19. THE INTERNET OF PEOPLE?
Reflections on the Future Regulation of Human-Implantable Radio Frequency Identification*

IAN KERR

I. RFID Technologies 337
  A. What Is an RFID? 337
  B. RFID Applications 339
  C. Human-Implantable RFIDs 341
II. The Current Regulatory Environment for RFID 343
  A. Communications 344
  B. Electronic Waste 344
  C. Health and Safety 345
  D. Privacy and Autonomy 347
III. The Internet of Things and the Not-So-Long Arm of the Law 353
IV. The Human-Machine Merger 354
V. The Internet of People 356

Convincing people to put computer chips in their bodies is a hard sell. Subcutaneous silicon has both the ozone smell of cyberpunk dystopia and the cornpone reek of the end-times Mark of the Beast.

. . . .

Still, for all its shortcomings, VeriChip's bold appearance on the public stage gives me a subcutaneous itch. I never imagined I'd want such a thing, but I'm seriously thinking about getting one. Not for the cumbersome medic-alert features or theatrical security clearances, but as the 21st century's first genuinely transgressive cyberpunk fashion statement.
—Bruce Sterling[1]

I remember sitting at the back of the Baja Beach Club in Barcelona's famous Olympic Port in July 2004 with twenty-five global law students on a "field trip" of sorts.

* This chapter emerged from ID Trail's 2006 Paris Workshop. The author wishes to extend his gratitude to Angela Long for her research assistance in preparation for the Workshop. A hearty thank-you, as well, to Latanya Sweeney, Jena McGill, David Matheson, Valerie Steeves, Carole Lucock, Jason Millar, and Hillary Young for the excellent suggestions for improvement that they so generously offered. Special thanks are owed to Katie Black for all of her extraordinary efforts and for the high quality of research assistance that she so regularly and reliably provides.

1. Bruce Sterling, "Go Ahead, Chip Me," *Wired Magazine*, October 2007, http://www.wired.com/wired/archive/13.10/posts.html?pg=7.

After paying for our meal, we were ushered into the VIP lounge to hear Baja's proprietor offer up a very strange sales pitch. In the weeks leading up to our visit, my class had studied the implications of emerging technologies on privacy and identity. Would my students seriously consider getting chipped? What did they think were the broader social implications of human-implantable radio frequency identification?

The proprietor's proposition was straightforward: become a VIP, get a VeriChip™, and you will not have to pay for drinks. Well, at least not one at a time. The 12 mm × 2 mm radio frequency identification (RFID) tag jammed into your triceps through a six-gauge needle might smart for a couple of weeks, but once implanted, it would enable an automated authentication scheme allowing easy access to the VIP lounge and a replenishable, cashless payment system for buying booze at the bar.

For most of my students, the allure was exactly the "transgressive cyberpunk fashion statement" described by Bruce Sterling at the outset of this chapter. Or, as Conrad Chase (the proprietor) put it to us that day in the VIP lounge, "the VIP chip takes body piercing to the next level." Numbed by an exponentially increasing array of new and emerging technologies introduced during the course of their short adult lives, my students predicted that this was yet another techno-fad doomed to the electronic trash-bin—the next "carbolic smoke ball."[2] I believed otherwise, and expressed my concern that chipping people might actually become a mainstream practice.

Only a few years later, with reported 2006 annual sales in the order of 1.7 million for human implantable chips and a projected increase through at least 2010,[3] Applied Digital Solutions Inc. seems to have found a way to make Bruce Sterling's hard sell easy, not just in nightclubs but in hospitals, too. The scheme is not much different from that of the Baja Beach Club. But instead of authenticating a patron's identity in order to link it to her bar tab, the implantable chip is linked to an electronic health record. As such, the chip enables the automated identification of incapacitated or disoriented individuals to facilitate health care delivery in the event of an emergency.

In this chapter, I examine some of the legal and ethical implications of human-implantable radio frequency identification (RFID). I commence Part I with a brief account of RFID technologies. In Part II, I examine the existing regulatory environment for RFID, suggesting in Part III that our current control and consent model of privacy and autonomy provides inadequate protection against an RFID-enabled Internet of things. In Part IV, I consider the broader implications of human-implantable RFIDs and their role in what I call the

2. Carbolic Smoke Ball Company Inc., "Carbolic Smoke Ball: Will Positively Cure," http://www.directly2u.co.uk/carbolic/index.htm.

3. Siobhan Morrissey, "Are Microchip Tags Safe?" *Time Magazine*, October 18, 2007, http://www.verichipcorp.com/news/1192716360.

"human-machine merger." I conclude in Part V by suggesting that, rather than giving up core principles and values just because they are in tension with RFID and other emerging technologies, we must (i) rethink the appropriate application of these principles, and (ii) determine whether there is sufficient justification for moving forward with human-implantable RFID, ubiquitous computing, and the Internet of things.

I. RFID TECHNOLOGIES

A. What Is an RFID?

RFID tags enable the remote and automatic identification of physical entities by way of radio signals that operate in the unlicensed part of the broadcast spectrum. RFID systems usually incorporate three main components: (i) a tag (transponder), which emits a unique identifier through radio waves; (ii) an interrogator (scanner), which receives the signal and identifies the object; and (iii) an associable database.[4]

Composed of a coupling element (the antenna) and an integrated circuit (also known as microchip), tags are classified as either passive or active depending on their power source requirements when emitting their identifying signal. Active tags rely on energy from a battery to power its antenna, giving it a long radio range. Passive tags do not require a power source, remaining dormant until activated by the proximate signal from an RFID scanner. It is the scanner's signal that powers the tag, enabling it to emit a radio signal of its own, though the radio range of a passive tag is thus shorter than an active tag. Passive tags, however, can be made smaller, more cheaply, and longer-lasting than their active counterparts.[5] Tag size also varies dramatically with tag memory and with speed and range of transmission. Active tags can be as large as a book, whereas the smallest commercially available passive tag, Hitachi's mu-chip—less than 0.4 mm wide—can be embedded in a piece of paper.[6] Antennas are either coiled or flattened to further reduce their size. At the time of writing, Mojix, a start-up company based in Los Angeles, recently announced a passive ultrahigh-frequency (UHF) RFID tag that can be read up to 600 feet away. Their readers can cover 2,500 square feet, providing users with three-dimensional location information.[7]

---

4. K. Finkenzeller, *RFID-Handbook*, 2nd ed., trans. R. Wadding (Chichester: Wiley & Sons, 2003), 7.

5. *Ibid.*, 8; Simson Garfinkel and Henry Holtzman, "Understanding RFID Technology," in *RFID: Applications, Security, and Privacy*, eds. Simson Garfinkel and Beth Rosenberg (Upper Saddle River, NJ: Addison-Wesley, 2005), 15–17.

6. See Hitachi's mu-chip at Hitachi, "The World's Smallest RFID IC," http://www.hitachi.co.jp/Prod/mu-chip/ (accessed July 22, 2008).

7. Mark Roberti, "Mojix Takes Passive UHF RFID to a New Level," *RFID Journal*, April 14, 2008, http://www.rfidjournal.com/article/articleview/4019/1/1/.

Information is stored on the RFID tag as strings of memory either burned into the chip in advance (read-only) or assigned later as read/write memory using a reader.[8] The signal of "promiscuous," or "dumb," tags can be read and understood by *any* RFID scanner within proximity. This possibility raises obvious privacy and security concerns. "Secure," or "smart," tags, on the other hand, incorporate authentication and encryption elements to prevent having their signal read without a key.[9] Tags featuring a kill switch can be deactivated, thus preventing future communications.[10]

RFID scanners are the eyes and ears of the system, ranging in size from a desktop computer to a handheld pricing gun and even smaller. Readers operate by constantly emitting radio waves until a tag is detected. When within range, the tag's antenna amplifies the signal and emits the chip's stored information back to the reader. The read range depends on the power, efficiency, and data integrity requirements of both the tag and the reader.[11]

If the reader functions as the eyes and ears, then the database to which the RFID is linked is the brain. To interpret data emitted from the tag, most readers need to link that information to other information, usually stored in a database. Using the human-implantable VeriChip as an example, the chip itself does not contain any medical information. It merely emits a unique 16-digit verification number when activated by a VeriChip scanner. The patient's medical record is made available only after the identification number has been entered into the password-protected Global VeriChip Subscriber (GVS) Registry. The VeriChip functions as an "access control" for the database, thereby limiting patient health information to the patient and authorized health care professionals. It is up to the patient to determine what information to provide, ranging from a list of the patient's medical conditions and medications, to the names and coordinates of the family physicians, to a PDF of the patient's living will. Because the passive RFID inside the VeriChip is always on, it will "speak on [the patient's] behalf"[12] to *any* scanner[13] in its read range—even if the patient is unconscious or otherwise incapacitated. This enables access to vital health information in emergency situations, and, in the case of unauthorized scanners, it offers valuable health information to identity thieves and other third-party information vendors who gain database access.

8. Garfinkel and Holtzman, "Understanding RFID," 18 (n. 5).

9. *Ibid.*

10. This is an important privacy-enhancing feature, as it enables RFID assistance in the supply chain without interfering with consumer rights after the point of sale.

11. Garfinkel and Holtzman, "Understanding RFID," 24 (n. 5).

12. VeriMed Patient Identification System, "Patients: For Patients, Caregivers, and Loved Ones," VeriMed, http://www.verimedinfo.com/for_patients.asp (accessed July 18, 2008).

13. This includes unauthorized scanners, because the VeriChip is a passive, unencrypted chip.

To fully understand the social implications of RFID, it is crucial to distinguish this technology from other radio frequency devices, such as the Electronic Article Surveillance systems (EAS) used to prevent shoplifting. RFID technology can be distinguished from EAS by virtue of its smaller size and, more importantly, its capacity to enable objects to announce their *presence* and their *unique identities*.[14] The latter set of capacities is significant. For example, consider having a scanner that indicates an unidentified "tagged object" is hidden in a knapsack (perhaps setting off an alarm after passing through the threshold of the door of a library or retail store). Now consider having a scanner tell you that the tagged object in the knapsack is a 1-kg bag of fertilizer (EPC# 016 37221 654321 2003004000), which was bought at the Home Depot store on Merivale Road in Ottawa on September 26, 2009, at 09:06:17 by CIBC credit card holder # 4408 0412 3456 7890 and is hidden in the knapsack beside Ottawa Library book call # 662.2014 B679 (titled: *Explosives*) signed out by Library cardholder # 11840003708286 on September 20, 2009, along with call # 921 H6755 (*Mein Kampf*), call # 320.533 H878 (*Les skinheads et l'extrême droite*), and call # 296.65 Kad (*Synagogues*).

When linked to databases and communications networks,[15] the amount of descriptive information associated with an RFID chip becomes practically limitless. Consequently, basic radio signals emitted from the tag can potentially provide incredibly descriptive information as they permeate clothing, knapsacks, body parts, and even buildings to communicate with RFID scanners and databases some distance away.

B. RFID Applications

Although the focus of this chapter is on human-implantable chips, RFID technology offers a wide range of applications across various segments of society. In the commercial sector, it is predicted that RFIDs will transform supply-chain management, allowing manufacturers, distributors, and retailers not only to increase their efficiency but, perhaps one day, to track individual items in the supply chain in real time from the point of production to the point of sale and beyond.[16] If achievable, item-level tagging could facilitate much greater coordination between supply and demand in a way that would allow warehouse space to be maximized, theft between production and sale to be minimized, and greater

14. Garfinkel and Holtzman, "Understanding RFID," xxv–xxvii (n. 5).

15. Such as Verichip's Verimed Patient Registry online database, which links a sixteen-digit RFID identifier to a patient's medical records; see VeriMed, "Patient Identification System" (n. 12).

16. See W. O. Hedgepeth, *RFID Metrics: Decision Making Tools for Today's Supply Chains* (Boca Raton, FL: CRC Press, 2007) and Jonathan Whitaker, Sunil Mithas, and Mayuram Krishnan, "IBM: A Field Study of RFID Deployment and Return Expectations," *Production and Operations Management* 16, no. 5 (2007): 599–612.

customer satisfaction to be achieved through the avoidance of delivery errors and lowered product costs.[17]

Likewise in the public sector, governments are using RFID technology to increase administrative efficiency and to track equipment. In 2003, the U.S. Department of Defense mandated that all suppliers must become RFID enabled by January 2005.[18] Aside from its use in product tracking,[19] supply-chain management,[20] and asset management,[21] RFIDs are being employed in numerous other government and commercial contexts, including passports, contactless payment systems, transportation payments, authentication systems, library management, baggage control, and health care applications. A number of hospitals, for example, are now using RFID-based systems used to "identify, locate and protect people and assets."[22]

Should it ever be realized, a universalizable item-level tagging combined with the capacity to track those items in real time is not merely another "disruptive" technology; it is predicted to be the precursor to something truly transformative, enabling what some people have called "the internet of things."[23] Adam Greenfield refers to this incredible technological capability as *everyware*, which he describes as follows:

> [A]ll of the information we now look to our phones or Web browsers to provide becomes accessible from just about anywhere, at anytime, and is delivered in a manner appropriate to our location and context.
> . . . the garment, the room and the street become sites of processing and mediation. Household objects from shower stalls to coffee pots are reimagined

17. John A Wolff, "RFID Tags: An Intelligent Bar Code Replacement" (IBM White Paper, IBM Global Services, June 2001), http://72.14.205.104/search?q=cache:Xg4_N35wPhYJ:ftp://ftp.software.ibm.com/software/pervasive/info/tech/gsoee200.pdf+RFID+Tags:+An+Intelligent+Bar+Code+Replacement&hl=en&ct=clnk&cd=2&gl=ca&client=firefox-a (accessed July 18, 2008).

18. Matthew Broersma, "Defense Department Drafts RFID Policy," cnet News.com, October 24, 2003, http://www.news.com/2100-1008-5097050.html (accessed July 18, 2008).

19. The Canadian Cattle Identification Agency started replacing barcodes with RFID tags in order to identify the origin of bovine herds. See Canadian Cattle Identification Agency (CCIA), "RFID and the Canadian Cattle Industry," CCIA, http://www.canadaid.com/ (accessed July 18, 2008).

20. Wal-Mart requires its top 100 suppliers to employ RFID labels in all shipments; see Wolff, "RFID Tags" (n.17).

21. Wise Track, "What Is Wise Track," http://www.wisetrack.com/ (accessed July 18, 2008).

22. VeriChip Corp., "VeriGuard Security Suite: RFID Security Never Before Possible" (working paper, VeriChip Corp.): 2, http://www.verichipcorp.com/files/VeriGuard(web).pdf (accessed July 18, 2008).

23. See International Telecommunications Union, *The Internet of Things, 2005*, 7th ed. (Geneva: ITU New Initiatives Programme, 2005).

> as places where facts about the world can be gathered, considered and acted upon. And all the familiar rituals of daily life—things as fundamental as the way we wake up in the morning, get to work, or shop for our groceries—are remade as an intricate dance of information about ourselves, the state of the external world, and the options available to us at any given moment.[24]

With human-implantable RFIDs, it is even possible to add people to the mix.

C. Human-Implantable RFIDs

The VeriChip human-implantable RFID that debuted at the Baja Beach Club is now available in U.S. hospitals.[25] At the time of writing, VeriChip claims that its RFID technology is used by more than five thousand installations worldwide, crossing health care, security, government, and industrial markets.[26] More than 900 hospitals in the United States have signed agreements with VeriChip, and 230 have implemented its protocols.[27] The VeriChip operates in much the same manner as other passive, unencrypted tags except that it is encased in glass and coated with a proprietary substance, known as biobond, that attaches the chip to connective tissue in the triceps in order to prevent migration within the body once implanted.[28] Each microchip contains a unique identifier that health care providers can scan and read to immediately identify patients and access personal health information.

VeriChip does not currently support an automated payment system for medical providers;[29] however, other automated payment systems are being tested, linking the chip to credit card information through a database. Consequently, it is not difficult to envision a day when payment for medical services takes place when a patient is scanned upon entering the hospital. Such a system would simply link the sixteen-digit identifier with the patient's health insurance plan or credit card number. It is likewise easy to imagine the chip's unique identifier being used for

---

24. Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (Berkeley, CA: New Riders, 2006), 1.

25. PR Inside.com, "VeriChip Corporation Adds More Than 200 Hospitals to Its VeriMed Patient Identification System at the American College of Emergency Physicians (ACEP) Conference, Far Surpassing Last Year's Enrollment," *Business Wire*, October 11, 2007, http://72.14.205.104/search?q=cache:MsuL9WtVjy8J:www.pr-inside.com/verichip-corporation-adds-more-than-r241908.htm+Verichip+900+hospitals&hl=en&ct=clnk&cd=1.

26. VeriChip, "Frequently Asked Questions," http://72.14.205.104/search?q=cache:Cng9ZrvpVNkJ:www.verichipcorp.com/content/company/corporatefaq+5,000+installations+worldwide+VeriChip&hl=en&ct=clnk&cd=1 (accessed July 19, 2008).

27. *Ibid.*

28. Biobond introduces complications to the subsequent surgical removal of the chip should it be compromised or otherwise revoked.

29. VeriChip, "What Does VeriChip NOT Do," http://www.verichipcorp.com/content/company/corporatefaq#g9 (accessed July 18, 2008).

secondary purposes, such as paying for groceries or expediting passage through a security system in an office or airport.

Given that current VeriChip applications employ passive RFID technology, the read range of the chip is at present only a few inches. This perhaps accidental privacy-enhancing feature is thought by some to be a bug, giving rise to the rapid increase in RFID scanning ranges and the coming RFID/GPS merger. The Mojix external passive chip, for example, can be read at 600 feet, and the Identec Solutions external GPS tag employs "satellites in combination with RFID to chart its route and movement."[30] As such, although the current VeriChip lacks an implantable transponder of appropriate size and specificity for such distance tracking, various commercial drivers in the logging industry[31] and elsewhere[32] will likely enable the development of an implantable version of these forms of technology in the near future. A GPS-enabled implant would allow people to be tracked in real time. It would add *everybody* to Greenfield's *everyware*; the supply chain could also become a kind of *human supply chain*, the Internet of things becoming an infrastructure for an "Internet of people."

It is interesting to think about the concept of an Internet of people in the context of more recent VeriChip developments, which include at least two new forms of implants.[33] Unlike its current ID chip, the newer biosensor devices offer diagnostic functions compatible with human biology. The first development is a biothermal temperature-sensing implantable RFID microchip, which can be used remotely to detect changes of temperature in a biological organism. Although the current use is geared toward early warning systems for avian flu in poultry farms,[34] human health applications have also been contemplated, such as "monitoring the location and medical condition of at-risk patients."[35]

---

30. Identec Solutions Inc, "Identec Solutions Develops Satellite Assisted RFID Tag Technology, June 2007," http://72.14.205.104/search?q=cache:SCzsQ08pqgoJ:www.identecsolutions.com/265%2BM5ef65d289bc.html+RFID+GPS+tag&hl=en&ct=clnk&cd=2 (accessed July 24, 2008).

31. Claire Swedberg, "Loggers Use Tags to Track Trucks, Timber: Papermakers and Sawmills Deploy RFID Systems in Forests to Facilitate the Loading, Weighing and Unloading of Logging Trucks," *RFID Journal*, November 28, 2005, http://www.rfidjournal.com/article/articleview/2007/1/1/.

32. Darren Murphy, "Fujitsu Unveils GPS Receiver with Integrated RFID Tag," *ENGADGET*, December 27, 2006, http://www.engadget.com/2006/12/27/fujitsu-unveils-gps-receiver-with-integrated-rfid-tag/.

33. These devices remain in the research and development phase and would require separate FDA approval for use in humans. See Digital Angel, "Bio-sensing: Miraculous Medical Potential," http://www.digitalangel.com/biosensor.aspx (accessed July 18, 2008).

34. Ephraim Schwartz, "Could Chips in Chickens Track Avian Flu?" *PC World*, December 6, 2005, http://www.pcworld.com/article/123845/could_chips_in_chickens_track_avian_flu.html.

35. Matt Hayden, "DEFA14A Filing: "Medical Advisory Systems' Stockholders to Vote on Digital Angel Merger on March 18, 2002," SEC Info, http://72.14.205.104/

The second development is a self-contained implantable RFID glucose-sensing chip.[36] Still in early stages of development, this device aims to provide artificial means for treating patients with diabetes.[37] Once contained in a biostable device with a biocompatible interface, this chip will interoperate with an electronics compatible signal transduction unit to create an "implantable, externally readable glucose sensor."[38] Current research and development is focused on a stable, self-contained glucose-sensing system that is contained in a selectively porous, biocompatible membrane. This "biostable sensing component will be incorporated into a millimeter scale signal transduction and RFID enabled communication device."[39]

Technological integration and interoperability of RFID with automated payment systems, GPS, and, in particular, biosensors will certainly enable implantable chips to transcend their original function as mere patient identification systems. They will become full-fledged medical devices providing therapeutic outcomes that restore and possibly even enhance biological function. It is the combination of these multifarious functions, however, that raises significant issues with regard to the appropriate regulatory environment for human-implantable RFID.

II. THE CURRENT REGULATORY ENVIRONMENT FOR RFID

Many law and policy makers around the world are just barely beginning to contemplate the appropriate regulatory environment for RFID—even less so for human-implantable RFID. Still, a number of existing laws already apply to RFID and more are likely on the way. These include municipal, provincial, federal, national, and international laws, regulations, and directives regarding such things as (a) communications, (b) electronic waste, (c) health and safety, and (d) privacy. My aim in this part is not to provide an exhaustive account of existing laws or their application. Instead, my brief explication aims to set the stage for Part III, where I claim that current approaches are too narrow and will fall short in protecting our privacy and autonomy interests if implantable RFID becomes part of the infrastructure of the so-called Internet of things.

---

search?q=cache:-mShO9SRctIJ:www.secinfo.com/dsvRq.3k4.htm+bio-sensor+digital+angel&hl=en&ct=clnk&cd=8 (accessed July 18, 2008).

36. Robert E. Carlson, Scott R. Silverman, and Zeke Mejia, "Development of an Implantable Glucose Sensor" (white paper, Digital Angel, April 12, 2007), http://www.digitalangel.com/documents/articles/GLU_120407.pdf (accessed July 19, 2008).

37. VeriChip, "VeriChip News: VeriChip Corporation's and Digital Angel Corporation's Self-Contained Implantable RFID Glucose Sensing Microchip, December 5, 2007," VeriChip, http://www.verichipcorp.com/news/1196870556 (accessed July 19, 2008).

38. Carlson, Silverman, and Mejia, "Implantable Glucose Sensor," 2 (n. 36).

39. *Ibid.*, 3.

A. Communications

Because RFID tags communicate with scanners and network databases by broadcasting signals on the electromagnetic spectrum, they are subject to communications regulations and standards set by bodies such as the U.S. Federal Communications Commission (FCC),[40] Industry Canada,[41] and the European Telecommunications Standards Institute (ETSI).[42] Generally speaking, these regulatory regimes aim to prevent interference and disruption of licensed spectrum services. Some parts of the spectrum are controlled for military use and public safety announcements. Others are for commercial services, including television, cellular phones, and broadband Internet. Regulatory bodies prevent interference and disruption of such services by prescribing and enforcing various technical, operational, and design requirements. RFID manufacturers must comply with these. In addition to standards aimed at coordinating proper allocation and use of the broadcast spectrum, some jurisdictions, such as Canada, set additional regulations aimed to prevent harmful emissions to human health.

B. Electronic Waste

In addition to health concerns generated by RFID emissions, bodies such as the European Union have published directives that protect against health concerns generated by electrical and electronic equipment waste (WEEE).[43] These directives require manufacturers of electrical and electronic equipment to establish an infrastructure for collecting WEEE in an ecologically friendly manner, such that users of electronic products can return them for disposal free of charge. RFID manufacturers are subject to these requirements.

---

40. See US Communications Act of 1934 ch 652 (US) s 302 and regulation made by the Federal Communication Commission pursuant to the Federal Communications Commission Authorization Act of 1988 (US).

41. See Canadian Radio Standards Specifications (RSS) and Radio Standards Procedures (RSP) at Industry Canada, "Spectrum Management and Telecommunications," http://www.ic.gc.ca/epic/site/smt-gst.nsf/en/h_sf01841e.html#guidelines; ministerial authority is conferred by Radiocommunication Act R.S. 1985 c. R-2 (Canada) s 5.

42. See ESTI, "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN): Overview of Radio Frequency Identification (RFID) Tags in the Telecommunications Industry" (ETSI TR 102 449 V1.1.1, January 25, 2006), and ESTI, "Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Short-Range Devices" (ESTI EN 300 220-1, 2000).

43. Council Directive (EC) 2002/95 of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment [2003] OJ L037: 19-23, and Council Directives (EC) 2002/96 of the European Parliament and of the Council of 27 January 2003 on waste electrical and electronic equipment (WEEE)—Joint Declaration of the European Parliament, the Council and the Commission relating to Article 9 [2003] OJ L037: 24.

C. Health and Safety

The more typical means of regulating the health implications of implantable RFID, however, are through provisions in food and drug laws.[44] Through these laws, bodies such as the U.S. Food and Drug Administration (FDA) or the Canadian Therapeutics Product Directorate (TPD) determine whether the RFID application in question is a "medical device" within the meaning of their guiding legislation and, if so, which category of device it falls into, depending on the degree of patient risk and the corresponding controls required to ensure safety and effectiveness. The core function of such regulation is to preclude and prevent the marketing of medical devices that are unhealthy or unsafe. Neither the FDA nor the TPD is charged with making broader determinations about the social implications of a proposed new medical device. For example, the FDA *did not* consider patient privacy or autonomy in its 2004 decision to approve the VeriChip as a Class II medical device.[45] The central issue was merely whether the device met basic health and safety requirements.[46]

Unlike its U.S. counterpart, Canada has not yet approved the VeriChip as a medical device. Although the regulations associated with Canada's Food and Drugs Act[47] contain a definition of "medical device" extremely similar to the one stipulated in U.S. legislation,[48] the two differ significantly in their application.

---

44. In Canada, this is done by the Food and Drugs Act R.S. c. F-27 and its associated regulation made pursuant to s. 30 of the Act. In the United States, this is done by the 1938 Food, Drug, and Cosmetic Act Title 21 ch 9 s 361.

45. U.S. Department of Health and Human Services, Food and Drug Administration, "Medical Devices; Classification of Implantable Radiofrequency Transponder System for Patient Identification and Health Information" (Docket No. 2004N-0477, December 10, 2004), http://www.fda.gov/ohrms/dockets/98fr/04-27077.htm.

46. The FDA may not have succeeded in this, as there are a number of recent reports indicating a link between implantable RFID and cancer. See Le Calvez et al., "Subcutaneous Microchip-Associated Tumours in B6C3F1 Mice: A Retrospective Study to Attempt to Determine Their Histogenesis," *Experimental and Toxicologic Pathology* 57 (2006): 255-265; Vascellari, Melchiotti, and Mutinelli, "Fibrosarcoma with Typical Features of Postinjection Sarcoma at Site of Microchip Implant in a Dog: Histologic and Immunohistochemical Study," *Veterinary Pathology* 43 (2006): 545–548; see also Katherine Albrecht, ed., "Microchip-Induced Tumors in Laboratory Rodents and Dogs: A Review of the Literature 1990–2006" (CASPIAN Consumer Privacy, 2007), http://www.antichips.com/cancer/index.html#Research_Article_Tables; Applied Digital disputes this claim. See William Wustenberg, "Effective Carcinogenicity Assessment of Permanent Implantable Medical Devices" (white paper, AlterNetMD Consulting, Farmington, MN, September 27, 2007), http://72.14.205.104/search?q=cache:jnOqeQdaIsUJ:www.verichipcorp.com/files/RodentSarcomagenesis092807Wustenberg.pdf+Effective+Carcinogenicity+Assessment+of+Permanent+Implantable+Medical+Devices&hl=en&ct=clnk&cd=1&gl=ca&client=firefox-a.

47. Food and Drug Act s 2 (n. 44).

48. Federal Food, Drug, and Cosmetic Act s 201(h) (n. 44).

Both refer to "medical devices" as implements involving diagnostics, treatment, mitigation of disease, restoring health, modifying bodily function, and the like. But Canadian regulators seem to employ a stricter definition of what constitutes a medical device. It is, therefore, plausible that the TPD would refuse an application from VeriChip because it is not an instrument of diagnosis or treatment, it does not mitigate or prevent diseases, and it plays no role in restoring, correcting, or modifying body function or structure.[49]

From a broader social perspective, not that much is riding on the legalities surrounding the appropriate statutory interpretation. After all, such legislation regulates only how VeriChip can and cannot be marketed. If it is not a medical device, then the regulation does not apply at all. Food and drug laws merely stipulate that medical devices on the market must meet basic health and safety requirements. Even on the assumption that VeriChip meets these standards,[50] the more important paucity in existing regulations, from a health and safety perspective, pertains to who can implant them, under what conditions, and for what purposes.

This became an issue in Canada for the first time in 2006 when the *Kitchener Record* reported that Jesse Villemaire implanted VeriChips into the hands of four students who drove up from Lockport, New York, for the procedure.[51] Leaving aside concerns about cancer and toxic shock,[52] the intricate connective tissues between the index finger and thumb do not render it an ideal location for the implantation of a VeriChip, which may be why the four sought out the well-known Cambridge tattoo artist and body-piercer to do this work rather than a licensed physician.

Although many jurisdictions have statutes regulating who can perform surgical acts, most do not specifically contemplate subdermal radio-emitting chip implants. In some Canadian provinces such as Ontario (where Jesse Villemaire resides), performing a procedure on the tissue of another person below the dermis is a regulated activity.[53] Not just anyone can do it. Subject to a limited

49. The yet-to-be-approved glucose and biothermal chips might one day, however, have therapeutic capabilities.

50. Recall that this is a contentious claim; see Albrecht, "Microchip-Induced Tumors" (n. 46).

51. Melinda Dalton, "Under Their Skin; Local Piercer Tries His Hand at Implanting Microchips;" *The Record*. Kitchener, February 4, 2006: A.1, http://64.233.167.104/search?q=cache:E1Un1HZfOqQJ:idtrail.org/files/The%2520Record%2520Archive.pdf+Kitchener+Record+Jesse+Villemaire+Chip&hl=en&ct=clnk&cd=1; Anna Bahney, "High Tech, Under the Skin," *New York Times*, February 2, 2006, http://www.nytimes.com/2006/02/02/fashion/thursdaystyles/02tags.html.

52. See V.P. McCarthy, "Toxic Shock Syndrome after Ear Piercing," *Pediatric Infectious Disease Journal* 7, no. 10 (1988): 741–742.

53. Regulated Health Professions Act S.O. 1991 c 18 (Ontario, Canada) s 27(2).

number of exemptions, one must be a licensed health professional.[54] Because implanting an RFID is a subdermal procedure, it is necessary in Ontario to determine whether a non-authorized person falls within the narrow range of exemptions set out in 8(1)–(4) of the Controlled Acts Regulations.[55] These include (i) acupuncture; (ii) ear or body piercing for the purpose of accommodating a piece of jewelry; (iii) electrolysis; and (iv) tattooing for a cosmetic purpose. Although "body piercing" is explicitly exempted, it is crucial to note that the exemption is strictly limited to piercing that accommodates jewelry.

The regulations nowhere define "piercing" and "jewellery." Ordinarily, the aim of ear or body piercing is to decorate the body by placing jewelry through a hole created for that purpose. Such ornamentation is usually visible to an onlooker. So while Baja Beach Club's Conrad Chase viewed the VeriChip as a next-generation body piercing,[56] the more plausible account is that a computer microchip is *not* jewelry or a piercing within the meaning of the regulations. Imbedded underneath the skin, the VeriChip is not a visible ornamentation, nor is its primary function decorative. This very likely means that the VeriChip and other RFIDs can be implanted in Ontario only by authorized health professionals. Even if the implantation of RFID chips is regulated in Ontario insofar as who can implant them, they are for the most part unregulated in terms of their use once implanted. The same is true for most jurisdictions.

D. Privacy and Autonomy

It requires little imagination to see how the implementation of human-implantable RFID systems could create serious risks to personal privacy and autonomy. As one journalist speculated, "it would be an interesting feature of an employee's first day: sign a contract, fill out a W-2 and roll up your sleeve for your microchip injection."[57]

---

54. *Ibid.*, s 27(1)(a); under s 40(1) of the Act, the consequences of performing such a procedure without the legal authority are not more than $25,000 in fines or imprisonment for a term of not more than one year or both for a first offense. This increases to $50,000 for all subsequent offenses.

55. Controlled Acts Regulations O. Reg 107/96 1991 (Ontario, Canada) ss 8(1)–(4), made pursuant to the Regulated Health Professions Act (n. 53).

56. Ian Kerr, "Not So Crazy about the Chips," *Innovate Magazine*, Spring 2005, http://www.idtrail.org/files/innovate%20-%20not%20so%20crazy%20about%20the%20chips%20%28may%202005%29.pdf.

57. Orr Shtuhl, "California Could Become Third State to Ban Forced Microchip Tag Implants (RFID), January 12, 2008," GlobalResearch.ca, http://64.233.167.104/search?q=cache:U2dcSe_njOcJ:www.globalresearch.ca/index.php%3Fcontext%3Dva%26aid%3D7781+It+would+be+an+interesting+feature+of+an+employee%E2%80%99s+first+day:+sign+a+contract,+fill+out+a+W-2+and+roll+up+your+sleeve+for+your+microchip+injection&hl=en&ct=clnk&cd=1&gl=ca&client=firefox-a (accessed July 21, 2008).

In response to the mere possibility of this scenario,[58] a handful of U.S. states have proposed, and some have passed, legislation that would ban the coerced implantation of RFIDs. Wisconsin was first to ban involuntary chipping.[59] Violators are subject to forfeiture not exceeding US$10,000. California[60] and North Dakota[61] quickly followed suit. Laws passed in Georgia[62] and New Hampshire[63] recently mandated expert study of the consumer privacy implications of RFID technology and the development of policy recommendations.

The central underpinning of these state laws is to ban implantation where there is a lack of consent on the part of the implantee. Like any other surgical procedure or medical "treatment," consent is a crucial prerequisite to implantation. But it does not end there. In the case of RFID implants, the issue of consent is ongoing, not only because of medical treatment laws, but also because of privacy law. From the perspective of informational privacy and data security, it is generally important to ensure knowledge and consent whenever there is a collection, use, or disclosure of information about an identifiable individual.[64]

The question about how to ensure that RFID complies with the consent principle and other fair information practices has occupied the minds of the Data Commissioners' community around the world for several years. For example, in Europe, the Article 29 Data Protection Working Party (Working Party) released its "Working Document on Data Protection Issues Related to RFID Technology" in January 19, 2005.[65] To the extent that RFID systems are used to collect, share,

58. HR-BLR.Com, "Ohio Employer First to Implant Employee Microchips, April 10, 2006," HR-BLR.Com, http://64.233.167.104/search?q=cache:O0CUcauGgzIJ:hr.blr.com/news.aspx%3Fid%3D17924+Ohio+employer+forced+chipping&hl=en&ct=clnk&cd=1&gl=ca&client=firefox-a.

59. 2005 Wisconsin Act 482 Assembly Bill 290, May 30, 2006 (Wisconsin, US).

60. An Act to Add Section 52.7 to the Civil Code, Relating to Identification Devices, Senate Bill 362 ch 538, June 19, 2007 (California, US).

61. Senate Bill No. 2415 ch 12.1-15 of the North Dakota Century Code, 2 (North Dakota, US).

62. Bill No.: H.B. 203 (Georgia, US), introduced on April 12, 2005, creates a Joint House and Senate Emerging Communications Technologies Study Commission.

63. New Hampshire House, HB 686-FN—As Amended by the House March 18, 2008 (New Hampshire).

64. Consent is, of course, only one of a larger set of privacy-protecting principles sometimes known as "fair information practice principles." See, e.g., Organisation for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Annex to the recommendation of the Council of 23 September 1980, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html and the Personal Information Protection and Electronic Documents Act (PIPEDA) S.C. 2000 c 5 (Canada) s 7.

65. This Working Party was set up under Article 29 of Council Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement

and store personal data, they must conform to the principles set out in the European Community Data Protection Directive[66] and the directive on privacy and electronic communications.[67] In its interpretation of the EU data protection law, the Working Party expressed concern "about the possibility for some applications of RFID technology to violate human dignity as well as data protection rights."[68] Specifically, the Working Party expressed unease regarding the possibility of government, business, and individual use of the technology to "pry into the privacy sphere of individuals. The ability to surreptitiously collect a variety of data all related to the same person; track individuals as they move into public places . . . [and] enhance profiles."[69]

The Working Party held that unambiguous consent "will be the only legal ground available to data controllers to legitimize the collection of information through RFID."[70] Further, they held that data controllers must provide data subjects with information as to the "identity of the controller, the purposes of the processing as well as, among others, information on the recipients of the data and the existence of a right of access."[71] In particular, they noted that "data controllers should be very clear in informing individuals that the presence of such devices enables the tags to broadcast information without individual engaging in any active action" and that the data subject should be informed about the RFID-garnered information's intended use, "including (a) the type of data with which RFID information will be associated and (b) whether the information will be made available to third parties."[72] In its ultimate conclusion, the Working Party was clear that RFID manufacturers must ensure that the technology is privacy compliant.[73]

Similarly, the Privacy Commissioner of Canada has recognized that certain uses of RFID are subject to federal regulation in Canada.[74] This legislation adopts

---

of such data [1995] OJ L281: 31. It is an independent European advisory body on data protection and privacy.

66. *Ibid.*

67. Council Directive (EC) 2002/58 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 on privacy and electronic communications) [2002] OJ L201: 37–47.

68. Article 29 Data Protection Working Party, *10107/05/EN: Working Document on Data Protection Issues related to RFID Technology* (Luxemburg: Article 29 Data Protection Working Party, January 19, 2005), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

69. *Ibid.*, 2.

70. *Ibid.*, 10. Note, however, that consent may not be required as foreseen by Article 7 of the Data Protection Directive (n. 57).

71. Article 29, "Working Document," 10 (n. 58).

72. *Ibid.*, 10.

73. *Ibid.*, 12.

74. PIPEDA (n. 54).

a version of the fair information practice principles similar to those first set out in the OECD Guidelines and implemented in the EU Data Protection Directive. According to the Privacy Commissioner of Canada:

1. If the chip has had the personal information of the individual written to it, then it is a repository of personal information;
2. If the tag is unique, and can be associated with an individual, it becomes a unique identifier or proxy for that individual; and
3. Information about possessions or purchases, which can be manipulated or processed to form a profile, is personal information, whether gathered through multiple visits to a facility or organization, or through access to the data base of RFID purchase information.[75]

Consequently, the Commissioner has noted that RFID systems can raise numerous privacy concerns, such as (i) the surreptitious collection of information; (ii) the ability to track an individual's movements; (iii) the ability to profile individuals; (iv) the ability to reveal secondary information about individuals; and (v) the capacity for massive data aggregation.[76]

The Ontario Information and Privacy Commissioner (OIPC) has also been a thought leader on this subject, producing the first ever set of best practices to ensure privacy compliance.[77] In addition to applying Canada's ten privacy principles to RFIDs, the OIPC offers three guiding principles: (i) focus on RFID information systems, not technologies; (ii) privacy and security must be built in at the design stage; and (iii) maximize individual participation and consent. In a white paper released January 2008,[78] the OIPC expressed concern about the use of RFID in the health care context, recognizing that RFIDs linked to people are governed by provincial legislation[79] because they implicate "organizations and individuals involved in the delivery of health care services in both the public and private sectors."[80] In highlighting its potential benefits, the OIPC found that if the

75. Office of the Privacy Commissioner, "Fact Sheet: RFID Technology," http://www.privcom.gc.ca/fs-fi/02_05_d_28_e.asp.

76. *Ibid.*

77. Ontario Information and Privacy Commissioner (OIPC), *Privacy* Guidelines for RFID Information Systems (RFID Privacy Guidelines) (Toronto: OPIC, 2006), http://www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf.

78. Ontario Information and Privacy Commissioner (OPIC), RFID and Privacy: Guidance for Health Care Providers (Toronto: OPIC, 2008), http://www.ipc.on.ca/images/Resources/up-1rfid_HealthCare.pdf.

79. Personal Health Information Protection Act (PHIPA), 2004, S.O. 2004, c 3 (Ontario, Canada).

80. Ontario Information and Privacy Commissioner Ann Cavoukian, "RFID and Privacy: Guidance for Health-Care Providers on RFID" (lecture, MaRS Centre, Toronto, 2008), OPIC, http://72.14.205.104/search?q=cache:JDTnfWCsCigJ:www.ipc.on.ca/

> . . . RFID patient identification program responds to a defined problem or issue in a limited, proportional and effective manner, and is deployed in a way that minimizes privacy and security risks, at least as effectively as any alternative solution, then in principle there should be few privacy concerns with the program.[81]

The OIPC, however, expressed concern about human-implantable RFID, recognizing that there are "complex legal and ethical questions" invoked by RFID "implants in the human body."[82] Stressing the importance of informed consent, the use of patient autonomy as the yardstick consent, and the need for the utmost transparency of its use in the health care context, the OIPC referred to the 2007 report issued by the U.S. Council on Ethical and Judicial Affairs (CEJA)[83] and the 2005 report by the European Group on Ethics (EGE) in Science and Technology to the European Commission.[84] Both reports held "that implantable RFID devices may compromise people's privacy and security because it is yet to be demonstrated that the information in the tags can be properly protected."[85]

In the United States, VeriChip is not directly subject to U.S. health privacy laws,[86] as VeriChip and its parent company are not health care providers, a health plan, or a health care clearinghouse.[87] However, both companies are bound to the extent that their contractual relationships with health care providers make them responsible for the protection of personal health care information. Applied Digital has, as a result, developed a policy to enable Health Insurance Portability and Accountability Act (HIPAA) compliant business associate agreements.[88] Moreover, VeriChip operates under Federal Trade Commission (FTC) oversight because the technology is governed by consumer protection regulation. To this end, the FTC will enforce promises made by businesses with regard to the use, control, and protection of personal information.

---

images/Resources%255C2008-03-05-HPRFIDCanada.pdf+RFID+Canada+implantable&hl=en&ct=clnk&cd=4&gl=ca&client=firefox-a.

81. OIPC, "RFID and Privacy," 29 (n. 78).

82. *Ibid.*, 30.

83. Robert M. Sade, "Report of the Council on Ethical and Judicial Affairs," *CEJA Report* 5 (2007), http://www.ama-assn.org/ama1/pub/upload/mm/369/ceja_5a07.pdf.

84. Rafael Capurro, "Ethical Aspects of ICT Implants in the Human Body," European Group on Ethics in Science and New Technologies (EGE) de la Comisión Europea: EGE Opinion (March 16, 2005), http://64.233.167.104/search?q=cache:jGz9zgxN-PAJ:www.capurro.de/talca.ppt+European+Group+on+Ethics+(EGE)+in+Science+and+Technology+to+the+European+Commission+Report+RFID+2005&hl=en&ct=clnk&cd=6.

85. See Ann Cavoukian, "RFID and Privacy Lecture" (n. 80).

86. E.g., Health Insurance Portability and Accountability Act of 1996 (HIPAA) 42 USC 201.

87. *Ibid.*, s 1172(a).

88. VeriChip Corp, "S-1/A SEC Filing, January 9, 2007," Edgar, http://sec.edgar-online.com/2007/01/09/0001193125-07-003171/Section16.asp.

Because the whole point of the VeriChip is to provide a unique identifier associated with a particular individual, and given the passive, promiscuous nature of the unencrypted VeriChip, there is little doubt that fundamental privacy principles are implicated whenever an implantee comes within the read range of a scanner. The key difference between RFID and traditional forms of identification (such as presenting a health card or medical history) is that the RFID identification process is entirely automated. When one considers that the design of VeriChip was meant to identify the implantee and collect information unbeknownst to that person (e.g., while unconscious or disoriented), one realizes the ease with which surreptitious collection of information becomes possible and the consequent challenges of obtaining meaningful consent.

It is tempting to think that the consent issue for human-implantable RFID is no different from other RFIDs, which can also be easily associated with an identifiable individual. In fact, Applied Digital and a number of other providers offer many kinds of less invasive forms of associable RFIDs, such as bracelets. The key differences are the potentially coercive elements around implantation and the fact that the current human-implantable RFIDs are read-only, not easily removed, and not encrypted, and they do not have an "on-off" switch. A read-only chip that is not easily removed is problematic in circumstances where the personal identifier in the chip becomes compromised. Because it is not possible to rewrite data to the current chips, it is not possible to "revoke" the identifier without physically removing the chip. This problem is compounded by the fact that the chip is purposefully unencrypted.[89] This makes the VeriChip entirely vulnerable from an information security perspective. It has been easily hacked and cloned, with the method for doing so widely available on the Internet.[90] Given its insecurity and the inability to revoke and rewrite new identifiers, its inability to be turned "off," compounded by the need to surgically remove the chip if compromised or no longer desired, it is unclear why anyone who wants the chip for anything other than a "transgressive cyberpunk fashion statement" would consent to its implantation in the first place.

VeriChip's only attempt to address these problems seems to be the addition of a password requirement for access to the portion of its database with which a given chip is associated. Ironically, this element undermines any need for the chip itself, because the rather weak form of authentication that a password affords is really all that is on offer. As a number of information security experts

89. It is has been said that the fact that human-implantable RFIDs are unencrypted is a feature rather than a bug; allowing the personal identifier to be easily intercepted prevents wrongdoers from using more coercive means of extracting the information on the chip. See John Halamka, et al., "The Security Implications of VeriChip Cloning," *Journal of American Medical Informatics Association* 13, no. 6 (2006): 601–607.

90. Jonathan Westhuese, "Demo: Cloning a VeriChip," http://cq.cx/verichip.pl (accessed July 23, 2008).

(including the Harvard Medical School's CIO, who implanted himself with the VeriChip) have clearly stated, "[t]he VeriChip should serve exclusively for *identification* and not *authentication* or access control."[91]

III. THE INTERNET OF THINGS AND THE NOT-SO-LONG ARM OF THE LAW

Setting aside VeriChip's current privacy and security concerns, the broader challenge with RFID will be its future collision course with the consent principle. RFIDs are subject to a "network effect."[92] Like the Internet itself, the so-called Internet of things will reach its true potential only if it is (near-) ubiquitous; the only way to derive the maximum benefit of an automated identification system is to make it pervasive and automatic.

Such a system would completely undermine the consent/control model of privacy, which is premised on the possibility that individuals can determine for themselves when, how, and to what extent information about them is communicated to others. To illustrate, let us continue with Greenfield's description of *everyware*, mentioned briefly in Part I.B:

> You close the door to your office because you want privacy, and your phone and IM channel are automatically set to "unavailable." You point to an unfamiliar word in a text, and a definition appears. You sit down to lunch with three friends, and the restaurant plays music that you've all rated highly.[93]

In order for the world to truly work like this, one would have to abandon altogether the requirements, recommendations, and guidelines set out by the European Working Party, the Privacy Commissioner of Canada, and the OIPC. In a world laced with RFIDs—a world many if not most network aficionados think inevitable—it will no longer be feasible to obtain individualized consent (or, for that matter, even individual waivers of privacy) for each informational transaction resulting in collection, use, or disclosure of personal information. The OIPC's excellent and important guideline to ensure "maximal individual participation and consent" is fundamentally at odds with a system geared toward pervasive and automated information transactions.

---

91. Halamka, "Security Implications of VeriChip," 601 (n. 89).

92. A network effect (sometimes called a "network externality") is an attribute by which the value of a good or service becomes dependent on its broad adoption by others. VeriChip would not provide a valuable emergency service if only one doctor, one hospital, or one patient used it. See John Halamka, "Straight from the Shoulder," *New England Journal of Medicine* 353 (2005): 331–333; in general, the only way to achieve ubiquity is a low unit cost for RFID, which itself requires mass adoption.

93. Greenfield, *Everyware*, 26–27 (n. 24).

Whether for personalized jukeboxes or emergency health services, such automated systems would instead require that all or almost all individuals opt in by way of *blanket-consent:* offering up, in advance and without limitation, a host of unforeseeable, unpredictable, and often unintended personal information collections, uses, and disclosures. In what meaningful sense could this be called "consent"? And if the goal of the Internet of things truly is ubiquitous efficiency, then there will be little or no opportunity to opt out of the system in any meaningful way—much like trying to live as an adult without a credit card, drivers license, or passport in contemporary North American or European society. In an RFID-enabled network society (not to mention RFIDs seamlessly integrated into human bodies), the nature of collection, use, and disclosure of information becomes what designer Naoto Fukasawa once spoke of as "design dissolving in behaviour." It is a system so well designed and so effortless for those who use it that the collection, use, and disclosure of personal information "effectively absconds from awareness."[94]

Whatever else remains unclear, it seems obvious that our current regulatory model—premised on control and consent—would provide a not-so-long arm of the law in an RFID-enabled Internet of things.

IV. THE HUMAN-MACHINE MERGER

To better grasp the potential shortcomings of our current regulatory environment, it is important to recognize that human-implantable RFIDs are just one drop in the bucket-load of implantable devices being developed as part of a growing trend in medicine that seeks to merge human bodies with machine parts. Mechanical and biomechanical implants and devices are not completely new to the health agenda.[95] To offer a few examples, cochlear implants have been available for several years to restore or enhance hearing.[96] Wireless sensors and pumps have been implanted to deliver insulin to patients with diabetes who lack a fully

94. *Ibid.*, 26.

95. Ray Kurzweil and Terry Grossman, *Fantastic Voyage: Live Long Enough to Live Forever* (Emmaus, PA: Rodale Press, 2004); Ian Kerr and James Wishart, "A Tsunami Wave of Science: How the Technologies of Transhumanist Medicine Are Shifting Canada's Health Research Agenda," *Health Law Review* (forthcoming); Ian Kerr and Timothy Caulfield, "Emerging Health Technologies," in *Canadian Health Law and Policy*, 3rd ed, eds. Jocelyn Downie, Timothy Caulfield, and Colleen Flood (Toronto: Butterworths, 2007): 509–538.

96. National Institute on Deafness and Other Communication Disorders, "Cochlear Implants, May 2007," http://www.nidcd.nih.gov/health/hearing/coch.asp (accessed July 17, 2008).

functioning pancreas.[97] Totally implantable artificial hearts have undergone extensive clinical trials and have extended life significantly for some patients with congestive heart failure and no hope for a transplant.[98]

In addition to these well-known examples, there are a number of interesting cybernetic implants and network devices that will interoperate with the human body. For example, RedTacton is a "human area networking" technology that uses the surface of the human body as a high-speed network transmission path. According to its corporate profile, RedTacton will enable "ubiquitous services based on human-centered interactions that are more intimate and easier for people to use."[99] RedTacton integrates communications with ordinary bodily functions and activities, providing greater control than implantable RFID: for example, "touching, gripping, sitting, walking, stepping and other human movements can be the triggers for unlocking or locking, starting or stopping equipment, or obtaining data."[100]

It is practically impossible not to marvel at the possibilities of this kind of innovation in the near future. Not *that* long ago (the year of my bar mitzvah), the famous philosopher and cognitive scientist, Daniel Dennett, dreamed in sci-fi prose of "mainlining Brahms" directly into his brain, which, he speculated, would be "an unforgettable experience for any stereo buff."[101] Are we not now on the precipice of Apple iTunes traveling wirelessly from a miniature implantable or wearable device across our skin and into cochlear implants that are "mainlined" directly to our auditory systems?

To show that this technological possibility is not far-fetched, consider a second example. Cybernetics professor Kevin Warwick has implanted a neural transducer, a device that allows him to "hook [his] nervous system up to the Internet."[102] Through direct links between the neural transducer and nerve fibers in his arm, he is able to transmit radio signals from a computer to the neural transducer implant and download them onto his nerve fibers and vice versa. Warwick and

97. Robert F. Service, "Can Sensors Make a Home in the Body?" *Science* 297, no. 5583 (2002): 962–963.

98. Wray Herbert, "The Artificial Heart: Not Just a Pump," *Scientific American Body*, February 2008, http://www.sciam.com/article.cfm?id=not-just-a-pump; Emily Singer, "An Artificial Heart That Doesn't Beat," *Technology Review*, September 21, 2006, http://www.technologyreview.com/read_article.aspx?id=17523&ch=biotech&pg=1.

99. RedTacton, "What's RedTacton?," http://www.redtacton.com/en/info/index.html (accessed July 17, 2008).

100. RedTacton, "Three Features," http://www.redtacton.com/en/feature/index.html (accessed July 17, 2008).

101. Daniel C. Dennett, "Where Am I?" in *Brainstorms: Philosophical Essays on Mind and Psychology*, ed. Daniel C. Dennett (Boston: MIT Press, 1981), 6, http://www.cs.umu.se/kurser/TDBC12/HT99/Dennett.html (accessed July 17, 2008).

102. Kevin Warwick, "Cyborg Morals, Cyborg Values, Cyborg Ethics," *Ethics and Information Technology* 5 (2003): 135–137, 135.

his research team have investigated the signals corresponding to his bodily movement. For example, when he moves his finger, some of the electronic signals from his nervous system that caused his muscles and tendons to operate are also transmitted to the computer, where they are then stored as a sequence. The team found that they can play back those same signals and thereby re-create much of the original movement. Likewise, Warwick's brain and central nervous system have successfully received and made sense of signals from external ultrasonic sensors and transmitters used in mobile robots. Warwick's "cyborg experiments" may seem like an eccentric exploration of an over-funded academic, but there is much hope within medical and bioengineering communities that such applications will soon become mainstream cures for paralysis and other physical impairments. In fact, many hope that such devices will one day enhance physiological function and capability *above and beyond* species-typical norms.

At the same time, reflecting upon the broader implications of radio frequency implants and other human-machine mergers, Professor Warwick has noted that this is not merely a question about enhancing human capabilities but also "a completely different basis on which the . . . brain operates in a mixed human, machine fashion."[103] According to Warwick, the human-machine merger implicates individual identity and personal autonomy. As he put it,

> . . . a human whose nervous system is linked to a computer not only puts forward their individuality for serious questioning but also, when the computer is part of a network or at least connected to a network, allows their autonomy to be compromised.[104]

V. THE INTERNET OF PEOPLE

When we think about human-implantable RFID in the context of the Internet of things and the human-machine merger, we see that the issues are much more profound than the perceived pros and cons of the current VeriChip. Our existing regulatory approaches provide some measure of protection against RFID and the misuse of the electromagnetic spectrum, improper disposal of electronic waste, and the dishonest marketing of unsafe medical devices. But in most North American and European jurisdictions, our laws are insufficient to deal with what devices can be implanted, by whom, and under what circumstances. Although existing data protection regimes currently afford individuals some measure of autonomy and control over the personal information transactions generated by today's *one-off* RFID applications, the suggested approaches and guidelines discussed above in Part II are premised on an ability to obtain meaningful

103. *Ibid.*, 136.
104. *Ibid.*, 132.

consent and individual participation. These approaches do not adequately contemplate the obfuscation and automation of information collection, use, and disclosure likely to occur should our world move closer to an integrated and ubiquitous Internet of things.

Here is how the International Telecommunications Union framed the problem back in 2005:

> When everyday items come equipped with some or all of the five senses (such as sight and smell) combined with computing and communication capabilities, concepts of data request and data consent risk becoming outdated. Invisible and constant data exchange between things and people, and between things and other things, will occur unknown to the owners and originators of such data. The sheer scale and capacity of the new technologies will magnify this problem. Who will ultimately control the data collected by all the eyes and ears embedded in the environment surrounding us?[105]

Consent is a serious bug in the code of automation.

Of perhaps even greater concern, technologists, physicians, and their regulators have yet to adequately consider what to do about the fact that human-implantable RFID and other innovations are adding humans to this ubiquitous network. Although the benefits that these innovations promise are considerable if not revolutionary, do we have *any* idea how humanity might change when the emerging Internet of things likewise becomes an Internet of people?

If we are to remain committed to fundamental principles and values such as consent, personal privacy, and autonomy, we will need to seriously rethink their application in light of RFID and other emerging network technologies. Given the paucity of an appropriately accommodating regulatory environment—*and, rather than giving up these bedrock values simply because they seem "outdated"*—we also need to continue thinking carefully about whether there is sufficient justification for moving forward with human-implantable RFID, ubiquitous computing, and the Internet of things. We must ensure that today's rather primitive specter of the VeriChip automatically enabling collection, use, or disclosure of the identity and health records of the somnambulist patient does not become the dystopic metaphor for the place of people in tomorrow's Internet of things.

105. ITU, *ITU Internet Reports 2005: The Internet of Things Executive Summary* (Geneva: ITU Strategy and Policy Unit (SPU), 2005): 15, www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf.