GETTING UNDER YOUR SKIN—LITERALLY: RFID IN THE EMPLOYMENT CONTEXT

Marisa Anne Pagnattaro†

I. INTRODUCTION

Consider this: nearly 12.4 million people in Shenzhen, China will have residency cards fitted with computer chips containing their name, address, work history, educational background, religion, ethnicity, police record, medical insurance status, and reproductive history.[1] The Chinese government also has ordered all large cities to issue such high-tech residency cards to approximately 150 million people who now live in a city but have not yet acquired permanent residency.[2] What are these computer chips? They are radio frequency identification ("RFID") chips, an automated data-capture technology system that can be used to identify, track and store information.[3]

These tiny computer chips use electromagnetic energy in the form of radio waves to communicate information.[4] The technology provides identification and tracking capabilities by using wireless communication to transmit data.[5] A number of federal agencies and a range of business and public sectors (e.g. health care, retail, transport, and pharmaceutical) are already using RFID systems for a variety of purposes, including logistics support, tracking shipments, electronic screening, preventing counterfeit drugs,

† Associate Professor of Legal Studies, Terry College of Business, University of Georgia; Ph.D., English, University of Georgia; J.D., New York Law School. The author acknowledges funding from a Terry-Sanford research grant and a Coca-Cola Center for International Business Programs award from the University of Georgia for this project. The author is also grateful to Ming Henderson-Vu Thi, Kramer Levin Naftalis & Frankel LLP, Paris, and Adam Kardash, Heenan Blakie LLP, Montreal, for their assistance.

1. Keith Bradsher, *China Enacting a High-Tech Plan to Track People*, N.Y. TIMES, Aug. 12, 2007, at A1, *available at* http://www.nytimes.com/2007/08/12/business/worldbusiness/12security.html?ex=1189137600&en=107bdb9d809c09b6&ei=5070.

2. *Id*.

3. KATHERINE ALBRECHT & LIZ MCINTYRE, SPYCHIPS: HOW MAJOR CORPORATIONS AND GOVERNMENT PLAN TO TRACK YOUR EVERY PURCHASE AND WATCH YOUR EVERY MOVE 1–9 (2006).

4. *The Basics of RFID Technology*, RFID J., http://www.rfidjournal.com/article/view/1337/1/129 (last visited Aug. 26, 2008).

5. *Id*.

security, and identification.[6] As RFID helps improve productivity, efficiency, and accuracy, many companies are considering a variety of ways to use this technology.

RFID chips can also be used to track employees.[7] They can be implanted under an employee's skin, worn in an employee's clothing, or attached to an identification badge.[8] The most widespread workplace use of RFID technology is chip-embedded staff identification ("ID") badges, which are primarily used for controlled access to an employer's premises.[9] Even this use, however, can be controversial if the data collected is used to discipline employees, as opposed to merely controlling door locks.[10] The potential number of workplace uses—not to mention off-site uses—is limited only by an employer's lack of imagination. Once the RFID is in an employee's badge or embedded under the employee's skin, the employer can collect data regarding the employee's location and movement by using strategically placed readers.[11] This data can then be entered into a database to learn more about the employee's whereabouts.[12]

This article explores the legal ramifications of the use of RFID by employers to track employees. Part II presents a brief history of RFID, including novel and interesting uses. This section also discusses security and safety concerns regarding the use of this technology.[13] Part III analyzes current and proposed law in the United States regulating RFID. Part IV details legal regulations in the international context, including Canada, the European Union ("EU"), and Australia. Lastly, Part V proposes recommendations about the use and legal regulation of RFID in the workplace.

II. A BRIEF HISTORY OF RFID AND ENSUING CONCERNS

RFID technology is based on a fairly simple system. There are three major components of an RFID device: (1) a tiny silicon computer chip or

6. U.S. GOV'T. ACCOUNTABILITY OFFICE, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT 2, 14, 22 (2005) [hereinafter GAO REPORT], *available at* http://www.gao.gov/new.items/d05551.pdf.

7. *Id.* at 21.

8. JEREMY GRUBER, RFID AND WORKPLACE PRIVACY, http://www.workrights.org/issue_electronic/RFIDWorkplacePrivacy.html (last visited Mar. 26, 2008).

9. *Id.*

10. *See id.* (discussing concerns over using RFID to monitor employees in order to control and intimidate workers).

11. *See* EDWARD BALKOVICH ET AL., 9 TO 5: DO YOU KNOW IF YOUR BOSS KNOWS WHERE YOU ARE? CASE STUDIES OF RADIO FREQUENCY IDENTIFICATION USAGE IN THE WORKPLACE 9 (2005), *available at* http://www.rand.org/pubs/technical_reports/ 2005/RAND_TR197.pdf (describing how access systems are structured).

12. *Id.*

13. *See generally* Laura Hildner, *Diffusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133 (2006) (discussing privacy issues concerning RFID use); Alan R. Peslak, *An Ethical Exploration of Privacy and Radio Frequency Identification*, 59 J. BUS. ETHICS 327 (2005) (examining RFIDs and privacy); Reepal S. Dalal, Note, *Chipping Away at the Constitution: The Increasing Use of RFID Chips Could Lead to an Erosion of Privacy Rights*, 86 B.U. L. REV. 485 (2006) (discussing privacy rights and RFID chips).

"integrated circuit" containing a unique identification number; (2) an antenna that is hooked to the chip; and (3) a reader, or scanning device.[14] The chip can be encrypted with a "unique product code that identifies the individual" object, product, or person "to which it is attached," and the "antenna is responsible for transmitting information from the chip to the reader via radio waves."[15] The reader, or scanning device, has its own antenna, which is used to communicate with the chip, also known as a tag. The reader sends the information to a database, or back-end logistics system, which stores information gathered from RFID tags.[16] RFID tags may be either passive or active.[17] A passive tag does not contain its own power source, such as a battery, and it cannot initiate communication with a reader.[18] Active tags, which "contain a power source and a transmitter," send a continuous signal.[19] This technology has been used since World War II, where it was used in aircraft Identification Friend or Foe systems.[20] During the 1970s, RFID technology began to be used in a limited way for inventory control.[21]

A. Novel and Interesting Uses

Tremendous growth in the use of RFID technology occurred in the 1990s, due to the ability of companies to use RFID systems to efficiently collect, manage, distribute, and store information on inventory.[22] At this time, RFID technology enjoys a wide range of uses,[23] such as tracking gourmet dinners at Marks & Spencer in London, tagging more than fifty million pets worldwide, guarding paintings at a museum in Rotterdam, screening Oscar goers, and tracking supplies in Iraq by the U.S. military.[24] Wal-Mart is making extensive use of RFID inventory tracking, yet it may not be resulting in anticipated cost savings to justify the use.[25] In 2003, Wal-Mart began using RFID technology in its Broken Arrow, Oklahoma store to track Max Factor lipstick.[26] When consumers removed the lipstick from the shelves, this triggered a video

14. FED. TRADE COMM'N, RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS 3–4 (2005) [hereinafter FTC REPORT], *available at* http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

15. *Id.*

16. *Id.* at 4.

17. *Id.* at 5.

18. *Id.* at 6.

19. GAO REPORT, *supra* note 6, at 7.

20. DEP'T OF COMMERCE, FREQUENCY IDENTIFICATION: OPPORTUNITIES AND CHALLENGES IN IMPLEMENTATION 5 (2005), *available at* http://www.technology.gov/reports/2005/RFID_April.pdf.

21. *Id.*

22. JEREMY LANDT, SHROUDS OF TIME: THE HISTORY OF RFID 5 (2001), *available at* http://www.transcore.com/pdf/AIM%20shrouds_of_time.pdf; DEP'T OF COMMERCE, *supra* note 20, at 6.

23. ROBERT O'HARROW, JR., NO PLACE TO HIDE 284–90 (2005).

24. Cathy Booth-Thomas, *The See-It-All Chip*, TIME, Sept. 22, 2003, http://www.time.com/time/magazine/article/0,9171,1005756,00.html.

25. Gary McWilliams, *Wal-Mart's Radio-Tracked Inventory Hits Static*, WALL ST. J., Feb. 15, 2007, at B1; *Wal-Mart RFID Plans Change*, RFID GAZETTE, Feb. 27, 2007, http://www.rfidgazette.org/walmart.

26. Ashlee Vance, *Wal-Mart Turns Customers into RFID Lab Rats*, THE REG., Nov. 13, 2003, http://www.theregister.co.uk/2003/11/13/walmart_turns_customers_into_rfid.

monitor, allowing researchers 750 miles away to watch consumers.[27] Researchers in Cincinnati at Proctor & Gamble could then analyze the behavior of consumers.[28]

There are also many other creative uses of RFID technology. On a very practical level, RFID technology is used in connection with the Homeland Security Container Security Initiative to develop "smart" containers that can notify authorities of any tampering or theft.[29] RFID chips can be used to create an "e-pedigree" of products through a supply chain to protect the food supply.[30] This can be particularly useful to thwart further injury once a dangerous product is identified, such as when there is an *E. coli* outbreak from a food source or contamination from a product manufactured with a harmful ingredient. On an even more micro level, the staple manufacturer Swingline has developed staples with RFID tags to facilitate document tracking.[31]

RFID technology is also useful to track people in a range of other contexts. Conference badges fitted with RFID chips allow conference organizers to determine who is attending what sessions, as well as when participants come and go.[32] The Principal and School Board of Brittan Elementary School in Sutter, California, proposed a controversial tracking system for school children with mandatory ID badges with RFID chips.[33] The school, however, withdrew the system following vocal opposition in California.[34] The Minnesota Department of Corrections is using a half-million dollar RFID system to track inmates in a minimum/medium security correctional facility,[35] and Alanco Technologies is using tracking systems in prisons in California, Michigan, and Ohio.[36] In a novel move, the Baja Beach

27. Hildner, *supra* note 13, at 133.

28. *E.g.*, Charles J. Murray, *Privacy Concerns Mount over Retail Use Of RFID*, TECHWEB NETWORK, Dec. 1, 2003, *http://www.techweb.com/wire/story/TWB20031201S0009*.

29. The AIM Global Network, *RFID and Homeland Security*, Dec. 2003, http://web.archive.org/web/20040505165547/http://www.aimglobal.org/technologies/rfid/resources/articles/dec03/homeland.htm.

30. *See Coping with Regulations*, RFID J., http://www.rfidjournal.com/magazine/article/910/1/100/definitions_off (last visited Mar. 31, 2008) (discussing the use of RFID to track food shipments as they are transported and identify any tampering); Posting of RFIDBLOGGER to RFID Law Blog, http://rfidlawblog.mckennalong.com/archives/drug-chain-security-fda-continues-to-push-for-rfid.html (Dec. 18, 2006) (noting that the FDA is pushing for the use of RFID technology to create an e-pedigree program for prescription drugs).

31. Nick Ferrell, *Stapler Gets RFID Make Over*, THE INQUIRER, Mar. 2, 2007, http://www.theinquirer.net/en/inquirer/news/2007/03/02/stapler-gets-rfid-make-over; Posting of Darren Murph to Engadget, http://www.engadget.com/2007/02/28/rfid-staples-omnipotent-pens-to-grace-offices-of-the-future (Feb. 28, 2007, 16:53 EST).

32. Rafael Ruffolo, *Alberta Company Brings RFID to Conference Badges*, ITBUSINESS.CA, June 20, 2007, http://www.itbusiness.ca/it/client/en/home/News.asp?id=44005&cid=5.

33. Austl. Privacy Found., *RFID Tags for School Children: Playing Tag? Or Taking Stock?*, http://www.privacy.org.au/Campaigns/RFIDSutter/ (last visited Feb. 06, 2008).

34. *Id.*

35. Marc L. Songini, *Minnesota Turns to RFID to Monitor Inmates*, COMPUTERWORLD, June 18, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024960&intsrc=news_ts_head (explaining that inmates know that they are monitored and are informed that the system is deemed to be extremely accurate).

36. Press Release, Alanco Techs., Inc., TSI Prism™ Prison Safety System Passes Comprehensive California Testing Program (Aug. 1, 2002), http://www.alanco.com/releases/073102.asp; *Using RFID to Track Prisoners*, RFID GAZETTE, Aug. 25, 2004, http://www.rfidgazette.org/2004/08/using_rfid_to_t.html.

Club in Barcelona began implanting an RFID microchip into a patron's arm for access into the VIP area of the club.[37] The chip is injected by a nurse using a syringe and a local anesthetic.[38] Lawmakers in the Indonesian province of Papua proposed a more ominous use by considering "selective use of [RFID] chip implants in HIV carriers to monitor their behaviour in a bid to keep them from infecting others."[39] There are approximately 3,000 people in Papua with HIV/AIDS out of a population of approximately 2.5 million.[40] In early 2007, Kodak filed an application for a patent on a digestible RFID tag.[41] The tag is ingested and ultimately dissolves in the body.[42] Although Kodak has not identified any specific plans for use of the tags, the patent application states that the devices can be used to "monitor internal bodily events."[43]

RFID technology is slowly making its way into the workplace where it can be used to track employees. For less than a thousand dollars, WaspTime, a product of Wasp Barcode Technologies, offers an RFID time and attendance system that includes an RFID time clock and twenty-five employee badges.[44] Control Module, a leading biometric workforce management and data collection technology provider, tracks employee time and attendance, and utilizes access control to keep unauthorized individuals from certain facilities and equipment.[45] Similarly, ActiveWave, Inc. offers RFID employee and passenger tracking systems for airports, railway stations, and passenger bus terminals; those systems require individuals to wear a clip-on badge, wristband, or badge with a necklace.[46] A comprehensive time and attendance system for employees is available from Absolute, located in Dubai, United Arab Emirates, offering the ability to:

1) Track and maintain employee attendance records;
2) Identify attendance exceptions such as tardiness and absenteeism;
3) Reduce or eliminate unwanted/unauthorized overtime by

37. Belle Mellor, *Wireless Incorporated: Gizmos Are Starting to be Slipped Inside People*, THE ECONOMIST, Apr. 26, 2007, at 15, *available at* http://www.economist.com/specialreports/displaystory.cfm?story_id=9032014.

38. *Id*.

39. *Microchips Mulled for HIV Carriers in Indonesia's Papua*, BREITBART, Jul. 24, 2007, http://www.breitbart.com/article.php?id=070724075657.4w2f978g&show_article=1.

40. *Id*.

41. Marc L. Songini, *Open Wide: Kodak Looks to Patent Edible RFID*, COMPUTERWORLD, Feb. 27, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011940&source=rss_news50.

42. *Id*.; *see also* System to Monitor the Ingestion of Medicines, U.S. Patent Appl. No. 11/351,140 (filed Feb. 9, 2006) (requesting a patent for an RFID tag that is attached to medicine and ingested).

43. Songini, *supra* note 41. The tags are used to monitor "bodily events," eliminating the need for surgery, x-rays, or access to a medical facility. *Id.* Such tags would allow probing of the body "without the effort expense, inconvenience, and risk of injury or infection involved with the above methods." *Id.*

44. WaspTime, RFID Time and Attendance System, http://www.waspbarcode.com/wasptime/wasptime_premium.asp (last visited Mar. 31, 2008).

45. Press Release, Control Module, Inc., Control Module Introduces First RFID Offering in Workforce Management Category (Jan. 8, 2007), http://www.controlmod.com/pdfs/pr_releases/RFID_Release.pdf.

46. ActiveWave, Inc., Airports and High Security, http://www.activewaveinc.com/applications_airport_security.php (last visited Aug. 26, 2008).

managing labor resources in real time, and eliminate 'Buddy-clocking';

4) Track, view, and report employee information in true, interactive real-time;
5) Generate detailed and summary reports/timesheets for each employee, including calculating daily and weekly overtime;
6) Measure employee behavior and enforce corporate HR and Health and Safety policies consistently through violation tracking;
7) Automate the most complex rules for accumulating vacation, sick time, and other types of benefit leave;
8) Provide real-time insight into ongoing labor costs and labor productivity with enhanced reporting capabilities;
9) Provide connectivity across wide area networks linking multiple locations to one centralized database through a true client-server; and
10) Provide for ease of maintenance and system upgrades through a central "browser" application.[47]

Although the use of RFID technology in the workplace is not yet widespread, there are several current applications of RFID that illustrate a range of potential uses. At the Dubai International Airport extension project, RFID technology is being used on a very large scale to track over 9,000 workers, from laborers to the highest management, who are all wearing green RFID tags.[48] The Star City Casino in Sydney, Australia manages a wardrobe inventory of 80,000 uniforms valued at approximately $1.8 million, and had a "laundry-tracking problem."[49] The solution from Accenture: embed RFID tags in the waistband, shirttail, or collar of each uniform.[50] From the point when the uniforms are issued to the point when they are turned back to the laundry, each uniform has a discrete identity that is tracked by strategically placed readers.[51] In the United States, at the security firm CityWatcher.com, the CEO and founder of the company and two employees have a microchip embedded in their forearm, which allows them entry into the company's data center, housing servers.[52] The RFID microchips are about the size of a grain of rice.[53] Known as "smart tags," the devices called VeriChips are apparently the first and only patented, FDA-approved implantable microchip with skin-

[47] Absolute, TimemaX (RFID), http://www.absolute-it.com/DisplayPage.aspx?PageID=104 (last visited Mar. 31, 2008).

48. *Keeping Tabs*, FACILITIES MGMT. MAG., Feb. 9, 2006, at 30, 30–31, *available at* http://www.absolute-it.com/rfid.pdf.

49. ACCENTURE, STAR CITY CASINO CASE STUDY (2002), http://www.accenture.com/Global/Services/By_Subject/Radio_Frequency_Identification/Client_Successes/StarCityCasino.htm.

50. *Id.*

51. *Id.*

52. *RFID Gets Under Their Skin*, ACCESS CONTROL & SECURITY SYS., Mar. 1, 2006, http://securitysolutions.com/mag/security_rfid_gets_skin/.

53. *Id.*

sensing capabilities.[54] Similarly, workers at the organized crime division of the Mexican Justice Ministry Office in Mexico City use VeriChips to access high-security areas.[55] At the Oak Ridge National Laboratories in Tennessee, RFID is used in an evacuation and monitoring accountability system to track whether employees have evacuated during an emergency and, if not, to let rescuers know where employees remain in the building.[56]

One of the newest developments in RFID workplace use is technology that provides real time location systems ("RTLS").[57] RTLS are being hailed as essential safety devices that could be used by emergency personnel to locate individuals in the event of a disaster.[58] In 2005, Cisco Systems, Inc. launched a large-scale RFID application using a wireless RFID server that can track people and equipment.[59] The system, Wireless Appliance 2700, is able to track RFID tags down to a few meters and display them on a central map.[60] Tags embedded in employees' uniforms can sound alarms if the tag moves out of a predefined area.[61] Most recently, in May 2007, Cisco initiated RTLS with the help of AeroScout, a pioneer in this aspect of RFID technology.[62] "The tags broadcast a signal, which is received by three reader antennas. The time each signal is received is passed on to a software system that uses triangulation to calculate the location of the asset."[63] In the application for Cisco, AeroScout tags "communicate with the Cisco Unified Wireless Network, which is also integrated with AeroScout's MobileView,"[64] providing very effective tracking of "key assets and people."[65]

54. Kathy Gurchiek, *Security Gets Under Employees' Skin*, HR MAG., Apr. 2006, at 32, 32; Daniel Sieberg, *Is RFID Tracking You?*, CNN, Oct. 23, 2006, http://www.cnn.com/2006/TECH/07/10/rfid/index.html.

55. *RFID Chips Under the Skin Can Open Doors*, GSN: GOV'T SECURITY NEWS, Mar. 18, 2006, at 7, *available at* http://www.verichipcorp.com/images/GSN_Mar06.pdf.

56. Press Release, Oak Ridge Nat'l Lab., ORNL Scores Hit with Nat'l Geospatial Intelligence Agency (Feb. 1, 2007), http://www.ornl.gov/info/press_releases/get_press_release.cfm?ReleaseNumber=mr20070201-00.

57. *See* Bert Moore, *RFID: Safety First*, RFID CONNECTIONS, Aug. 16, 2007, http://www.aimglobal.org/members/news/anmviewer.asp?a=2787&print=yes (discussing alternate approaches to using a facility's existing RTLs).

58. *Id*.

59. Iain Thomson, *CISCO Slammed for RFID Staff Tracker*, VNUNET.COM, May 4, 2005, http://www.vnunet.com/vnunet/news/2127277/cisco-slammed-rfid-staff-tracker.

60. *Id.*

61. *Id.*

62. Simon Holloway, *Real Time Location Systems are the New Buzz in RFID*, THE REG., Aug. 21, 2007, http://www.theregister.co.uk/2007/08/21/aeroscout_location_systems/print.html (discussing Cisco's recent actions and the reaction of privacy groups to those activities).

63. *Id*.

64. MobileView is an AeroScout application that organizes raw data gathered from tags into a user friendly format. *See* AeroScout Enterprise Visability Solutions, AeroScout MobileView 4.0: Enterprise Software for Unified Asset Visibility, http://www.managingautomation.com/maonline/directory/product/MobileView_4_228514?CurrentCat=17314&dirld=1 ("MobileView turns asset visibility information received from a wide variety of data sources into real business solutions, delivering sophisticated mapping, rules-based alerting and reporting functions in a scalable, enterprise-proven software platform.") (last visited Aug. 26, 2008).

65. Holloway, *supra* note 62.

B. Security and Safety Issues

Whenever new technology is introduced, particularly when it can yield information about a person's whereabouts, concerns are raised.[66] Even if a legitimate reason for the tracking is proffered, there are still concerns about misuse of the data. In the case of RFID, recent information about a link between RFID chips and cancer is also prompting serious inquiry into the safety of using chips in humans.[67] In a speech at Georgetown Law Center, Senator Patrick Leahy encapsulated the main concerns about RFID:

> With RFID technology as with many other surveillance technologies, we need to consider how it will be used, and will it be effective. [sic] What information will it gather, and how long will that data be kept? Who will have access to those data banks, and under what checks-and-balances? Will the public have appropriate notice, opportunity to consent and due process in the case mistakes are made? How will the data be secured from theft, negligence and abuse, and how will accuracy be ensured? In what cases should law enforcement agencies be able to use this information, and what safeguards should apply? There should be a general presumption that Americans can know when their personal information is collected, and to see, check and correct any errors.[68]

The questions raised are being echoed and underscored by many consumer and privacy advocates, such as the American Civil Liberties Union,[69] Privacy Rights Clearinghouse,[70] and the Electronic Frontier Foundation.[71] The major concerns about using RFID to track employees fall into the following three categories: surveillance by any person with access to the reader or database, "profiling" or maintaining a profile on a "target" based on the information gathered, and actions that may be taken based on information collected by using an RFID device.[72]

---

66. *See generally* Serena G. Stein, *Where Will Consumers Find Privacy Protection from RFIDS?: A Case for Federal Legislation*, 2007 Duke L. & Tech. Rev. 3 (2007) (discussing the use of RFID to track consumers and privacy issues).

67. Barnaby J. Feder, *Report of Cancer Hurts Maker of Chip Implants*, N.Y. TIMES, Sept. 11, 2007, at C9 (examining the health concerns associated with RFID).

68. Patrick Leahy, U.S. Senator, The Dawn of Micro Monitoring: Its Promise, and Its Challenges to Privacy and Security, Remarks at the Georgetown University Law Center, Conference on Video Surveillance: Legal and Technological Challenges (Mar. 23, 2004), *available at* http://leahy.senate.gov/press/200403/032304.html.

69. *See, e.g.*, ACLU, NAKED DATA: HOW THE U.S. IGNORED INTERNATIONAL CONCERNS AND PUSHED FOR RADIO CHIPS IN PASSPORTS WITHOUT SECURITY (2004), *available at* http://www.aclu.org/pdfs/privacy/nakeddata20041124.pdf (expressing concerns about putting RFID chips in passports).

70. Privacy Rights Clearinghouse, RFID Position Statement of Consumer Privacy and Civil Liberties Organizations (Nov. 20, 2003), http://www.privacyrights.org/ar/RFIDposition.htm (summarizing positions of various civil liberties organizations on RFID chips).

71. *See, e.g.*, Letter from Elec. Frontier Found. to the San Francisco Pub. Library Comm'n (Oct. 1, 2003), *available at* http:www.eff.org/files/ filenode/rfid/sfpl_comments_oct012003.pdf (raising privacy concerns about RFID tagging of library books).

72. *See generally* Peslak, *supra* note 13 (providing an overview of the privacy issues associated with RFID and approaches to addressing them). For an exploration of ethical issues regarding the use of technology in the workplace, see RICHARD T. DE GEORGE, THE ETHICS OF INFORMATION TECHNOLOGY AND BUSINESS

Even if employers can use RFID to track employees in the workplace without violating any laws,[73] employees may have concerns about the security of RFID systems from use by unauthorized individuals. In a well-publicized case, a security expert cracked one of the United Kingdom's new biometric passports and was able to siphon off information, leaving no evidence of tampering.[74] The chips in the passports currently contain the printed details on the passport and the person's photograph.[75] Eventually the British government wants to incorporate fingerprints and other biometric data on the chips.[76] The fact that someone was able to hack into these ostensibly "secure" chips is a source of great concern, especially in light of additional personal identifying data that may be stored on the chips. Another concern is that RFID tags will be vulnerable to viruses, just as computers have been under siege.[77] Moreover, at least one expert claims that he can clone RFID-enabled badges,[78] the use of which would distort information gathered using the RFID technology.

Other security concerns pertain to the lack of reliability of systems. In February 2007, the United States Department of Homeland Security decided to stop "using RFID in its US Visitor and Immigration Status Indicator Technology . . . program after the technology's read rates proved inadequate."[79] Moreover, there are concerns that a shortage of RFID professionals can be a hindrance to adoption and effective use of RFID technology.[80]

In addition to these concerns, a recent report suggested that VeriChip and federal regulators either ignored or overlooked animal studies indicating that RFID chips implanted in dogs and laboratory rodents could cause cancer.[81] This would be a very significant and adverse development for VeriChip as they seek to broaden the use of RFID for human tracking.[82] VeriChip reportedly will undertake independent studies to determine if there is a correlation between the implants and cancer.[83] As of September 2007, approximately 2000 humans have an RFID implant, and the largest producer of these chips

(2003).

73. *See infra* Part III.

74. Jeremy Kirk, *Crack! Security Expert Hacks RFID in UK Passport*, COMPUTERWORLD, Mar. 6, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9012406&source=NLT_AM&nlid=1.

75. *Id*.

76. *Id*.

77. Jeremy Kirk, *RFID Tags Vulnerable to Viruses, Study Says*, COMPUTERWORLD Mar. 15, 2006, http://www.computerworld.com/mobiletopics/mobile/story/0,10801,109560,00.html.

78. Dennis Fisher, *RFID Cloning Presentation Moves Forward Despite Legal Threats*, SEARCHSECURITY.COM, Mar. 1, 2007, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1245778,00.html.

79. *RFID Border Tracking Plagued by Low Read Rates*, RFID UPDATE, Feb. 20, 2007, http://www.rfidupdate.com/articles/index.php?id=1301.

80. Mary Catherine O'Connor, *Two Studies Describe the RFID Workforce*, RFID J., June 7, 2007, http://www.rfidjournal.com/article/articleview/3389 .

81. Feder, *supra* note 67, at C9.

82. *Id*.

83. *Id*.

hopes there could be a market as large as 45 million Americans.[84]

III. UNITED STATES LAW

Despite concerns about the use of RFID technology, there are currently no federal laws and only a few state laws regulating its use in the workplace by private employers.[85] At the core of the concerns is the inevitable legal question of whether there is a reasonable expectation of privacy in the workplace regarding the use of this technology to track employees.[86] At this point, most nongovernment employees in the United States are exposed to a variety of forms of monitoring, including drug testing, closed circuit video filming, monitoring calls with clients or customers, monitoring e-mail and computer input and transmissions, using GPS systems in company cars and company phones, and personality and psychological testing.[87] There is no comprehensive right to privacy for employees in American workplaces regarding electronic monitoring.[88] As such, in the current legal landscape it would be an uphill battle for employees to argue that tracking movement within the workplace using RFID chips would violate any reasonable expectation of privacy.[89]

To the extent that RFID is used by any government employers, there are Fourth Amendment search and seizure considerations under the United States Constitution.[90] Even the Fourth Amendment, however, is not sufficient to prevent the use of RFID for public employees. To the extent that a public employer argues that it has a reasonable, work-related need to use RFID, and the scope of the use of the technology does not exceed what is necessary to fulfill the employer's needs, RFID may arguably be used to track public

84. Todd Lewan, *Chip Implants Linked to Animal Tumors*, WASH. POST, Sept. 8, 2007, http://www.washingtonpost.com/wp-dyn/content/Article/2007/09/08/AR2007090800997_pf.html.

85. *See infra* text accompanying notes 98-104.

86. Corey A. Ciocchetti, *Monitoring Employee E-mail: Efficient Workplaces vs. Employee Privacy*, 2001 DUKE L. & TECH. REV. 26, 1 (2001).

87. There are many articles generally discussing workplace privacy. *E.g.*, *id.*; Micah Echols, *Striking a Balance Between Employer Business Interests and Employee Privacy: Using Respondeat Superior to Justify the Monitoring of Web-Based, Personal Electronic Mail Accounts of Employees in the Workplace*, 7 COMP. L. REV. & TECH. J. 273 (2003); Pauline T. Kim, *Collective and Individual Approaches to Protecting Employee Privacy: The Experience with Workplace Drug Testing*, 66 LA. L. REV. 1009 (2006); Gail Lasprogata et al., *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH. L. REV. 4 (2004); Amanda Richman, *Restoring the Balance: Employer Liability and Employee Privacy*, 86 IOWA L. REV. 1337 (2001); Michael L. Rustad & Sandra R. Paulsson, *Monitoring Employee E-mail and Internet Useage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe*, 7 U. PA. J. LAB. & EMP. L. 829 (2005).

88. For a discussion about laws regarding monitoring of employees performance and conduct, *see* MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW 213–350, 357–62 (2d ed. 2003) (illustrating different methods of regulating employees' conduct, i.e. drug testing, polygraph testing, and access to personnel records).

89. *See generally* Jennifer E. Smith, *You Can Run, but You Can't Hide: Protecting Privacy from Radio Frequency Identification Technology*, 8 N.C. J. L. & TECH. 249 (2007) (discussing privacy implications of widespread RFID use and arguing for regulation).

90. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 188–209 (2004); Dalal, *supra* note 13, at 495–506.

employees.[91]

It is worth noting, however, that there has been some federal action regarding the use of RFID in contexts other than employment. The Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 ("SAFETY Act") encourages the development and deployment of new and innovative anti-terror products and services.[92] This legislation eliminates or minimizes tort liability for companies that sell or provide anti-terror technology approved by the Department of Homeland Security.[93] To the extent that RFID products can be used to track products and minimize the possibility of a terror attack, they may qualify as a covered product under the SAFETY Act.[94] To the extent that RFID is used for medical purposes, the strict requirements of the Health Insurance Portability and Accountability Act ("HIPAA") are triggered.[95] Privacy and security rules under HIPAA have strict restrictions on the disclosure and use of health information.[96] Further, the Federal Trade Commission ("FTC") has discretionary authority to prohibit deceptive or unfair practices in, or affecting, commerce.[97] At this point, the FTC supports industry initiatives to address privacy concerns (e.g. putting consumers on notice) and supports consumer education, but it has not taken any steps to issue specific guidelines about the use of RFID technology.[98]

Given the lack of federal law regulating RFID technology, there has been a good bit of discussion and proposal at the state legislative level.[99] To date, a number of states have introduced legislation relating to the use of RFID.[100] Most of these proposed laws pertain to uses other than the employment context, although some expressly prohibit requiring an individual to undergo the implantation of a microchip.[101]

A limited number of states have enacted legislation that limits the use of RFID in various contexts. The earliest of those laws were in Wyoming and

---

91. *See* O'Connor v. Ortega, 480 U.S. 709, 714–18 (1987) (considering what is a reasonable search by a public employer under the Fourth Amendment).

92. Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, Pub. L. No. 107-296, § 862(b)(7), 116 Stat. 2135, 2239 (1996) [hereinafter SAFETY Act], *available at* https://www.safetyact.gov/DHS/SActHome.nsf/Main?OpenFrameset&6HLD82.

93. Interview by John Havens with Raymond Biagini, Leader with Product Liability Defense Practice, McKenna, Long and Aldridge (June 28, 2007), *available at* http://www.aimglobal.org/members/news/templates/template.aspx?articleid=265.

94. *Id*.

95. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110, § 1172(c)(2), 110 Stat. 1936 (1996).

96. *See generally* Lisa J. Sotto, *An RFID Code of Conduct*, RFID J., May 30, 2005, http://www.hunton.com/files/tbl_s47Details/FileUpload265/1128/RFIDJrnl-Lisa_Sotto_5.30.05.pdf (arguing that RFID stakeholders should develop a code of conduct to prevent misuse of medical information in connection with RFID technology).

97. Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) (2007).

98. FTC REPORT, *supra* note 14, at 21–23.

99. RFID and Privacy, Federal & State Government, http://rfidprivacy.mit.edu/access/happening_legislation.html (last visited Mar. 31, 2008).

100. *Id*. (including Alabama, Illinois, Maryland, Massachusetts, Missouri, New Hampshire, California, New York, Rhode Island, and South Dakota).

101. *See, e.g.*, H.B. 4088, 94th Gen. Assem. (Ill. 2005) (providing hospitals must use RFID tag); H.B. 1114, 2005 Leg., 80th Sess. (S.D. 2005) (restricting the use of RFID in humans).

Utah. Amendments[102] to the Wyoming Pharmacy Act authorized telepharmacies to use automated inventory control, including RFID.[103] Just over a week later, on March 11, 2005, the Utah Computer Crimes Act Amendments (H.B. 185)[104] were signed by the governor.[105] The Utah law makes it clear that computer crimes apply to wireless networks, and importantly for proponents of RFID, exempts from the Computer Crimes Act certain collections of information through the use of RFID technology by retailers to identify, track or price goods located within the retailer's location.[106] In a departure from these laws protecting the use of RFID, Wisconsin was the first state to ban required human RFID chipping.[107] Effective May 30, 2006:

> (1) No person may require an individual to undergo the implanting of a microchip.
>
> (2) Any person who violates sub. (1) may be required to forfeit not more than $10,000. Each day of continued violation constitutes a separate offense.[108]

The passage of this law immediately gave rise to questions.[109] For example, under what circumstances is chipping "required"? If it is a condition of continued employment, and the individual consents to avoid losing her job, would it violate the law?

State legislative attempts to limit and regulate the use of RFID technology gained more momentum in 2007. In early spring, Washington state seriously considered House Bill 1031.[110] This Electronic Bill of Rights would have required parties to obtain consent from consumers "before using RFID to collect, maintain and disclose information" on them.[111] Soon thereafter, in April 2007, North Dakota passed a ban on requiring implants in individuals.[112] The law states that a "person may not require that an individual have inserted into that individual's body a microchip containing a radio frequency identification device."[113] Violations of this statute are a misdemeanor

---

102. H.B. 0258, 58th Leg., 2005 Gen. Sess. (Wyo. 2005).

103. WYO. STAT. ANN. § 33-24-156 (2007).

104. H.B. 185, 2005 Gen. Assem. (Utah 2005), *available at* http://www.le.state.ut.us/~2005/bills/hbillenr/hb0185.pdf.

105. Press Release, Jon M. Huntsman, Jr., Governor of Utah, Governor Huntsman Signed More Bills Today (Mar. 11, 2005), *available at* http://www.utah.gov/governor/news/2005/news_03_11a_05.html.

106. UTAH CODE ANN. §§ 76-6-702, 76-6-703 (2007).

107. Orr Shtuhl, *California Could Become Third State to Ban Forced Microchip Tag Implants (RFID)*, GLOBAL RESEARCH, Jan. 12, 2008, http://www.globalresearch.ca/index.php?context=va&aid=7781.

108. WIS. STAT. § 146.25 (2007).

109. *See, e.g.* RFID Law Blog, Wisconsin Bans Compulsory RFID Surgery, June 2, 2006, http://rfidlawblog.mckennalong.com/archives/state-legislation-wisconsin-bans-compulsory-rfid-surgery.html.

110. Mary Catherine O'Connor, *Washington's RFID Bill Halted*, RFID J., Mar. 23, 2007, http://www.rfidjournal.com/article/articleview/3168/.

111. *Id.* Note that, because the bill was not placed on the House legislative floor early enough, it will not be heard by the full House in 2007. *Id.*

112. Marc L. Songini, *North Dakota Band Forced RFID Chipping*, COMPUTERWORLD, Apr. 12, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=15&articleId=9016385&intsrc=hm_topic.

113. S. 2415, 60th Legis. Assem., Reg. Sess. (N.D. 2007), *available at* http://www.legis.nd.gov/

crime.[114] Again, the literal language of this statute raises questions about what constitutes "required" chipping, as well as whether a swallowed RFID device is within the scope of the law.[115] Most recently, on May 24, 2007, the California Senate overwhelmingly passed the Identity Information Protection Act.[116] The Act requires privacy and security measures for RFID tags.[117] California Senator Joe Simitian introduced the bill in December 2006, focusing on four measures: (1) prohibiting an employer from implanting chips in workers; (2) blocking RFID technology from being embedded in driver's licenses; (3) prohibiting schools from issuing ID cards to track student attendance; and (4) making it a misdemeanor to skim ID cards.[118] Senate Bill 362 became law in October 2007.[119] As public concern grows over the use of RFID, more states are likely to pass similar legislation in their upcoming sessions.

IV. INTERNATIONAL PERSPECTIVES

In 1997, the International Labour Organization ("ILO") of the United Nations published a nonbinding Code of Practice for the protection of workers' personal data, which addresses concerns about the potential for misuse of workers' personal information; the guidelines address collection, security, storage, use, and communication of this data.[120] At the core of its general principles is the requirement that limits the collection of data to that which is "directly relevant to the employment of the worker."[121] These general principles are reflected in the Resolution on Radio-Frequency Identification, which was adopted at the 25th International Conference of Data Protection and Privacy Commissioners in November 2003.[122] The resolution states that basic principles of data protection and privacy law must be observed when designing, implementing, and using RFID technology, specifically:

> a) any controller—before introducing RFID tags linked to personal information or leading to customer profiles—should first consider alternatives which achieve the same goal without collecting personal information or profiling customers;
>
> b) if the controller can show that personal data are indispensable, they

assembly/60-2007/bill-text/HBPJ0300.pdf.

114. *Id.*

115. *Id.*

116. S.B. 30, 2007 Leg., Reg. Sess. (Cal. 2007).

117. *Id.*

118. Note that "skimming" is a method used by identity thieves to secretly read cards and obtain that individual's personal information. *Identity Theft: How to Protect and Restore your Good Name, Hearing Before the Subcomm. on Tech., Terrorism, and Gov't Info. of the S. Comm. on the Judiciary*, 106th Cong. 18 (2000) (testimony of Jodie Bernstein, Dir., Bureau of Consumer Protection, Fed. Trade Comm'n).

119. 2007 Cal. Stat. 538.

120. INT'L LABOUR ORG., PROTECTION OF WORKERS' PERSONAL DATA, 1–3, 15–22 (1997), *available at* http://www.ilo.org/public/english/protection/condtrav/pdf/wc-code-97.pdf.

121. *Id.* at 2.

122. INT'L CONFERENCE OF DATA PROT. & PRIVACY COMM'RS, RESOLUTION ON RADIO-FREQUENCY IDENTIFICATION 1 (2003), *available at* http://www.privacyconference2003.org/resolutions/res5.DOC.

> must be collected in an open and transparent way;
> c) personal data may only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve (or carry out) this purpose, and
> d) whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags.[123]

Against this backdrop of general principles, nations in addition to the United States are exploring the best practices and legal guidelines that should be implemented to regulate the use of RFID. Countries such as Canada, Australia and countries in the EU, maintain active discussions on RFID. These jurisdictions are discussed to provide an international comparison.

A. Canada

Canada's private-sector privacy law, the Personal Information Protection and Electronic Documents Act ("PIPEDA"), protects the information of employees working for companies operating in federally regulated sectors, including telecommunications, broadcasting, inter-provincial transportation, aviation, banking, nuclear energy, maritime navigation, and shipping.[124] Similarly, Canada's Privacy Act imposes obligations on some 150 federal government departments and agencies to respect privacy rights by limiting the collection, use, and disclosure of personal information.[125] Consistent with the requirements of these laws, a 2004 Report by Ann Cavoukian, Ontario, Canada's Information and Privacy Commissioner, emphasizes three major principles that must be respected by any deployment and use of RFID systems to comply with Canada's Fair Information Practices law:

> (1) Notice and Consent – The right to know whether a product contains an EPC RFID tag and whether an RFID reader is being used in a public place . . . .
> (2) Choice – The right to have the RFID tag in a purchased product deactivated without cost.
> (3) Control – The right to have personal identity information kept separate from information identifying an object.[126]

Additionally, the report identifies eight other principles that are essential to achieve full informational privacy: Collection Limitations, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability.[127]

---

123. *Id*. at 1.

124. *See* Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5 (Can.), *available at* http://laws.justice.gc.ca/en/P-8.6/258031.html (establishing the right to protection of information collected electronically).

125. Privacy Act, R.S.C., ch. P-21 (1985), *available at* http://laws.justice.gc.ca/en/P-21/index.html.

126. ANN CAVOUKIAN, TAG, YOU'RE IT: PRIVACY IMPLICATIONS OF RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY 20 (2004), *available at* http://www.ipc.on.ca/images/Resources/up-rfid.pdf.

127. *Id*. at 21.

Echoing the importance of these principles, a speech by Canadian Privacy Commissioner Jennifer Stoddart notes that employers need to "start thinking more about workplace privacy and the potential implications of emerging surveillance technologies."[128] Citing the 2006 research report, "Under the Radar? The Employer Perspective on Workplace Privacy," Stoddart expressed her disappointment about some of the employer attitudes about workplace privacy.[129] The report finds that some see workplace privacy as a privilege granted to employees; no one agreed with the idea that workers are entitled to a certain measure of privacy that cannot be taken away.[130] Moreover, Stoddart notes a survey that found that there is a gap between what "employers and employees think is an acceptable privacy practice."[131] Emphasizing her concern about the "effects" that privacy-invasive measures could have "on the dignity of employees," Stoddart called for a balance between the "rights of the individual to privacy and the needs of organizations to collect, use or disclose personal information."[132] In 2006, Ontario's Information and Privacy Commissioner released a comprehensive set of guidelines for using RFID systems.[133] The guidelines are based on three major principles: (1) focusing on RFID systems rather than technologies (i.e. if the deployment of the systems raises privacy concerns); (2) building in privacy and security measures early in the design of the system, including minimizing the "identifiability, observability, and linkability of RFID tags with personal information;" and (3) maximizing individual participation and consent, and enabling individuals to make informed decisions about the use of RFID systems affecting them.[134] Additionally, it should be noted that Canada also has other private sector personal data protection legislation in Quebec,[135] British Columbia,[136] and Alberta,[137] which supplement PIPEDA.[138]

---

128. Jennifer Stoddart, Privacy Comm'r of Canada, Finding the Right Workplace Privacy Balance, Address at the Ryerson University Workshop on Workplace Privacy (Nov. 30, 2006), *available at* http://www.privcom.gc.ca/speech/2006/sp-d_061130_e.asp.

129. *Id.* (citing AVNER LEVIN ET AL., UNDER THE RADAR? THE EMPLOYER PERSPECTIVE ON WORKPLACE PRIVACY (2006)), *available at* http://www.ryerson.ca/tedrogersschool/news/archive/UnderTheRadar.pdf (discussing two conceptual approaches to workplace privacy in Canada).

130. LEVIN ET AL., *supra* note 129.

131. Stoddart, *supra* note 128.

132. *Id*.

133. ANN CAVOUKIAN, PRIVACY GUIDELINES FOR RFID INFORMATION SYSTEMS (2006), *available at* http://canada.ihs.com/NR/rdonlyres/9C4250F8-0C18-4E2D-A605-1F7F8643BE70/0/rfidgdlines.pdf.

134. *Id*. at 2.

135. Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., ch. P-39.1 (2007), *available at* http://www.canlii.org/qc/laws/sta/p-39.1/20030911/whole.html.

136. Personal Information Protection Act, S.B.C., ch. 63 (2003), *available at* http://www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm.

137. Personal Information Protection Act, S.A. ch. P-6.5 (2003), *available at* http://www.qp.gov.ab.ca/documents/Acts/P06P5.cfm?frm_isbn=0779725816.

138. *See generally* TERESA SCASSA ET AL., OFFICE OF THE PRIVACY COMM'R OF CAN., AN ANALYSIS OF LEGAL AND TECHNICAL PRIVACY IMPLICATIONS OF RADIO FREQUENCY IDENTIFICATION TECHNOLOGIES, 4 n.16, 50 (2005), *available at* http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf (identifying supplemental jurisdiction that has been enacted in individual provinces).

B. European Union

Similar to discussions in the United States and Canada, the EU is actively considering what restrictions, if any, should be placed on the use of RFID technology.[139] Although one might think that EU Directive 95/46/EC, which restricts the processing and movement of certain forms of data on individuals,[140] might automatically restrict the use of RFID technology, the issue is far from resolved in the EU. In January 2005, an Article 29 Working Party[141] on data protection issued a working document studying privacy concerns related to the use of RFID technology in the EU.[142] The Working Party expressed concern "about the possibility for some applications of RFID technology to violate human dignity as well as data protection rights."[143] The report specifically cited concerns "about the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals" through their "ability to surreptitiously collect" data on the same person in multiple venues.[144] Heading off public concern, the European Commission ("Commission"), the executive branch of the EU, explained that its role is to "help build a cross-society consensus on technical, legal and ethical issues associated with RFID and to intervene, where required, with regulatory instruments."[145] In so doing, it cited a number of questions associated with the use of the technology such as: "how do we credibly ensure that RFID tags are not abused to invade the privacy of consumers? Do we need to destroy an RFID tag when it could be useful for self-configuring products (built from autonomous components and assemblies), automating warranty checks, etc.?"[146]

These initial concerns made it appear as if the EU might issue comprehensive, restrictive policies about the use of RFID technology to protect the privacy of its citizens. In a 2006 speech, Viviane Reding, the member of the Commission who is responsible for Information Society and Media, advocated for a set of European rules for safe and secure development of RFID technology.[147] Thereafter, in March 2007, the Commission issued a report

139. *See EU Opts for Hands-off Approach to RFID Regulation*, RFID UPDATE, Mar. 16, 2007, http://www.rfidupdate.com/articles/index.php?id=1319 [hereinafter *Hands-off Approach*] (discussing the EU's proposed regulation of RFID).

140. Council Directive 95/46, art. 13 1995 O.J. (L 281) 31 (EC), *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

141. An Article 29 Working Party is a working party established by the European Communities to give advice about privacy protection in the European Community and other countries. *Id.* arts. 29, 30, at 48–49.

142. ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO RFID TECHNOLOGY 2 (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

143. *Id*.

144. *Id*.

145. Press Release, European Commission, Information Society, Radio Frequency Identification Devices (RFID): Frequently Asked Questions on the Commission's Public Consultation (Oct. 16, 2006), *available at* http://ec.europa.eu/information_society/newsroom/cf/itemshortdetail.cfm?item_id=2927.

146. *Id*.

147. Viviane Reding, Member, Comm'n for Info. Soc'y & Media, RFID: Why We need a European Policy, Address at the EU RFID 2006 Conference: Heading for the Future (Oct. 16, 2006), *available at*

proposing a "European policy strategy" for using smart radio tags.[148] According to the report, the Commission will "[c]reate in 2007 an RFID Stakeholder Group to provide advice and assistance to the Commission in developing a European policy position concerning RFID applications."[149] The work of this group is to be "carried out in association with, among others, the Article 29 Data Protection Working Party."[150] By mid 2007, the Commission was to propose amendments to the e-Privacy Directive to take account of RFID applications, as part of the EU Telecom Rules' review.[151] The Commission also planned to publish—by the end of 2007—an assessment of policy options and a recommendation to Member States and stakeholders on how to handle data security and privacy of smart radio tags.[152]

Industries utilizing identification technologies viewed the RFID report as a welcome development because, at least for the time being, the EU will use self-regulation and existing laws to manage RFID technology.[153] Although the EU opted against formal legislation and will move forward with what is characterized as "soft law"—i.e., the Commission is developing a set of security and privacy guidelines for the RFID industry—this still seems to be a very positive signal for those seeking to use RFID.[154] In fact, U.S. Department of Commerce Under Secretary for Technology Robert Cresanti "characterized the EU decision as a 'big victory,' making a nod to free-market economics that advocates less governmental intervention in matters of commerce."[155]

It should be noted that, in addition to the action being considered in the EU, some member nations have their own initiatives. For example, in France the data protection authority, *la Commission nationale de l'informatique et des libertés* ("CNIL"), is monitoring RFID use, as it considers RFID chips to be "personal identifiers" within the meaning of the 6 January 1978 Act and the EU 95/45 Directive.[156] As such, the CNIL is already advising all employers to ensure that employees are fully informed on any use of RFID in employee badges, and it calls for workers to have access to their own data records.[157] In the United Kingdom, the Information Commissioner's Office is making recommendations in its Employment Practice Code similar to those referenced

---

http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/06/597&format=HTML&aged=1&language=EN&guiLanguage=fr.

148. Press Release, EU Commission, Commission Proposes a European Policy Strategy for Smart Radio Tags (Mar. 15, 2007), *available at* http://www.europa.eu/rapid/pressReleasesAction.do?reference=IP/07/332&format=HTML&aged=0&language=EN&guiLanguage=en.

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.*

153. *Hands-off Approach*, *supra* note 139.

154. *EU's Decision Not to Legislate RFID Is Conditional*, RFID UPDATE, Apr. 4, 2007, http://www.rfidupdate.com/articles/index.php?id=1332.

155. *US Considers EU Decision on RFID a "Big Victory,"* RFID UPDATE, Apr. 10, 2007, http://www.rfidupdate.com/articles/index.php?id=1335.

156. Press Release, *La Commission nationale de l'informatique et des libertés*, Radio-Identifiers (Aug. 31, 2004), *available at* http://www.cnil.fr/index.php?id=1514.

157. Andrew Bibby, *Invasion of the Privacy Snatchers*, FIN. TIMES, Jan. 8, 2006, at 10, *available at* http://www.andrewbibby.com/misc/rfid.html.

in France.[158] The British union G.M.B. recently argued that requiring some workers in retail distribution centers to wear RFID tags was dehumanizing, turning workplaces into "battery farms."[159] Additionally, in Germany, before any technological device is used to monitor workers, permission must be obtained from the company's works council pursuant to the labor law.[160]

C. Australia

The RFID Association of Australia ("RFIDAA") is an independent association supported by the government with the goal of creating a "strong, dynamic and informed Australian RFID market."[161] In Australia, 60 percent of the RFID technology market is in security and access control and animal applications.[162] Encompassed within the security and access category are applications for employee access tracking.[163] The most celebrated use in the employment context is by the Star City Casino in Sydney where RFID tags are sewn into employee uniforms.[164]

In 2006, the RFIDAA worked with Booz Allen Hamilton, a leading consulting firm, to survey the views and position of the government regarding the adoption of RFID technology.[165] The Booz Allen Hamilton study showed that "less than 30% of Australian government departments gave RFID technology any priority in their business plan."[166] However, the study also revealed that 75 percent of the respondents plan to investigate or use RFID within three years.[167] In any event, the Australian Privacy Commissioner issued a report on developing technologies.[168] Although the report acknowledged that "RFID may help businesses improve the way they manage the supply of their products and so save consumers money," it also expressed concern that "[RFID chips] also have equal potential to invade personal

158. *Id.*

159. Christine Buckley, *This Is the Wrist Tag that Makes your Time at Work More Productive—or Turns You into a Robot*, TIMES, June 7, 2005, http://www.timesonline.co.uk/tol/news/uk/article530747.ece.

160. GERMAN FEDERAL OFFICE FOR INFORMATION SECURITY, SECURITY ASPECTS AND PROSPECTIVE APPLICATIONS OF RFID SYSTEMS 96 (2006), *available at* http://www.bsi.de/fachthem/rfid/RIKCHA_englisch_Layout.pdf (citing § 87 Abs. 1 Nr. 6 BetriebsVG, the relevant German law in a preface to a fictive case study).

161. RFID Ass'n Austl., http://www.rfidaa.org/ (last visited Apr. 1, 2008).

162. Paul Oswal, Editorial, *Australia RFID Applications*, HIGH TECH AIDCOURIER, Oct. 2005, http://www.hightechaid.com/newsletter/2005/Guest_Editorial-Oct05.htm.

163. *Id*.

164. Ben Woodhead, *Fast Track for Radio Tags*, AUST. IT, Oct. 3, 2006, http://www.australianit.news.com.au/story/0,24897,20500547-15302,00.html. The Star City Casino is also looking into using RFID gambling chips, allowing the casino to track individual gamblers and to reduce fraud. *Id.*

165. RFID Ass'n Austl., *supra* note 161.

166. BOOZ ALLEN HAMILTON, RFID YET TO REACH GOVERNMENT TIPPING POINT, www.boozeallen.com/news/14521943?1pid=827466 (last visited Apr. 1, 2008)

167. *Id.*

168. AUSTL. OFFICE OF THE PRIVACY COMM'R, SUBMISSION TO THE AUSTRALIAN LAW REFORM COMMISSION'S REVIEW OF PRIVACY—ISSUES PAPER 31 (2007), *available at* http://www.privacy.gov.au/publications/submissions/alrc/all.pdf.

privacy if deployed wrongly."[169]

Based on these concerns, the Office of the Privacy Commissioner stated that "all the basic principles of privacy law should be adopted when designing, implementing and using RFID technology."[170] In summary, the following observations and general guidelines were issued:

> [1] RFID tags should only be linked to personal information or used to profile customers if there is no other way of achieving the goal sought; [2] individuals should be fully informed if personal information is collected using RFID tags; [3] personal information collected using RFID tags should only be used for the specific purpose for which it is first collected and destroyed after that purpose is achieved; and [4] individuals should be able to delete information, or disable or destroy any RFID tag that they have in their possession.[171]

Thus, Australians share the same concerns about privacy and information that have been raised in the United States, Canada, and the EU.

V. PROPOSED RECOMMENDATIONS

Inasmuch as there is very little legislation regulating the use of RFID to track employees, and there is a good bit of public concern about the use of this technology, it is important for employers to thoroughly weigh the pros and cons before implementing an employee tracking system. Cavalier or imprudent use of this technology could lead to reactionary laws, which ultimately undermine what could be legitimate and reasonable uses of RFID in the workplace. Prudent use by employers could lead to more efficient and safe workplaces, and also stem employee fears. Ideally, employers using RFID will develop a code of conduct balancing the potential effective use of RFID in the workplace with privacy concerns of employees. Although RFID technology is not "one-size-fits-all" in terms of the applications in the employment context, the following nine recommendations are designed to help employers implement comprehensive and thoughtful procedures in the deployment of RFID systems to track employees.[172]

1. Assess Business Necessity and Legitimate Goals

The first step is for employers to review the proposed use of RFID technology to track employees to ensure that there is a business necessity and that using a less intrusive means would not serve the purpose of achieving the desired goal. Employers should reflect on whether the system is proportional to a lawful goal. These specific and limited purposes should be fully explained

169. *Id.* at 437.
170. *Id*.
171. *Id*. at 437–38.
172. Note that these recommendations incorporate and elaborate on considerations and recommendations expressed by the ILO, Canada, the EU, and Australia. *See supra* Part IV (discussing international approaches to RFID technology).

to the affected employees. Moreover, employers should circumscribe the scope of data collected; it should be limited to what is reasonably necessary for a legitimate business goal.

2. Obtain Informed Consent from Employees

Prior to collecting data, informed consent should be obtained from all employees subject to tracking. Specifically, they should be informed about: when, where, and why the RFID tag is being read; punitive or disciplinary measures that may be taken based on information gathered by using the RFID tag; and what will happen to the data when the employee leaves the employer, such as whether the tags will be deactivated or removed. Along these lines, at least two states have passed laws aimed at preventing (and criminalizing) forced implanting. Employees should not be coerced into RFID tracking through the use of implants. Lastly, there should be full disclosure of any medical uncertainties and safety concerns associated with implanted devices.

3. Address Security Concerns

Employers using RFID should deploy an appropriate level of security, including: encrypting data collected; establishing read-range limitations to minimize ability of tags to be read by unauthorized readers; and authenticating data to prevent unauthorized access to the information collected. The security of the RFID system should be assessed on a regular basis, including its vulnerability to viruses or other corruption of data.

4. Ensure Openness and Transparency

All policies and practices associated with the use of RFID in the workplace should be readily available to those who are affected by the deployment. This could be accomplished in employee handbooks, including online employee resources. It is particularly important for employees to be aware of punitive or disciplinary measures that may be taken based on information gathered by using the RFID tag. It should be clear that collected data will never be used to illegally discriminate against individuals or groups of workers.

5. Provide Employee Access to Records

Employees should have reasonable and timely access to the RFID data collected on their whereabouts. Employee access to records will help obviate concerns about the content of the records, including fears about inaccurate data. Additionally, employee access would reduce employee feelings about lack of control over the monitoring.

6. Mandate Accountability

One individual should be designated to ensure compliance with internal procedures, as well as to answer employee questions and train employees on uses and restrictions of the tracking system. To the extent that any external service providers are used to collect and process data, they should be supervised by a designated individual within the company to ensure that there is accountability.

7. Safeguard Data Collected

Security measures should be implemented to protect the integrity and accuracy of the information, as well as to limit access to the data collected to only the affected employee and those with legitimate reasons to review the data. Additionally, safeguards should be followed to ensure that the data collected are accurate and current.

8. Grant Employees the Right to Challenge Data Collected

Procedures should be established to allow employees to contest the information collected for completeness and accuracy. Employees should be informed about these procedures and should have the right to file a complaint or register concerns. If appropriate, the disputed information should be amended for accuracy. Such procedures should be designed to correct mistakes in the data, not to block lawful and accurate collection of data. A compliance person should be designated to handle all such employee challenges to data.

9. Establish Clear Data Retention Policies

Lastly, data should not be retained any longer than is reasonably necessary to achieve the business necessity. If there is a judicial or disciplinary procedure initiated based on any data collected, the data should be retained until the full resolution of the matter.

VI. CONCLUSION

At this point, the proverbial "genie" is out of the bottle. Assuming that researchers are able to create reasonably secure RFID systems, the usefulness of RFID technology has already been demonstrated in a number of varied contexts. The potential for workplace use is no exception. What is critical, however, is that employers should deploy RFID systems in a responsible way with legitimate business goals. To that end, if employers implement systems consistent with the proposed recommendations herein, a satisfactory balance can be achieved between the employer's use of RFID and the employee's expectations of privacy.