means for detecting the nearby presence of RFID readers, jamming an RFID reader's capability of reading their RFID implant and for providing implantees the ability to control access and authentication.[796] Ideally and for practical purposes, the RFID Guardian will need to be small enough in order to be embedded, for example, within smartphones or other mobile computing devices.[797] The development of radio-reflective shields worn over the area of the body where the implant is located, however, is likely an easier non-technological alternative to the RFID Guardian or on/off switch.

7.10.7 Notice and awareness

As the Data Privacy and Integrity Advisory Committee of the DHS proposed, "[i]ndividuals should know how and why RFID technology is being used, including what information is being collected and by whom".[798] RFID readers in public space must be clearly visible and not covertly hidden. Standardized and generic icons or emblems must also be clearly visible in order to indicate that RFID readers are present nearby[799] or inform individuals that they are entering into a "RFID-read zone" similar to the way the presence of CCTV cameras is indicated.[800] The responsibility of ensuring that this notice is clearly present, accurate and appropriate should fall on both the data controllers and the entity, whether public or private, that has permitted the installation of RFID readers in the specific public space. The signs must accurately reveal the identity and contact information of the data controllers. The signs could also briefly explain the limited purpose and extent of the data collection.

---

796 For more information on the RFID Guardian project/device, see: http://www.rfidguardian.org

797 *Ibid.*

798 The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, p. 11, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

799 *Ibid.*

800 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification "RFID Privacy, Data Protection and Security Recommendation" {C(2009) 3200 final}.

Preferably, a "universal accepted symbol" should be established, as proposed, albeit unsuccessfully, in a New Hampshire bill.[801] A standard gold icon can already be found on passports from around the world indicating that the passport is embedded with a RFID microchip, but this is not suitable for RFID readers in public spaces. The Association for Automatic Identification and Mobility (AIM) has already developed a RFID emblem free for use, but it is nonetheless still the intellectual property of AIM. An ISO RFID emblem is currently in development. Once adopted, the ISO RFID emblem would be suitable for use in the US and could substitute the need for the US to create and adopt its own emblem. The ISO RFID emblem will contain the data controller's name and contact information.[802]

The implantees should, once again, also be informed via the standardized HIM purpose declaration/end-user agreement/service contract on the purposes of the collection and processing of their personal data.

In addition, the concerned implantees should be notified, where possible, of any unauthorized access and/or disclosure of the location information or other personal information associated with their HIM or of any security breach concerning such information.[803] Implantees should also have the option of being notified of any authorized access of their location information and should have the option of receiving recurring notices on who has been authorized to access this information, obviously with exception to legitimate law enforcement activities.

7.10.8 Security

As the DHS Privacy Office Annual Report to Congress (2007-2008) recommended, several concepts and approaches reflected in the OECD Guidelines for the Security of Information Systems and Networks could be adapted to support the implementation of the OECD Privacy Guidelines.

Any RFID system, especially when involving human beings, as opposed to physical objects or animals, should be carefully designed to prevent the risk of various attacks, such as spoofing or cloning, encryption key cracking and eavesdropping or unauthorized

---

801 N.H. H.R. 203 (defining "universally accepted symbol" as "a graphical system designed to provide a standard way to show the presence of an RFID transponder, its frequency, and data structure").

802 Europe, however, is in the process of creating its own RFID emblem.

803 US Senator Patrick Leahy introduced S.1490, titled "The Personal Data Privacy and Security Act of 2009", which provided for a national standard for data breach notification.

interception. As one commenter urged during the FTC workshop on RFID, "[a]uthorization, authentication, and encryption for RFID . . . [should] be developed and applied on a routine basis to ensure trustworthiness of RFID radio communications".[804] Therefore, RFID implants for human use must no longer be based on the ISO11784/85 standard.

Accordingly, the law should mandate that RFID implants incorporate cryptographic functionalities and use symmetric encryption with a minimum key size of 128 bits, which requires the application of the Advanced Encryption Standard (AES) (Feldhofer et al., 2004). A 128-bit encryption key requires over fifty years to crack with the capabilities of modern computers and the data contained on a RFID tag is basically useless if the encryption key cannot be cracked.[805] Alternatively, instead of using key encryption, RFID implants could adopt Verayo's authentication solution called "Physical Unclonable Functions" (PUFs), which is comprised of tiny, low power circuit primitives that exploit the unlimited, unique variations of the electrical behavior of each silicon chip.[806]

Moreover, since HIMs are a component of an information network, the law must equally mandate that the network itself and the databases that store location information and the personal data associated with any type of HIM (or any other PLD) are equally secure.

A public authority (or authorized third party certification body) can certify that manufacturers of HIMs, data controllers and service providers are meeting these standards. A similar option was recommended by the EC for RFID applications.[807] Any relevant party that fails to implement these security measures may then be held liable.

Accordingly, official RFID security guidelines will be helpful. The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik or BSI), for example, has already developed Technical Guidelines on how to implement RFID applications/systems in a secure, but functional way, in order to better ensure the privacy of the associated personal data. The BSI recommended that these Technical Guidelines be incorporated into the pan-European PIA Framework for RFID applica-

---

804 FTC staff report on RFID, p. 20.

805 see Williams, Lorraine C. *A Discussion of the Importance of Key Length in Symmetric and Asymmetric Cryptography*, SANS Institute, GIAC practical repository, 2002, p. 3, available at: http://www.giac.org/certified_professionals/practicals/gsec/0848.php

806 see Verayo, available at: http://www.verayo.com/technology.html

807 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, "RFID Privacy, Data Protection and Security Recommendation" {C(2009) 3200 final}, 5.2.3., Option I.c.

tions.[808] The BSI also plans to offer a certification service that certifies the adequate implementation of these Technical Guidelines.

7.10.9 Privacy Impact Assessment

In addition, the US Government should also formally adopt a comprehensive RFID PIA framework[809] that is similar (though not identical) to the European version.[810] The PIA should be compulsory for any RFID application that involves personal data, regardless whether that data is held by public or private entities.[811]

Accordingly, the law should be altered to require PIAs for both public and private entities, and the requirement should additionally also be relevant for all instances where data processing activities may pose threats to the privacy of data subjects.

Like the EU's RFID PIA framework, the US framework should include the requirement to specifically carry out an *ex-ante* assessment/evaluation of the data protection risks and threats to privacy and, based on the assessment, to identify and evaluate measures to counter, mitigate, prevent and/or eliminate these risks and threats.[812] Furthermore, similar to the EU's PIA framework, the US PIA framework could be primarily

---

808 The BSI presented this recommendation during the 3rd meeting of the RFID Recommendation Implementation Informal Working Group at the EC. During the meeting, the establishment of the European RFID PIA was discussed. Industry associations, standardization bodies, public authorities and a representative from the Article 29 Working Party were present at the meeting.

809 In US law, a PIA is described as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks" (E-Government Act of 2002, Section 208).

810 see Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, available at: http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf

811 As a step further, PIAs should be mandatory before the deployment of any IT system which involves personal data, regardless of the sector (see Cannataci, 2011). Cannataci also argues that this may be possible in the EU by 2015, as part of the EC's wider review of data protection policy options (2011, p. 180).

812 For further discussion, see Cannataci, Joseph A. *Recent developments in privacy and healthcare: Different paths for RFID in Europe and North America?* (International Journal of RF Technologies, Volume 2, 2010/2011), pp. 173-187.

developed by significant industry players/stakeholders and reviewed and approved by regulators.[813]

However, contrary to the EU's RFID PIA, the US framework should also be applicable to the manufacturers/developers of RFID infrastructures/systems, and not only RFID application service providers. Therefore, a PIA should be carried out in both stages – before a RFID infrastructure/system is developed and deployed, and before a RFID application/service is developed and deployed. Accordingly, PIAs should be required for both IT service providers *and* manufacturers/developers.

7.10.10 Definitions

The definition of location information would need to be formulated in a way to cover not only the extensively more intrusive location information HIMs are capable of generating, but to ensure, as far as possible, technological neutrality for protecting the privacy of the movements of individuals overall. Instead of the limited scope of location information to telephones, cell phones and computers, as understood within the Telecom Act (and perhaps also by Article 2 of the ePrivacy Directive[814]), the definition should read as follows:

> Location information shall either mean the precise physical location of an identifiable individual at any given moment and/or any collection of the daily movements of that individual tracked over any given period of time, using any means, whether in public or private areas, and shall include, but not limited to, geographic coordinates, street addresses, buildings, landmarks and tag read events, where relevant.

Only then will the privacy of location information or 'location privacy' have real meaning and effect in a court of law in the US.

The definition of a tracking device should also be expanded to include not just electronic devices, such as RFID microchips and GPS devices, but any other automatic iden-

---

[813] see Spiekermann, Sarah. "The RFID PIA – developed by industry, agreed by regulators" in David Wright and Paul de Hert (eds.), Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy (Springer, 2012).

[814] Article 2(c) of the ePrivacy Directive defines location data as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".

tification technology, which permits the tracking of the movement of a person or object.[815] Other automatic identification technologies include Somark's ID system, which is based on "a biocompatible ink tattoo with chipless RFID functionality"[816] and QR code (2D barcode) tattoos. This will allow the law to cover all existing, foreseeable and unforeseeable advancements in human tracking, as similarly pointed out by Albrecht.[817] Accordingly, the modified definition of a tracking device should read as follows:

> *A tracking device shall mean <u>any device, mechanism or system</u> which permits the tracking of the movement of an <u>individual and/or object carried by an individual</u>, either by storing and/or transmitting location information and/or transmitting the identity of an individual via any associated number, symbol, mark or other individual identifier.*

Cyberstalking/electronic tracking laws should be amended to eliminate the restriction that cyberstalking occurs only when the perpetrator threatens, harasses or annoys another person by means of a telecommunications device. This will allow for the prohibition of the use of any tracking device, including HIMs, or any other RFID microchip or GPS tracking device, for the unauthorized tracking of another person, unless done so by law enforcement agencies with a proper warrant.

The Identity Theft and Assumption Deterrence Act of 1998 should already clearly cover identity theft via RFID implants and, therefore, the legislation does not necessarily need to be amended to explicitly include the unique ID number of HIMs.

7.10.11 Constitutional and case law considerations

Above and beyond explicitly regulating HIMs and the use of the location information generated by them, US courts must begin to recognize accordingly that there is an increasing overlap between the private sphere and the public sphere and also that the physical world and the virtual world are gradually merging, as a result of the potential for Internet of Things, Internet of Persons and Ambient Intelligence/ubiquitous com-

---

815 see Katherine's Albrecht's AntiChips website, available at: http://www.antichips.com

816 Somark, available at: http://www.somarkinnovations.com

817 see Katherine's Albrecht's AntiChips website, available at: http://www.antichips.com

puting. Only then will the desired rules concerning HIMs, for instance, and the definition and adequate protection of location information turn out to be legally feasible.

The law must first better accommodate for the fact that one's privacy can indeed be violated while out in public. The analysis of the Fourth Amendment by US courts must, therefore, shift the primary focus concerning the reasonable expectation of privacy from simply where the search is conducted to the nature, content and purpose of the collected information itself (Karim, 2004). Moreover, the reasonable expectation of privacy should rather be driven by the common understandings of the level of privacy society expects overall when out in public. Nissenbaum's "alternative account of privacy in terms of "contextual integrity"" (2004, p. 106) is equally relevant and may also be helpful for understanding the scope of privacy out in public and how it relates to public surveillance. In addition, the courts should also focus more on whether the loss of privacy is desirable or undesirable (Gavison, 1980). In any case, the reasonable expectation of privacy out in public should not be held hostage by the scale of the availability, deployment and use of PITs capable of mass public surveillance.

Regardless if individuals carry around a GPS-enabled smartphone, mobile phone or PLD or have an HIM implanted, it is probably fair to say that most people have a reasonable expectation that their movements or constant whereabouts in public should not be tracked or disclosed without their explicit knowledge and consent, unless done so by law enforcement agencies with a warrant backed by probable cause. In fact, the majority of people believe their movements and whereabouts should be afforded the protections of the Fourth Amendment, albeit to a certain extent. For example, as a survey conducted in California previously showed, 72% of respondents supported legal limits on law enforcement access to location information generated by mobile phones.[818]

Ultimately, courts should officially recognize the notion of 'public privacy', which also deserves protection in tort applications (McClurg, 1995). Stalking laws, as McClurg additionally points out, may already constitute the implied recognition of 'public privacy' (*Ibid*.).

Furthermore, given that the location information generated by RFID implants or constantly transmitted by GPS implants or GPS-enabled smartphones can also be self-incriminating, as Ramesh (1997) points out, the Fifth Amendment should be applied to this location information by categorizing its transmission as a 'communicative act'.[819]

---

[818] see King, Jennifer and Chris Jay Hoofnagle. *A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information* (18 April 2008), p. 8.

[819] see Ramesh, Elaine M. *Time Enough? Consequences of Human Microchip Implantation*, Franklin Pierce Law Center (1997), available at: http://www.fplc.edu/risk/vol8/fall/ramesh.htm.

7.10.12 The international dimension

As a matter of DHS policy, known as the "Mixed Use Policy", any personal information processed in connection with a 'mixed system'[820] by the DHS should be treated as if it were subject to the Privacy Act 1974, regardless of whether the information pertains to a US citizen, LPR, visitor, or alien.[821] Since implantees from foreign countries who travel to the US should enjoy the same privacy protection rights, the "Mixed Use Policy" should equally be applied to HIMs and any associated databases.

7.11 CONCLUDING REMARKS

RFID or GPS implants do not necessarily need to be banned, as there are public security and personal safety gains, commercial advantages and healthcare delivery benefits to them. Besides, a total ban on HIMs would be an extreme measure and would not necessarily stop with HIMs. Banning HIMs could call into question why other similar or related technologies are not equally banned. Moreover, as the use of RFID and GPS technology grows evermore rapidly, people will, more than likely, accept the existence of HIMs and recognize these benefits, especially if the deployment of HIMs is carried out legitimately and proportionally.

While the security and commercial gains of the widespread deployment and greater use of RFID and GPS technology should be welcomed, the US legal framework, in particular, lacks the appropriate laws to ensure that both the associated privacy threats and security risks are tackled accordingly. However, this is not just a policy or legal issue, but also a matter of technology. Tested technological solutions, mandated by law, are also required.

The establishment and implementation of the required legal and technological safeguards should both ensure that the prospective widespread deployment and use of HIMs, and other applications of RFID and GPS technology, does not erode privacy and personal freedom, while also ensuring that the benefits of RFID and GPS technology, whether security, health, social or commercial, are maintained.

---

820 A mixed system is a system that contains information on both US and non-US citizens.

821 see DHS Privacy Office memorandum, *Privacy Policy Guidance Memorandum Number 2007-1 ("Mixed Use Policy")*, issued on 19 January 2007.