University of Georgia

From the SelectedWorks of marisa pagnattaro

September 30, 2007

Getting Under Your Skin--Literally: RFID in the Employment Context

Marisa Anne Pagnattaro

Available at: https://works.bepress.com/marisa_pagnattaro/1/
GETTING UNDER YOUR SKIN -- LITERALLY: RFID IN THE EMPLOYMENT CONTEXT

ABSTRACT: This article explores the legal ramifications of the use of radio frequency identification chips (“RFID”) by employers. RFID is an automated data-capture technology that can be used to identify, track and store information contained on a tiny computer chip, which uses electromagnetic energy in the form of radio waves to communicate information. These chips can be implanted under an employee’s skin, worn in an employee’s clothing or in an identification badge. Part I presents a brief history of RFID, as well as novel and interesting uses in the workplace. This section also discusses security and safety concerns regarding the use of this technology. Part II analyzes current and proposed law in the United States regulating RFID, and privacy implications. Part III details legal regulations in the international context, including in Canada, the European Union and Australia. Lastly, in Part IV, recommendations about the use and legal regulation of RFID in the workplace are proposed.

TABLE OF CONTENTS

INTRODUCTION

I. A BRIEF HISTORY OF RFID AND ENSUING CONCERNS
   A. Novel and Interesting Uses
   B. Security and Safety Concerns

II. UNITED STATES LAW

III. INTERNATIONAL PERSPECTIVES
    A. Canada
    B. European Union
    C. Australia

IV. PROPOSED RECOMMENDATIONS

CONCLUSION

* Acknowledgments: 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.
**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. The technology provides identification and tracking capabilities by using wireless communication to transmit data. RFID systems are already being used or there are plans for its use by a number of federal agencies and in a range of business and public sectors (e.g. health care, retail, transport, and pharmaceutical) for a variety of purposes, such as logistics support, tracking


\(^2\) *Id*.

shipments, electronic screening, preventing counterfeit drugs, security, and identification. Because RFID allows companies to substantially improve productivity, efficiency, and accuracy, many are considering a variety of ways to use this technology.

RFID chips can also be used to track employees. They can be implanted under an employee’s skin, worn in an employee’s clothing or in an identification badge. The most widespread workplace use of RFID technology is chip-embedded staff ID badges, which are primarily used for controlled access to an employer’s premises. Even this use, however, can be controversial if the data collected is used to discipline employees, as opposed to merely controlling door locks. 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 her skin, the employer can collect data regarding the employee’s location and movement by using strategically placed readers. This data then can be entered into a data base to learn more about the employee’s whereabouts.

This article explores the legal ramifications of the use of RFID by employers to track employees. Part I, 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. Part II analyzes current and proposed law in the United States regulating RFID. Part III, details legal regulations in the international context, including in Canada, the European Union and Australia. Lastly, in Part IV, recommendations about the use and legal regulation of RFID in the workplace are proposed.

I. A BRIEF HISTORY OF RFID AND ENSUING CONCERNS

RFID technology is based on a fairly simple system. There are two major components to a RFID “tag”: 1) a tiny silicon computer chip or “integrated circuit” containing a unique identification number; and 2) an antenna which is hooked to the chip. The chip can be encrypted with a unique product code that identifies the individual object or product or person to which it is attached and the antenna is responsible for transmitting information from the chip to the reader using radio waves. In addition to these two components, a reader or scanning device, with an antenna is used to communicate with the tag and the technology will have a database or back-end


logistics system, which stores information gathered from RFID tags. RFID tags may be either “passive” or “active.” A passive tag does not contain its own power source, such as a battery, and it cannot initiate communication with a reader. Active tags, which contain a power source and a transmitter, send a continuous signal. This technology has been used since WWII, where it was used in aircraft identification Friend or Foe systems. During the 1970s, RFID technology began to be used in a limited way for inventory control.

Tremendous growth in the use of this 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. At this time, RFID technology enjoys a wide range of uses, such as tracking gourmet dinners at Marks & Spencer in London, tagging more than 50 million pets worldwide, guarding paintings at a museum in Rotterdam, screening Oscar goers, and tracking supplies in Iraq by the

9 Id.
10 GAO Report, supra note __ at 6.
11 GAO Report, supra note __ at 7.
13 Department of Commerce Report, supra note __ at 5.
Department of Commerce Report, supra note __ at 6.
15 ROBERT O’HARROW, JR., NO PLACE TO HIDE 284-284-90 (20050.
U.S. military. Wal-Mart is making extensive use of RFID inventory tracking, yet it may not be resulting in anticipated cost savings to justify the use. In 2003, Wal-Mart began using RFID technology in its Broken Arrow, Oklahoma store to track Max Factor lipstick. When consumers removed the lipstick from the shelves, this triggered a video monitor, allowing researchers 750 miles away to watch consumers. Researchers in Cincinnati at Proctor & Gamble then could analyze the behavior of consumers.

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 (CSI), to develop “smart” containers that can notify authorities of any tampering or theft. RFID chips can be used to create an “e-


“pedigree” of products through a supply chain, to protect the food supply.\textsuperscript{20} 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, Swingline has developed staples with RFID tags to facilitate document tracking.\textsuperscript{21}

RFID technology is also useful to track people in a range of contexts. Conference badges fitted with RFID chips allow conference organizers to determine who is attending which sessions, as well as when participants come and go.\textsuperscript{22} A controversial tracking system for school children with mandatory ID badges with

\textsuperscript{20} See generally Coping with Regulations, RFID JOURNAL (Feb. 2, 2007), \url{http://www.rfidjournal.com/magazine/article/910/1/100/definitions_off} (discussing the use of RFID to prevent terrorist attacks and to protect the food supply); and McKenna Long & Aldridge, RFID Law Blog, \url{http://rfidlawblog.mckennalong.com/archives/cat-new-rfid-uses.html} (providing on-going commentary about new uses for RFID technology).


\textsuperscript{22} Rafael Ruffolo, Alberta Company Brings RFID to Conference Badges, IT BUSINESS.CA (June 20, 2007), \url{http://www.itbusiness.ca/it/client/en/home/News.asp?id=44005&cid=5}. 
RFID chips was proposed then withdrawn following vocal opposition in California.23 The Minnesota Department of Corrections is using a half-million dollar RFID system to track inmates in a minimum/medium security correctional facility24 and Alanco Technologies has tracking systems is prisons in California, Michigan and Ohio.25 In a novel move, the Baja Beach Club in Barcelona implants a RFID microchip into the patron’s arm for access into the VIP area of the club.26 The chip is injected by a nurse using a syringe and a local anesthetic. A more ominous use was proposed by lawmakers in Indonesia’s Papua who are considering selective use of RFID chip


implants in HIV carriers to monitor their behavior and keep them from infecting others; there are approximately 3,000 people in Papua with HIV/AIDS (population of approximately 2.5 million). In early 2007, Kodak filed an application for a patent on a RFID tag that can be ingested, and then will ultimately dissolve in the body.

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.”

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” offers a RFID time and attendance system that includes an RFID time clock and 25 employee

27 Microchips Mulled for HIV Carriers in Indonesia’s Papua, BREITBART.COM (Jul. 24, 2007),
http://www.breitbart.com/article.php?id=070724075657.4w2f978g&show_article=1.

28 Marc L. Songini, Open Wide: Kodak Looks to Patent Edible RFID, COMPUTER WORLD (Feb. 27, 2007),

29 Id.
badges.\textsuperscript{30} Control Module, a leading biometric workforce management and data collection technology provider has a RFID system that can be used to track employees time and attendance, as well as access control to keep unauthorized individuals from certain facilities and equipment.\textsuperscript{31} Similarly, ActiveWave, Inc., offers RFID employee and passenger tracking systems for airports, railway stations and passenger bus terminals which require individuals to ear a clip on badge, wrist band or badge with a necklace.\textsuperscript{32} A comprehensive time and attendance system for employees is available from absolute-it, located in Dubai, U.A.E., offering the following key features:

- Track and maintain employee attendance records
- Identify attendance exceptions such as tardiness and absenteeism
- Reduce or eliminate unwanted/unauthorized overtime by managing labor resources in real time
- Eliminate ‘Buddy-clocking’
- Instant capture of employee arrival/departure times and location
- In-depth employee database
- Caters for unlimited employees
- Extensive data filtering and drill-down capabilities quickly get to the heart of the information at the employee or enterprise level
- Ability to track, view and report employee information in true, interactive real-time
- Calculates daily and weekly overtime
- Generates detailed and summary reports/timesheets for each employee
- Reports emailed directly from the system to manager’s inbox

\textsuperscript{30} WaspTime, RFID Time and Attendance System (2007),

\textsuperscript{31} Control Module, Inc., \textit{Control Module Introduces first RFID Offering in Workforce Management Category} (Jan. 8, 2007),

\textsuperscript{32} ActiveWave, Inc., \textit{Airports and High Security} (2005),
• Graphical dashboards ensure easy and efficient use of the system
• Violation tracking measures employee behavior and enforces corporate HR and Health and Safety policies consistently
• Capability to automate the most complex rules for accumulating vacation, sick time, and other types of benefit leave
• Shift differential tracking with simple or complex pay rules
• Provides real-time insight into ongoing labor costs and labor productivity with enhanced reporting capabilities
• Reduces or eliminates unauthorized tardiness and absences along with their subsequent costs and losses in productivity
• Robust, flexible setup, allowing management to implement and enforce complex work and pay rules, reducing unwanted overtime and increasing accuracy throughout the organization
• True client-server provides connectivity across wide area networks linking multiple locations to one centralized database
• Central “browser” application for ease of maintenance and system upgrades.\(^3^3\)

Although the use of RFID technology in the workplace is not yet widespread, there several current applications in use illustrating a range of potential uses. On a very large scale, at the Dubai International Airport extension project, RFID technology is being used to track over 9,000 workers from laborers to the highest management, who are all wearing green RFID tags.\(^3^4\) In Sydney, Australia, Star City Casino, which manages a wardrobe inventory of 80,000 uniforms valued at approximately $1.8 million, had a “laundry-tracking problem.”\(^3^5\) The solution from Accenture: embed RFID tags in the waistband, shirttail or collar of each uniform. From the point when the uniforms are issued to the point when they are turned back


\(^3^4\) *Keeping Tabs*, FM MAGAZINE (Feb. 9, 2006), http://www.absolute-it.com/RFID.pdf.

to the laundry, each uniform has a discrete identity that is tracked by strategically placed readers. In the United States, at the security firm CityWatcher.com, the CEO/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. The RFID microchips are about the size of a grain of rice. Known as “smart tags,” the devices called VeriChips are apparently the first and only patented, FDA approved implantable microchip with skin-sensing capabilities. Similarly, workers at the organized-crime division of the Mexican Justice Ministry office in Mexico City use VeriChips for access to high-security areas. 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.

36 Id.
One of the newest developments in RFID workplace use is technology which provides real time location systems (RTLS).\textsuperscript{41} RTLS are being hailed as essential safety devices that could be used by emergency personnel to locate individuals in the event of a disaster.\textsuperscript{42} In 2005, Cisco launched a large-scale RFID application using a wireless RFID server that can track people and equipment.\textsuperscript{43} The system, Wireless Appliance 2700, is able to track RFID tags down to a few metres and display them on a central map. Using tags embedded in employees’ uniforms, alarms can be sounded if the tag moves out of a predefined area.\textsuperscript{44} Most recently, in May 2007, Cisco initiated RTLS with the help of AeroScout, a pioneer in this aspect of RFID technology.\textsuperscript{45} 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

\begin{flushright}\footnotesize\textsuperscript{41} Bert Moore, \textit{RFID: Safety First}, RFID CONNECTIONS (Aug. 16, 2007), http://www.aimglobal.org/members/news/anmviewer.asp?a=2787&p\textasciitilde print=yes.\end{flushright}

\begin{flushright}\footnotesize\textsuperscript{42} Id.\end{flushright}

\begin{flushright}\footnotesize\textsuperscript{43} Ian Thomson, \textit{CISCO Slammed for RFID Staff Tracker}, VNUNET.COM (May 4, 2005), http://www.vnunet.com/vnunet/news/2127277/cisco-slammed-rfid-staff-tracker.\end{flushright}

\begin{flushright}\footnotesize\textsuperscript{44} Id.\end{flushright}

\begin{flushright}\footnotesize\textsuperscript{45} Simon Holloway, \textit{Real Time Location Systems are the New Buzz in RFID}, THE REGISTER (Aug. 21, 2007), http://www.theregister.co.uk/2007/08/21/aeroscout_location_systems/print.html.\end{flushright}
triangulation to calculate the location of the asset.\textsuperscript{46} In the application for Cisco, AeroScout Tags communicate with the Cisco Unified Wireless Network, which is also integrated with AeroScout's MobileView, providing very effective tracking of key assets and people.\textsuperscript{47}

\textit{B. Security and Safety Issues}

Whenever new technology is introduced, particularly when it can yield information about a person’s whereabouts, concerns are raised.\textsuperscript{48} 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.\textsuperscript{49} In a speech at Georgetown Law Center, Senator Patrick Leahy encapsulated the main concerns about RFID:

\begin{quote}
With RFID technology as with many other surveillance technologies, we need to consider how it will be used, and will it be effective. 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
\end{quote}

\textsuperscript{46} Id.

\textsuperscript{47} Id.


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.50

The questions raised, are being echoed and underscored by many consumer and privacy advocates, such as the American Civil Liberties Union,51 Privacy Rights Clearinghouse52 and the Electronic Frontier Foundation.53 The major concerns about using RFID to track employees fall into the following categories: surveillance can be accomplished by any person with access to the reader or database; “profiling” or maintaining a profile on a “target” based on the information gathered; and concerns about action that may be taken based on information collected by using a RFID device.54


Even if employers can use RFID to track employees in the workplace without violating any laws,\textsuperscript{55} 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 U.K.’s new biometric passports and was able to siphon off information, leaving no evidence of tampering.\textsuperscript{56} The chips in the passports currently contain the printed details on the passport, the person’s photograph; eventually the British government wants to incorporate fingerprints and other biometric data on the chips. The fact that someone was able to hack into these ostensibly “secure” chips is the source of great concern, especially in light of additional personal identifying data that may be stored on the chips. Other concerns are that RFID tags will be vulnerable to viruses, just as computers have been under siege.\textsuperscript{57} Moreover, at least one expert

\textsuperscript{55} See, infra, Part II.


claims that he can clone RFID-enabled badges,\(^{58}\) causing distortions in the accuracy of the data collected.

Other security concerns pertain to the lack of reliability of systems. In February 2007, the U.S. Department of Homeland Security decided to stop using RFID technology in its U.S. Visitor and Immigration Status Indicator Technology program after the read rates proved to be inadequate.\(^{59}\) Moreover, there are concerns that a shortage of RFID professionals can be a hindrance to adoption and effective use of RFID technology.\(^{60}\)

In addition to these concerns, recently a report was published suggesting that VeriChip and federal regulators either ignored or overlooked animal studies indicating that RFID chips implanted in dogs and laboratory rodents could cause cancer.\(^{61}\) This would be a very significant and adverse development for VeriChip as they seek to broaden the use of RFID for human tracking. Verichip reportedly will undertake independent studies to determine if there is a correlation between the

---


\(^{61}\) Feder, *supra* note __.
implants and cancer. To date, about 2,000 RFID chips have been implanted in humans, and the company reportedly sees a target market of 45 million Americans for its medical monitoring chips.

II. 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. 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. At this point, most (non-government) 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.

62 Id.


64 There are many articles generally discussing workplace privacy. See, e.g. Pauline T. Kim, Collective and Individual Approaches to Protecting Employee Privacy: The Experience with Workplace Drug Testing, 66 LA. L. REV. 1009 (2006); Michael L. Rustad, Monitoring Employee E-Mail and Internet Useage: Avoiding the Omniscient Electronic Sweatshop: Insights From Europe, 7 U. PA. J. LAB. & EMP. L. 829 (2005);
Inasmuch as there is no legal protection against these forms of monitoring, it is difficult to argue that an employer would violate an employee’s reasonable expectation of privacy, by tracking movement within the workplace using RFID chips.65

To the extent that RFID is used by any government employers, there are Fourth Amendment search and seizure considerations under the U.S. Constitution.66


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 employees.67

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.68 This legislation eliminates or minimizes tort liability for companies that sell or provide anti-terror technology approved by the Department of Homeland Security.69 To the extent that RFID products can be used to track products and minimize the possibility of a terror attack, they qualify as a coverable product under the SAFETY Act.70 To the extent that RFID is used in for medical purposes, the strict

67 See O’Connor v. Ortega, 480 U.S. 709 (1987) (considering what is a reasonable search by a public employer under the Fourth Amendment).

68 Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 [hereinafter “SAFETY Act”].


70 Id.
requirements of the Health Insurance Portability and Accountability Act (“HIPAA”) are triggered.\textsuperscript{71} Privacy and security rules under HIPAA have strict restrictions on the disclosure and use of health information.\textsuperscript{72} The Federal Trade Commission has discretionary authority to prohibit deceptive or unfair acts or practices in or affecting commerce.\textsuperscript{73} 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.\textsuperscript{74}

Given the lack of federal law regulating RFID technology, there has been a good bit of discussion and proposal at the state legislative level. To date, a number of states have introduced legislation relating to the use of RFID, including Alabama (S.B. 310), Illinois (H.B. 4088 and S.B. 2558), Maryland (H.B. 354), Massachusetts (H.B. 1447 and S.B. 181), Missouri (S.B. 128 & 638), Nevada (A.B. 264), New Hampshire (H.B. 203), New Mexico (H.B. 215), New York (State/Bill #A09504), Rhode Island (H.B. 5929), South Dakota (H.B. 1114 and H.B. 1136), Tennessee

\textsuperscript{71} Health Insurance Portability and Accountability Act – NEED CITE

\textsuperscript{72} See generally Lisa J. Sotto, An RFID Code of Conduct, RFID JOURNAL (May 30, 2005), \url{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).

\textsuperscript{73} Federal Trade Commission Act Section 5.

\textsuperscript{74} FTC Report, \textit{supra} note ___ at 21-23.
(H.B. 300 AND S.B. 699), Texas (H.B. 2953 and H.B. 2), and Virginia (H.B. 1304). 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.

A limited number of states have enacted legislation limiting the use of RFID in various contexts. The earliest of those laws were in Wyoming and Utah. In Wyoming, amendments to the Wyoming Pharmacy Act were signed on March 3, 2005, authorizing telepharmacies to use automated inventory control, including RFID. Just over a week later, on March 11, 2005, the Utah Computer Crimes Act Amendments (H.B. 185) were signed by the governor. 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. In a departure from these laws protecting the

---


78 Id.
use of RFID, Wisconsin was the first state to ban forced human RFID chipping.\textsuperscript{79}

Effective May 30, 2006,

(1) No person may require an individual to undergo the implanting of a microchip; and
(2) Any person who violates subsection (1) may be required to forfeit not more than $10,000. Each day of continued violation constitutes a separate offense.\textsuperscript{80}

The passage of this law immediately gave rise to questions. For example, under what circumstances is chipping “forced”? 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 Washington, House Bill 1031, the Electronic Bill of Rights, which would have required parties to obtain consent from consumers “before using RFID to collect, maintain and disclose information” on them was seriously considered in the early spring.\textsuperscript{81} Soon thereafter, in April 2007, North Dakota passed ban on requiring implants.\textsuperscript{82} The law states that “A person may not

\textsuperscript{79} 2005 Wisconsin Act 482 (creating 146.25),


\textsuperscript{80} Id.

\textsuperscript{81} Mary Catherine O’Connor, Washington’s RFID Bill Halted, RFID JOURNAL (Mar. 23, 2007), http://www.rfidjournal.com/article/articleview/3168/. 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.

\textsuperscript{82} Marc L. Songini, North Dakota Band Forced RFID Chipping, COMPUTERWORLD (Apr. 12, 2007),
require that an individual have inserted into that individual’s body a microchip containing a radio frequency identification device.” 83 Violations of this statute are a misdemeanor crime. 84 Again, the literal language of this statute raises questions about what constitutes forced chipping, as well as whether, a swallowed RFID device is within the scope of the law. Most recently, the Identity Information Protection Act overwhelmingly passed California Senate on May 07, 2007. SB 30 (formerly SB 768) requires privacy and security measures for RFID tags. 85 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) prohibit schools from issuing ID cards to track student attendance; and 4) make it a misdemeanor to skim identification cards. 86 Senate Bill 362 passed August 2007. 87 As public concern grows

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=15&amp;articleId=9016385&amp;intsrc=hm_topic.


84 Id.


86 Note that “skimming” is a method used by identity thieves to secretly read cards and obtain that individual’s personal information.

over the use of RFID, more states are likely to pass similar legislation in their upcoming sessions.

**III. INTERNATIONAL PERSPECTIVES**

In 1997, the International Labor Organization (“ILO”) published a nonbinding Code of Practice for the protection of workers’ personal data addressing such concerns as: collection, storage, use, and communication of personal data.\(^88\) 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.”\(^89\) Addressing concerns about the potential for misuse of workers’ personal information, the guidelines address collection, security, storage use and communication of this data.\(^90\) These general principles are reflected in the Resolution on Radio-Frequency Identification which was adopted at the 25\(^{th}\) International Conference of Data Protection and Privacy Commissioners in November 2003.\(^91\) 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;


\(^89\) *Id.* at 12.

\(^90\) *Id.* at 12-14.

b) if the controller can show that personal data are indispensable, they
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.\textsuperscript{92}

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. Here, actions taking place in Canada, the European Union
and Australia are discussed as a representative international sample.

\textbf{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.\textsuperscript{93} 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.\textsuperscript{94} 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:

\textsuperscript{92} \textit{Id.} at 1.

\textsuperscript{93} Personal Information Protection and Electronic Documents Act (“PIPEDA”) (2000
c.5), \url{http://laws.justice.gc.ca/en/P-8.6/258031.html}.

\textsuperscript{94} Privacy Act (R.S., 1985 c. P-21), \url{http://laws.justice.gc.ca/en/P-21/index.html}. 

26
1) Notice and Consent - The right to know whether a product contains a RFID tag and whether a 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 identification information kept separate from information identifying an object.\(^{95}\)

Additionally, the report identifies 8 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.\(^{96}\)

Echoing the importance of these principles, a speech by the Privacy Commissioner of Canada, Jennifer Stoddard, notes that employers need to “start thinking more about workplace privacy and the potential implications of emerging surveillance technologies.”\(^{97}\) Citing the 2006 Research Report “Under the Radar? The Employer Perspective on Workplace Privacy,” Stoddard expressed her disappointment about some of the employer attitudes about workplace privacy.\(^{98}\)


\(^{96}\) Id. at 21.


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.\footnote{Id.} Moreover, Stoddard notes that a survey finding that there is a gap between what “employers and employees think s an acceptable privacy practice.”\footnote{Stoddard, 
supra
 note __ .} Emphasizing her concern about the “effects on the dignity of employees” of privacy invasive measures in the workplace, Stoddard called for a balance between the “rights of the individual to privacy and the needs of organizations to collect, use or disclose personal information.”\footnote{Id.} In 2006, a comprehensive set of guidelines for using RFID systems was released in Canada.\footnote{Ann Cavoukian, Canada’s Commissioner for Information and Privacy, \textit{Privacy Guidelines for RFID Information Systems} (June 2006) [hereinafter “Canadian RFID Privacy Guidelines”], http://canada.ihs.com/NR/rdonlyres/9C4250F8-0C18-4E2D-A605-1F7F8643BE70/0/rfidgdlines.pdf.} The guidelines are based on three major principles: 1) focusing on RFID systems, not technologies (i.e. if the deployment of the systems raise 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, enabling individuals to make informed decisions about the use of RFID systems affecting them.\(^\text{103}\)

**B. European Union**

Similar to discussions in the United States and Canada, in the European Union (“EU”) is actively considering what restrictions, if any, should be placed on the use of RFID technology. Although one might think that EU Directive 95/46/EC,\(^\text{104}\) which restricts the processing and movement of certain forms of data on individuals, 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 on data protection issued a working document studying privacy concerns related to the use of RFID technology in the EU.\(^\text{105}\) The Working Party expressed “concern about the possibility for some applications of RFID technology to violate human dignity, as well as data protection rights.”\(^\text{106}\) 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

\(^{103}\) *Id.* at 2.


\(^{106}\) *Id.* at 2.
multiple venues.\textsuperscript{107} Heading off public concern, the EU Commission 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.”\textsuperscript{108} 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.?\textsuperscript{109}"

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 by Viviane Reding, the member of the European Commission responsible for Information Society and Media, she advocated for a set of European rules for safe and secure development of RFID technology.\textsuperscript{110} Thereafter, in March 2007, the EU Commission issued a report proposing a

\begin{flushright}
\textsuperscript{107} \textit{Id.}
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{109} \textit{Id.}
\end{flushright}

\begin{flushright}
\end{flushright}
“European Policy Strategy” for using smart radio tags. According to the report, the Commission will create in 2007 an RFID Stakeholder Group to provide advice and assistance to the Commission in developing a European policy position concerning RFID applications. The work of this group is to be carried out in association with, among others, the Article 29 Data Protection Working Party. Also, by mid 2007, they were to propose amendments to the e-Privacy Directive to take account of RFID applications, as part of the EU Telecom Rules' review, to publish, by the end of 2007, a Recommendation on how to handle data security and privacy of smart radio tags to Member States and stakeholders, and to assess policy options and need for further legislative steps, by the end of 2008.

The RFID report was viewed as a welcome development by the industry because, at least for the time bring the EU will use self-regulation and existing laws to manage RFID technology. 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 was still seem as a very positive signal for those seeking to use RFID.\textsuperscript{114} In fact, the U.S. Dept of Commerce undersecretary 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.”\textsuperscript{115}

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, Commission nationale de l’informatique et des libertés “CNIL” is monitoring RFID use, as it considers RFID to be “personal identifiers” within the meaning of the 6 January 1978 Act and the EU 95/45 Directive.\textsuperscript{116} 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.\textsuperscript{117} In the United Kingdom, the Information Commissioner’s Office is making recommendations in its Employment Practice Code similar to those referenced in France.\textsuperscript{118} Moreover, the British union GMB recently argued that

---


\textsuperscript{117} Id.

\textsuperscript{118} Information Commissioner’s Office, Data Protection Technical Guidance RFID (Sept. 8, 2006),
requiring some workers in retail distribution centers to wear RFID tags was
dehumanizing, turning workplaces into “battery farms.”\textsuperscript{119}

\textbf{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.”\textsuperscript{120} In Australia, 60 percent of the RFID
technology market is in security/access control and animal applications.\textsuperscript{121}

Encompassed within the security/access category are applications for employee
access tracking.\textsuperscript{122} The most celebrated use in the employment context is by the Star
City Casino in Sydney where RFID tags are sewn in employee uniforms.\textsuperscript{123}

\begin{quote}
\end{quote}

\textsuperscript{119} Christine Buckley, \textit{This is the Wrist Tag that Makes your Time at Work More
Productive – or Turns You Into a Robot} (June 7, 2005),

http://www.timesonline.co.uk/tol/news/uk/article530747.ece.

\textsuperscript{120} RFID Association of Australia, http://www.rfidaa.org/.

\textsuperscript{121} Paul Oswal, Australia RFID Applications, \textit{HIGH TECH AIDCOURIER} (Oct. 2005),


\textsuperscript{122} \textit{Id.}

\textsuperscript{123} Ben Woodhead, \textit{Fast Track for Radio Tags}, \textit{AUSTRALIAN IT} (Oct. 3, 2006),

recently, the Star City Casino is looking into using RFID gambling chips, allowing
the casino to track individual gamblers and to reduce fraud. \textit{Id.}

33
In 2006, the RFIDAA worked with Booze Allen Hamilton, a leading consulting firm, to survey the views and position of the government regarding the adoption of RFID technology. The Booze Allen Hamilton study showed that less than 30% of Australian government departments gave RFID technology any priority in their business plan. However, the study also revealed that 75% of the respondents plan to investigate or use RFID within three years. In any event, the Australian Office of the Privacy Commissioner issued a report on developing technologies. 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 “they also have equal potential to invade personal privacy if deployed wrongly.”

Based on these concerns, the Office of the Australian Privacy Commissioner stated that “all the basic principles of privacy law should be adopted when designing,

\[\text{124} \quad \text{RFIDAA, } \text{RFIDAA Supports Survey on Government Position with RFID (2006),}\]
\[\text{http://www.rfidaa.org/templates/listDetail.jsp?id=99}\]
\[\text{125} \quad \text{Booze, Allen, Hamilton, } \text{RFID Yet To Reach Government Tipping Point (Oct. 2, 2006),}\]
\[\text{http://www.boozallen.com/publications/article/14521943?lpid=6606}\]
\[\text{14.}\]
\[\text{126} \quad \text{Id.}\]
\[\text{127} \quad \text{Australian Government, Office of the Privacy Commissioner, } \text{Chapter 11, Developing Technologies,}\]
\[\text{128} \quad \text{Id.}\]
implementing and using RFID technology.” 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. Thus, Australians share the same concerns about privacy and information that have been raised in the United States, Canada, and the EU.

IV. PROPOSED RECOMMENDATIONS

Inasmuch as there is very little legislation regulating the use of RFID to track employees and 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. 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 ten recommendations are designed to help employers implement

129 Id.
130 Id.
comprehensive and thoughtful procedures in the deployment of RFID systems to track employees.

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 that purpose 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 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. Consistent with at least two states which have passed laws aimed at preventing (and criminalizing) forced implanting, employees should not be coerced into forced implanting. 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; 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 on-line 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.

6. Mandate Accountability

On 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 date collected to only those with legitimate reasons to review the data and the affected employee. Additionally, safeguards should be followed to ensure that the data collected is accurate and current.
9. Grant Employees the Right to Challenge Data Collected

Procedures should be established to allow employees to contest the information collected, its 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.

10. 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.

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 and the employee’s expectations of privacy.