RADIO FREQUENCY IDENTIFICATION AND PRIVACY: SHOPPING INTO SURVEILLANCE

Written by George Hariton, John Lawford
and Hasini Palihapitiya
Public Interest Advocacy Centre
1204 – ONE Nicholas St.
Ottawa, Ontario
K1N 7B7

February 2006

With Funding from Industry Canada

The Public Interest Advocacy Centre
(PIAC)
Suite 1204
ONE Nicholas Street
Ottawa, ON
K1N 7B7

Canadian Cataloguing and Publication Data

Hariton, George
Lawford, John
Palihapitiya, Hasini

Radio Frequency Identification and Privacy:
Shopping Into Surveillance

ISBN 1-895-060-73-7

EXECUTIVE SUMMARY

Radio Frequency Identification (RFID) is a technology that allows people and objects to be identified and tracked via a radio frequency signal. This report looks at privacy issues surrounding the likely use of RFID by major retailers, and suggests limits to these systems consistent with present privacy laws, as well as comments on whether the present privacy law regimes adequately protect consumers from retail surveillance. As this is a new technology, the report will seek to define the new technology, and to report on its applications and likely applications thus far as well as to report on consumer attitudes to the technology.

RFID is well-established in the supply chain of major retailers already. To a certain extent, RFID use in manufacturing and supply chain management has been encouraged by government safety concerns with products such as pharmaceuticals and automobile tires. However, government, when encouraging such 'pre-retail' uses, does not generally require privacy impact assessments, which might limit the extension of RFIDs from manufacturing into the retail environment.

Consumers soon will face RFIDs at the retail level. It is this 'item-level' use of RFID that raises consumer privacy and related concerns. Item level RFIDs produce individual data which, when linked to an individual shopper through a loyalty card or otherwise, constitutes a form of low-level, distributed consumer surveillance. This potential surveillance raises the specter of consumer profiles that track consumer behaviour in relation to objects. Such profiles may become available to not only the original retailer, but also affiliated companies, or even to the federal government under national security exceptions to Canada's private sector privacy law. RFID tags, if left live 'post-sales' (whether consciously for warranty and related purposes or unconsciously – that is, not 'killed' at the point of sale) risk being read by third parties, if encryption or similar security measures are not applied by the original retailer.

RFID technology presents a novel challenge to Canadian privacy law. The "primitive" surveillance capabilities of RFID at present are unlikely to violate a reasonable expectation of privacy as interpreted by the Supreme Court of Canada. However, Canada's private sector *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) does appear to severely limit RFID use for consumer surveillance purposes. RFID technology has caught the eye of Canada's Office of the Privacy Commissioner (OPCC), which has asked retailers for details of their planned RFID uses.

PIPEDA appears to require retailers who wish to track individual shoppers to obtain the informed consent of customers for the use or disclosure of the shopping patterns the RFID chips reveal about their customers. Such 'informed consent' will be difficult to achieve without extensive disclosure to the customer

of the full implications of RFID surveillance and a positive indication of consent to the use and disclosure of RFID surveillance.

Retailers with more modest goals of controlling in-store inventory, rather than tracking customers will face less rigour in informing customers of RFID use. But, they will still be required as a matter of course to 'kill' RFID tags at the point-of-sale or undertake encryption or similar technological measures to safeguard the personal information of their shoppers from third party interception post-sales. Such retailers would appear to be prohibited from associating personal information from loyalty card or other customer information databases with RFID data obtained from interaction of individual customers with RFID chipped products.

Consumer polling appears to indicate great consumer discomfort in the surveillance aspect of RFID technology. While consumers may welcome certain safety and convenience benefits from RFID, their concern with privacy-invasive aspects of RFID outweighs it to the point where RFID use as surveillance appears unreasonable. In addition, some of the benefits of RFID promised by retailers may in fact interfere with established consumer rights and expectations – for example regarding hassle-free return policies.

As RFID implementation is moving forward quickly, it is recommended that immediate action be undertaken by the OPCC to provide RFID-specific guidelines which explain the constraints on the use of the technology for consumer surveillance and profiling, at least in the absence of very clear, and informed consumer consent. Ideally, the OPCC should ask that RFID- or surveillance-specific provisions be added to *PIPEDA* during the Parliamentary review of the legislation slated for 2006.

TABLE OF CONTENTS

"My anxiety is that we don't sleepwalk into a surveillance society where much more information is collected about people, accessible to far more people shared across many more boundaries than British society would feel comfortable with". - Richard Thomas, U.K. Information Commissioner [1]

"It isn't just the coin on the counter that the shopper leaves, but the steps they took to get there." - Herb Sorensen, President of Sorensen Associates, maker of PathTracker RFID grocery cart tracker [2]

INTRODUCTION

Radio Frequency Identification (RFID) is a technology that allows people and objects to be identified and tracked via a radio frequency signal. Originally intended as a more functional replacement for bar codes in retail stores and the supply chain, the range of applications associated with RFID has increased enormously. This has led to a rapid proliferation of the number of systems being deployed – a trend that is expected only to accelerate in the near future,[3] – and one that has given rise to a number of privacy concerns. This report looks at privacy issues surrounding the proposed use of RFID by major retailers, and explores the potential risks associated with the widespread use of RFID technology in terms of mass surveillance. Specifically, this paper draws a parallel between mass surveillance issues produced by use of video surveillance and the privacy concerns that arise through use of RFID tags in the retail context. This report also suggests limits to these systems consistent with present privacy laws, and comments on the present privacy law regime's protection of consumers from retail surveillance. The report seeks to define this emerging technology, and discusses its current and likely future applications.

---

[1] Richard Thomas, U.K. Information Commissioner, quoted in "Beware rise of Big Brother state, warns data watchdog." The Times (London), August 16, 2004, online: http://www.timesonline.co.uk/newspaper/0%2C%2C2710-1218615%2C00.html

[2] As quoted in E. Murphy, "Tracking Grocery Hot Spots" Portland Press Herald, January 27, 2004.

[3] Business consultants Frost and Sullivan, for example, forecast a global market for RFID in 2005 of some $10 billion, while IDTechEx predicts that "all the leading analysts see double-digit growth of RFID markets by value over the next few years, 25 percent yearly being a typical figure". IDTechEx, "RFID Market Forecasts", January 1, 2004, online: http://www.idtechex.com/products/en/articles/00000031.asp

RFID Technology

RFID is an automatic identification method that relies on tags that are attached or incorporated into products, animals or people, and RFID transceivers.[4] There are a wide range of RFID systems commercially available. At the lower end, primitive RFID systems have little more functionality than bar code systems, while at the top end, they can be equivalent to "smart cards".[5]

An RFID system consists, at a minimum, of transponders (commonly called tags), and readers (technically referred to as "interrogators").[6] The reader contains an antenna and a transceiver or decoder, as well as memory and some processing capability. In most applications, it sends out a signal several times a second, querying tags.

RFID tags can be passive or active. A passive tag does not have its own source of power, but rather uses energy from the signal sent by the reader to send a reply. As a result, the range is limited. In theory, the range is up to ten feet, but in practice, the range is often less, sometimes only a few inches.

A passive tag has minimal memory and little or no processing capability. The tag must have a unique identifier or number that corresponds to that tag, and, by association, to the object or person to which the tag is attached. Low-end tags may have no other information. Rather, the reader uses the identifier to look up the object in a database, where a more or less extensive description can be found. The reader may update the database after detecting an item, adding the new observation and the circumstances surrounding it (e.g. time and place).

Some passive tags allow the writing of new information into their memory by the reader, so that the tag is updated. As an example, an event log may be maintained. More importantly, the identifier may be deactivated, temporarily or permanently, by making appropriate changes in the header.

Active tags have thin-film batteries or "Power Paper" to power them, allowing for very thin tags. They are generally more expensive than passive tags, but have

---

[4] For a comprehensive discussion of RFID technology, also refer to Ann Cavoukian's "Tag, You're It: Privacy Implications of Radio Fredquency Identification (RFID) Technology", Information and Privacy Commissioner/Ontario, February 2004, [***Cavoukian, Tag You're It***] at pp. 5-7, online: http://www.ipc.on.ca/docs/rfid.pdf.

[5] Smart Cards provide data portability capabilities, and come in two varieties: memory and microprocessor. While memory cards simply store data, microprocessor cards can add, delete and manipulate information stored in the card's memory like a miniature computer, and offer built-in security features. Additional information online: http://www.gemplus.com/smart/cards/basics/what.html.

[6] The discussion in this section is based on Heiko Knospe and Hartmut Pohl, "RFID Security", *Information Security Technical Report*, Vol. 9, No. 4, Elsevier Ltd. (2004), at pp.30-41.

better radio characteristics, in particular a bigger range. They have processing capabilities, and may include other functional components, e.g., sensors. Functionality is much improved if readers are networked, with access to a central database. In such a case, a simple identifier on a tag can be used to elicit a wealth of information on the item tagged. Information obtained by readers can be used to update the central database in real time as well.[7]

Because RFID systems are diverse, there are as of yet no international standards for them. However, work on international standards has been ongoing since the 1990s,[8] and several protocols are becoming *de facto* industry standards in the meantime. [9]

[7] For a more detailed explanation of the types of RFID systems please see Cavoukian, Tag You're It, *supra* note 4.

[8] See for example the work of the International Organization for Standardization and the International Electro Technical Commission (IEC) Joint Technical Committee 31 "Automatic Identification and Data Capture Techniques" and in particular, the sub-committee JTC 1/SC 31/WG 4 "Radio Frequency Identification for Item Management" online: http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=156.

[9] See, for example, EPSglobal Inc. Standards online: http://www.epcglobalinc.org/.

RFID IN THE RETAIL CONTEXT

RFID technology is being used in increasingly innovative and aggressive ways, from implantation in livestock and household animals,[10] use in passports,[11] use in employee identification cards,[12] for micro-payments,[13] and even implantation in medical patients.[14] The European Union has even proposed putting RFID tags into currency.[15] This report will consider RFID tagging of products in the retail context, the situation most consumers will be faced with.[16] RFID tagging promises to deliver increased business efficiencies in every sphere of the retail chain from manufacturing, to pre- and post-sales applications, as well as payment and commercial transactions. However, each application also gives rise to potential privacy concerns for the consumer.

---

[10] Approximately 40 million RFID chips have been implanted in livestock worldwide. For example, the Canadian Cattle identification Agency (CCIA) plans to use RFID tags to monitor "birth to burger" movements of beef cattle. Such monitoring has taken on special urgency considering the spread of "mad cow" disease. As of September 1, 2006, all cattle leaving their farm of origin must be tagged with a CCIA approved RFID tag. (CCIA Online: http://www.canadaid.com/155471%20CCIARFIDFINALbrochure.pdf).

Pet owners and animal shelters are also implanting RFID tags subcutaneously to aid in identification in case of loss (online: http://www.24petwatch.com/LatestNews.asp).

[11] The U.S. State Department has recently announced that all U.S. passports will be implanted with remotely readable computer chips starting in October 2006. Information including: name, nationality, sex, date and place of birth, and digitized photograph of the passport holder will be embedded in the RFID chips. Other nations, including the U.K. and Germany have announced similar plans. Declan McCullagh, "Passports to get RFID Chip Implants", *News.Com*, (October 25, 2005), online: http://netscape.com.com/2102-7348_3-5913644.html?tag=st.util.print.

Use of RFID chips in passports has raised considerable debate from privacy advocates. See for example, Bruce Schneier, "Fatal Flaw Weakens RFID Passports", *Wired News*, (November 3, 2005), online: http://www.wired.com/news/privacy/0,1848,69453,00.html.

[12] RFID tags could be placed in employee badges or uniforms, and used, for example for security purposes, as well as tracking employee movement and productivity. Alternate uses have been developed by the U.S. military and police forces, which are contemplating use of subcutaneous chips. Dr. Teresa Scassa et. al. "An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies", Prepared for the Office of the Privacy Commissioner of Canada, April 28, 2005, [***Scassa***] at pp. 13, online: http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf.

[13] Jonathan Collins, "Dexit Turns RFID Cards into Cash: A Canadian Company's new service lets consumers make small purchases using a contactless system". *RFID Journal*, (December 3, 2003), online: http://www.rfidjournal.com/article/articleview/673/1/1/

[14] The U.S. Food and Drug Administration (FDA) has approved use of a 16-digit RFID tag that is similar to those embedded in livestock and pets to be implanted into human subjects. When the tag is scanned, the number would provide quick and easy access to specific medical data about the patient, including information about life-threatening diseases, or the presence of implantable devices like pacemakers, which could prove invaluable during an emergency. Laurie Sullivan, "FDA Approved RFID Tags for Humans", *InformationWeek*, (October 14, 2004), online: http://informationweek.com/story/showArticle.jhtml?articleID=49901698.

[15] Kim Yon-Young, "Radio ID chips may track banknotes", *CNET News*, (May 22, 2003), online: http://news.com.com/Radio+ID+chips+may+track+banknotes/2100-1017_3-1009155.html

[16] Although this report will not consider the identification documents debate nor human implantation, these questions are deserving of more scrutiny even than retail applications.

Manufacturing and Supply Chain

Before hitting the sales floor, products already have lived a long and sometimes tortuous life in the manufacturing and supply chain. RFID is already widely deployed in these "behind the scenes" situations. In a manufacturing environment, RFID systems are routinely used for control of parts and just-in-time logistics. Manufacturers track parts from the time they are produced until the assembled goods are to be sold. Commercial trucking companies and railways too have long used RFID in tracking shipments, attaching RFID tags to pallets and containers, and even high-value parts which may be individually tagged because of their value. However, the utility and ubiquity of RFID in manufacturing and supply-chain management may ultimately have an effect on consumers.

Use of RFID technology in manufacturing has also been either encouraged or actually mandated by government. In the pharmaceutical sector, the U.S. Food and Drug Administration (FDA) has recommended RFID tagging of medications with a view to enhancing their safety.[17] The rationale is that by improving supply chain performance through widespread use of RFID technology, counterfeit drugs could be more easily prevented from reaching the market. This motivation for supply chain purity is, however, driving tagging of pharmaceuticals down to near-retail level. For example, it was recently announced that RFID tags will be added to bottles of the impotency drug Viagra, which will allow the drug to be tracked electronically from the production plant to the pharmacy – creating an "electronic pedigree".[18] Counterfeit drugs would not carry such records. However, such tagging carries potential privacy implications should the tag be delivered intact on a pill container for the patient.[19]

U.S. FDA officials expect widespread use of RFID tags in this manner by 2007, since the agency has endorsed voluntary guidelines and intends to "facilitate"

---

[17] See U.S. FDA, "Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs - Guidance for FDA Staff and Industry - Compliance Policy Guides - Sec. 400.210 - Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs", November 2004, online: http://www.fda.gov/oc/initiatives/counterfeit/rfid_cpg.html. The Guidelines state in part "RFID will be used only for inventory control, tracking and tracing of products, verification of shipment and receipt of such products, or finished product authentication."

[18] The RFID tags would look like ordinary labels, but actually consist of computer chips with antennas wrapped around them. The tags would work like passports, picking up notations at each stage of the distribution chain when the chip is activated. Sensors at distribution centers use radio waves to activate the tags, which are electronically read and stamped with a record of where they have been. See Mary Catherine O'Connor "Pfizer Using RFID to Fight Fake Viagra" RFID Journal January 6, 2006, online: http://www.rfidjournal.com/article/articleview/2075/1/1/.

[19] Although "the bottles that most patients take home from the pharmacy won't contain RFID tags because most pharmacists usually transfer medicines from manufacturers' bottles to generic amber bottles when dispensing the pills", Pfizer has not guaranteed that it will not require pharmacists to dispense the pills in the tagged containers in the future. Alorie Gilbert, "Pfizer fights fake Viagra with RFID", CNET News, January 6, 2006, online: http://news.com.com/Pfizer+fights+fake+Viagra+with+RFID/2100-1012_3-6022485.html.

deployment of RFID by this date.[20] However, the guidelines make no mention of privacy. [21] Health Canada has not yet endorsed a similar requirement for drugs manufactured in Canada. [22]

A similar effect has occurred with a product safety issue in the U.S. The United States passed the *TREAD Act* (*Transportation, Recall, Enhancement, Accountability and Documentation Act*),[23] which was instituted following the Bridgestone/Firestone, Ford Explorer recall of 6.5 million Firestone tires. The facility exists to link RFIDs in tires with vehicle identification numbers, leading to concerns of trackability of automobiles for unrelated secondary purposes, including speeding.[24] However, it appears that the privacy aspects of the embedding of permanent RFID into tires were not addressed in the *TREAD Act*.

Inventory is also controlled in great detail through RFID. This allows re-ordering and restocking within tight time intervals, and ensures that shortages do not develop. Another major goal of RFID use in the supply chain is to reduce "shrinkage" – industry's euphemism for (usually employee) theft of products between manufacture and delivery.

Thus, it seems apparent that for various "safety-related" reasons, government is actively encouraging the inclusion of RFID in the supply chain down to just above the retail level.[25] But, little attention is being paid to the study of the likely privacy

---

[20] See Alorie Gilbert, "FDA Endorses ID Tags for Drugmakers", CNET News, February 18, 2004, online: http://news.com.com/FDA+endorses+ID+tags+for+drugmakers/2100-1008_3-5161220.html.

[21] The report upon which they are based does, however, state: "Lastly, stakeholders will need to ensure that they comply with the patient privacy protections provided by the *Health Insurance Portability and Accountability Act* as they implement use of RFID technology". See U.S. FDA, "Combating Counterfeit Drugs - A Report of the Food and Drug Administration," February 2004, s. 1(e), online: http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html#radiofrequency.

[22] However, there have been allegations that a prime motivation for the use of RFID in pharmaceuticals in the U.S. is to help stem the importation of Canadian drugs to the American market. Chris Newmarker, "Drug Makers Consider Adding RFID Tags to Labels", Associated Press, Posted 9/7/2004 3:04 AM, online: http://www.usatoday.com/tech/news/surveillance/2004-09-07-rfid-for-pharma_x.htm.

[23] The Act mandates that car manufacturers closely track tires from the 2004 model year on, in order to inform customers in the event of a recall. "Michelin Embeds RFID Tags in Tires", RFID Journal, January 17, 2003, online: http://www.rfidjournal.com/article/articleview/269/1/1/. RFID transponders are embedded into the tire during manufacturing and allows the tire's unique identification number to be associated with a vehicle identification number (VIN) describing when and where the tire was made, and so on. (Michelin Press Release, March 9, 2005, online: http://www.michelinman.com/difference/releases/pressrelease03092005a.html).

[24] See Melissa M. Ezarik, "Is Big Brother your Backseat Spy?" Bankrate.com, February 15, 2005, online: http://www.bankrate.com/brm/news/auto/car-guide-2005/big-brother1.asp.

[25] CASPIAN charges that they have found documents indicating the U.S. government agencies are encouraging RFID use. See "CASPIAN Uncovers U.S. Government RFID Promotion Scheme, Heads of Federal Agencies encouraged to 'advance the industry'", Press Release, January 31, 2005, online: http://www.spychips.com/press-releases/gsa-document.html. Notable is the complete lack of the word or concept of "privacy" in the Bulletin CASPIAN refers to

effects at the *retail* level of aggressively promoting such technology upstream in the supply chain – at least not in advance of the actual deployment of RFID at the retail level.[26]

As for consumer products, however, Ann Cavoukian, Privacy Commissioner of Ontario notes in her paper, "Tag, You're It" on RFID, notes the potential inseparability of manufacturing and retail information gathering that RFID can represent:

> RFID systems enable tagged objects to 'speak' to electronic readers potentially over the entire course of a product's lifecycle – from production to disposal – providing retailers or manufacturers with an unblinking, voyeuristic view of consumer attitudes and purchase behaviour.[27]

This report now considers where consumers meet RFID – and what's in store.

---

in their press release. See General Services Administration, "GSA Bulletin Fmr B-7 Radio Frequency Identification (RFID)" December 6, 2004, online: http://www.gsa.gov/gsa/cm_attachments/GSA_BASIC/rfid_sign_R2-sS2O_0Z5RDZ-i34K-pR.doc

[26] Typical of the encouragement to manufacturers to use RFID is the Industry Canada Guidance Document "Radio Frequency Identification (RFID); Beyond Customer Mandate", March 2005, online: http://strategis.ic.gc.ca/epic/internet/indsib-logi.nsf/vwapj/RFID%20Beyond%20Customer%20Mandate%20Final-eng.pdf/$file/RFID%20Beyond%20Customer%20Mandate%20Final-eng.pdf Like the GSA document, this one contains no reference at all to 'privacy'.

Note, however, the initial approach to the subject of the Office of the Privacy Commissioner of Canada to RFID, who states she will study RFID and poll the industry on privacy questions (see below). See too, the paper prepared by the Ontaio Information and Privacy Commissioner, Ann Cavoukian. Cavoukian, Tag You're It *supra* note 4.

[27] Cavoukian, Tag You're It *supra* note 4, at pp. 8.

Retail Applications and Item-Level Tagging

Although RFID technology was originally intended to track the movement of products through the manufacturing cycle, it appears that most RFID suppliers are focusing now on the retail arena for growth. In other words, creating "item level" RFID chips is the new profit-driver.[28] Most item-level chips carry Electronic Product Code (EPC) information, which is a serial created by the Auto-ID Centre intended to complement barcodes. The EPC has digits to identify the manufacturer, product category and the individual item.

The Auto-ID Center, created at MIT in the 1990s, intends to create a standard for tracking of all products electronically, and create, in effect, an 'internet of things'.[29] In other words, this is the 'barcode on steroids' referred to in Ann Cavoukian's paper, "Tag, You're It".[30] Its real value is designed for the sales floor – and beyond.

Contributing to the future ubiquity of RFID tags is the declining price of using the technology.[31] Presently, the least expensive tags have limited functionality, and some can do no more than signal a product identifier. However, this functionality and the read distance may become more robust as the technology advances.

There are four important differences between RFID tags and bar codes: [32]

1. An RFID tag contains an identifier that is unique to that particular object. By contrast, a bar code only identifies the class to which the object belongs, but not the object itself.

2. While bar codes must be scanned with a laser, the RFID tag only needs to pass near a reader, as far as several feet away.

---

[28] See, for example, Tagsys RFID, a French RFID manufacturer, that trumpets "TAGSYS is the global leader in item-level RFID systems and tags", online: http://www.tagsysrfid.com/.

[29] The system such as these electronically-linked devices permit is, to boosters, an 'ambient intelligence' where humans interact electronically with all physical objects in the world. For example, an AmI (ambient intelligent) home:

> Is highly networked, connected to public networks and other homes at very high bandwidths (tens of megabits per second). Inside the home, a wireless network connects a wide variety of appliances and displays - not just PCs - as well as the personal area networks of each person living in the house. Content - both broadcast and personal - is stored in a home server, making it accessible across the network.

The EU presently is studying the issue. See Europe's Information Society – Thematic Portal "Policy : Ambient Intelligence", online: http://europa.eu.int/information_society/policy/ambienti/index_en.htm.

[30] Cavoukian, Tag You're It, *supra* note 4.

[31] RFID tags are currently in the $0.20 to $0.75 range.

[32] See also Cavoukian, Tag You're It, *supra* note 4, at pp. 8.

3. RFID tags can be read more quickly, and multiple tags can be read at the same time.

4. RFID tags can be read unobtrusively, without customers or others being aware of it happening.

There are major pre-sale advantages of RFID tags from the retailers' perspective. First, RFID tags allow for better inventory management. Products are not merely inventoried at checkout, as with bar codes; they can be identified wherever they may be in the supply chain. Additionally, shelves can track their own inventory and signal for replenishment when necessary.[33]

Consumers likely will see item-level tagging at the retail level first in fashion retailing. The CEO of a leading tag manufacturer, Alien Technology, supports this trend: [34]

> Apparel manufacturers are starting to recognize the value of RFID, particularly branded-apparel retailers. […] It's not a matter of having three cases of jeans on the shelf. It's a matter of knowing you have this many size 34 jeans and this many size 32. Many believe it could be one of the first sectors to tag at the item level.

The second major use of RFID tags on the sales floor would be to aid in loss prevention or "shrinkage". RFID tags could help combat shoplifting and employee theft, as items carrying such tags are difficult to conceal because of their signaling capabilities.

The third, and final, use of item-level RFID tags in the pre-sales context is more problematic. Tags can be used to signal when prospective customers pick up merchandise, where they carry it through the store, and ultimately uncover the combination of items they collect. Tags can even be used to trigger video cameras to film consumer behavior.

For example, there were reports of customers being filmed interacting with RFID-tagged Gillette razor blades in a Massachusetts Wal-Mart.[35] According to the

---

[33] This technology, commonly referred to as "smart shelf" technology, can include everything from simple inventory tracking to ultra-advanced systems that can provide instantaneous price and article information, as well as interactive cross-promotions. For example, Checkpoint's Smart Shelf, incorporates video on demand features. (CheckpointEurope, online: http://www.checkpointeurope.com/app/?page=newsitem&locale=eu&id=570). At one point Wal-Mart was interested in testing the technology for use in its retail empire, but unexpectedly abandoned trials planned with partner manufacturer, Gillette. Richard Shim, "Wal-Mart Cancels 'Smart Shelf' Trial", ZDNet, (July 9, 2003), online: http://news.zdnet.com/2100-9584_22-1023934.html.

[34] Mark Roberti, "Tipping Point Is Closer, says Alien CEO" RFID Journal, January 27, 2006, online: http://www.rfidjournal.com/article/articleview/2107/1/1/.

[35] This story, first broken by CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering), alleges that packages of Gillette Mach3 razors were tagged with RFID chips in a

Chicago Sun Times, Lipfinity brand lipstick packages were tagged with RFID chips at a Wal-Mart in Broken Arrow, Oklahoma in July of 2003, allowing executives from Proctor & Gamble to spy on customers from the comfort of their offices.[36]

The potential to monitor the pre-sales behavior of consumers and potentially build consumer profiles and make predictive offers based on transaction history is the most pressing concern surrounding RFID tagging at the pre-sales level. Retailers maintain that use of RFID tags will benefit consumers through reductions in overhead costs, reduced loss and greater efficiency in maintaining inventory, ultimately resulting in lower prices for consumers.[37] However, the potential for retailers to exploit the technology and use it to conduct consumer research certainly exists. As noted in the paper by Dr. Teresa Scassa et al commissioned by the Privacy Commissioner of Canada:

> RFID tags on individual product items could also be used to track consumer movements within a given store. For example, by installing a series of readers through a store, a business could garner information about how customers move through the store, which areas are most heavily browsed, and so on. [38]

Video surveillance monitoring in retail spaces, when combined with readers and RFID tags such as those discussed, could facilitate identification of individual customers. However, mere recording of RFID-signaled location and related information could produce a fairly accurate trajectory for the consumer even without accompanying video surveillance. Such use would enable retailers to link this information with pre-sales behaviour, either from that day or past visits, [39] provided the consumer were identified by the retailer through payment identification, loyalty card or other similar program.[40]

Massachusetts Wal-Mart, as well as a Tesco store in Cambridge, U.K. The Gillette tracking system sensed when a product was removed from the shelf and took photographs of shoppers, which were subsequently compared to photos taken when the razors reached the checkout. This trial with RFID was instituted to curtail shoplifting, but was not surprisingly received with shock and concern by privacy advocates (see for example, www.boycottgillette.com). Chris Richard, "Can Your Razor Blade Spy on You?" Christian Science Monitor, (November 6, 2003), online: www.csmonitor.com/2003/1106/p14s01-stct.htm.

[36] "P&G, Wal-Mart Store Did Secret Test of RFID", *Chicago Sun Times*, (November 9, 2003).

[37] Customers react to these claims with skepticism. Laurie Sullivan, "Majority of European Consumers Worry RFID Threatens Their Privacy, Survey Says", *InformationWeek*, (February 9, 2005), online: http://www.informationweek.com/story/showArticle.jhtml?articleID=59302233.

[38] Scassa, *supra* note 12, at pp.11.

[39] *Ibid*. at pp. 12, citing the EU Article 29 Data Protection Working Party Document, note the fact that such surveillance could even include a record of a customer handling items but not purchasing them. Therefore, retailers or security staff could monitor when customers transported items from their "proper" shelf to elsewhere in the store and then speculate from either past buying patterns or what was actually purchased as to the reason for the consumer behaviour.

[40] See especially Scassa, *supra* note 12 at pp. 12-13.

Although concerns about RFID privacy invasions of the individual tracking type appear to be remote, even to some privacy commentators, the sheer number of tags that may soon be in circulation will provide for nearly ubiquitous opportunity to integrate RFID signals with existing customer relationship management systems, such as loyalty cards. In addition, much of the initial RFID industry literature and statements indicated that the only use of item-level RFID tagging would be aggregated information streams not tied to any one consumer, used only for mapping out the ideal placement of products in-store.[41] Privacy advocate Katherine Albrecht of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) comments, "this trial [in Germany's METRO stores, described below] is a perfect illustration of how easy it is to set up a secret RFID infrastructure and use it to spy on people".[42]

Fears that the real goal of item-level tagging is customer surveillance appear justified. In fact, the first large-scale retail trial of RFID, involved customer surveillance, and the industry openly markets RFID this way. [43] Finally, despite evidence of this ulterior purpose, the industry continues to insist strongly that the continued activity of RFID tags post-sales is an undisputed "benefit" to consumers. The real goal, however, may be something more sinister: the death of shopping anonymity for consumers.

---

41 See Mark S. Sullivan, "'Tracking' Tags: Tool or Threat? Growing use of RFID technology draws privacy concerns and defense by retailers." PC World Magazine, July 15, 2004, online http://www.pcworld.com/news/article/0,aid,116918,00.asp:

> "Witnesses representing Wal-Mart and Proctor & Gamble assured the panel that they use RFID technology exclusively to collect "aggregate data," not data specific to individual products or people. Even the technical capability to do that, the witnesses added, is "at least ten years away."

42 "Scandal: Wal-Mart, P&G Involved in Secret RFID Testing", Spychips.com, (November 10, 2003), online: http://www.spychips.com/press-releases/broken-arrow.html. Symmetrically, RFID enthusiasts negate the idea that Wal-Mart and P&G did anything wrong, claiming, among other things, that the camera was meant to spy only on the shelf, and not the customers. See Mark Roberti, "The Real Scandal", *RFID Journal*, (November 17, 2003), online: http://www.rfidjournal.com/article/articleprint/654/-1/2.

43 See discussion below regarding 'media awareness networks'.

A Real Retail Scandal

The deliberate tracking of customers via RFID was found by CASPIAN to be the real intention of the self-proclaimed first RFID-enabled store, in Germany.[44] What made this a particularly egregious example of consumer monitoring via RFID was the placement of a hidden, undocumented RFID chip within the store's "Payback" loyalty card. Customers were tracked using the card each time they entered the store using information linked to the RFID chip transmitted to RFID readers. To make matters worse, the store in question had a partnership program with other retailers to share data collected using the card. Thus, whenever a customer of the original store entered a partner store, they could be tracked, by their personal information, if carrying a recognized RFID tag.

The METRO store in question recalled the RFID-chipped loyalty cards after criticism mounted once CASPIAN's discovered their activities. This real-world example proves that business is indeed interested in tracking individuals, and will do so through RFID.

RFID Industry Marketing

The RFID industry itself is marketing the technology as a way to track shoppers' individual movements (and not just anonymous "shopper-flow" in the aggregate). A recent press release from Capgemini, Intel Corporation and Micro Industries touts a system called *Retail Media Networks* that "can even be tailored to an individual shopper by coordination with a store loyalty program."[45] RFID information is so granular, identifying the actual item the consumer has picked up or purchased, that the 'customer relationship management' potential of the data is enormous to retailers and advertisers.[46]

---

[44] See CASPIAN, "The METRO 'Future Store' Special Report - Katherine Albrecht Tours the World's RFID Showcase" online: http://www.spychips.com/metro/albrecht-tour-1.html.

[45] "Retail Media Networks; Influencing Buying Behaviour in Real-Time" online: http://www.us.capgemini.com/DownloadLibrary/files/factsheets/Capgemini_RetailMediaNetworks_FS.pdf. See also Press Release: "Retail Shopping Made Easy", Capgemini, January 17, 2006, online: http://www.us.capgemini.com/news/current_news.asp?ID=539.

[46] *Ibid*. "With RMNs, retailers can drive 1:1 relationships with consumers and leverage knowledge of consumers' buying patterns and preferences."

RFID Industry Post-Sales 'Benefits' to Consumers

Retailers looking to convince consumers of the 'benefits' of live tags after purchase point to many examples. First, RFID tags could carry relevant information that is now printed on receipts, including store identification, price, purchase date, discounts applied and so on. RFID tags could also be used to carry warranty protection information, [47] and as noted, would aid in recalls. The goal would be "receipt-less" item returns, based on EPCs embedded in RFID tags. Second, RFID could also mean "increased convenience" through the interaction of tagged objects and "smart appliances". Examples of smart appliances given by the industry include, for example, reader-equipped refrigerators that allow consumers to itemize products based on expiry date, or issue notifications when items are out of stock.

At present, however, the appeal to consumers of after-sales RFID applications is not clear. Warranties could now be voided if the RFID information is not kept intact.[48] Similarly, product returns may not be accepted for the same reason.[49] Retailers may well place RFID chips in locations that would be inaccessible to attempt to avoid warranty or shoplifting fraud[50] – and in so doing ensure trackability of an item without consumer consent.

---

[47] Refer to Scassa, *supra* note 12. This raises the added concern of dealing with customers who choose to remove RFID tags from their products and maintaining and honoring warranties in those cases where RFID tags have been disabled.

[48] Wal-Mart has stated cryptically, "Consumers may wish to keep RFID tags on packaging to facilitate returns and warranty servicing" in response to questioning by EFF.

[49] See Mary Catherine O'Connor, "Ending Retail Scams with RFID", RFID Journal, November 30, 2004, online: http://www.rfidjournal.com/article/articleprint/1260/-1/1/.

[50] *Ibid*. Evidently, to avoid frustration of the RFID security for fraudulent returns, the tag must essentially be hidden or inaccessible to the point where removing it would leave damage:

> Retailers would place the tags at their own discretion, but would most likely locate them in discrete parts of the product where the tag is not susceptible to physical damage. If an item were returned with a tag that showed signs of tampering or an attempt to disable it, the retailer may decide not to accept the return.

Post-Sales Privacy Concerns

If these trends continue unabated, consumers will likely soon carry around many RFID tags that have not been 'killed',[51] at the point of purchase. Indeed, many Canadian consumers are beginning to discover tags in purchased items from larger retailers, particularly in clothing. These 'live', tags, if read periodically, could potentially allow movements to be tracked in time and space.[52] Furthermore, if a consumer physically possesses several tagged items simultaneously, and carries them into a scanning environment, these items could be linked to one another. Each item could be looked up in the appropriate database, and the information from each cross-referenced.[53] The cumulative effects of these hypothetical uses could prove to be powerful in constructing detailed consumer profiles, and may produce revealing conclusions.

As Ann Cavoukian posits in her paper:

> Corporations which compile the data transmitted by the tags could determine which products a consumer purchases, how often those products are used, and even where the product – and by extension the consumer – travels. By aggregating data to form consumer profiles, corporations could make inferential assumptions about a consumer's income, health, lifestyle, buying habits, and location. That information could be sold or exchanged with government agencies to create dossiers of individual citizens, or simply sold to other corporations for marketing purposes. [54]

---

[51] Refer to pp. 49 below for discussion on Killing Tags.

[52] It must be noted that tracking customers after they have left the retail environment, using live RFID tags, is unlikely at this time. There are several obstacles to the widespread use of this practice, including the following:

1. Retailers typically use low-end tags that don't work at long distances, or oftentimes, outside of the store (Ultra High Frequency (UHF) tags, the kind most likely to be widely used, are virtually unreadable near the human body because of its high water content. Scanning RFID-tagged clothing is not necessarily an easy matter. RSA Laboratories, Protecting Consumer Privacy, 2004, online: http://www.rsasecurity.com/rsalabs/node.asp?id=2119. See also http://www.ccip.govt.nz/ccip-newsletter/2004/ccip_newsletter_V318.pdf. Ultra High Frequency (UHF) is in the 850 to 920 Mhz range);
2. There hasn't yet been a standardization of RFID tags, especially at the low end of the spectrum, thus rendering many systems incompatible;
3. Finally, data sharing would necessarily require agreement to share data collected, which may or may not be attractive to competitors.

While this concern is somewhat theoretical at present, as tags improve and standardization spreads, real privacy risks may develop as a direct consequence.

[53] See "Total Surveillance" an interview of Katherine Albrecht by Michael Beckel, Mother Jones, December 6, 2005, online: http://www.motherjones.com/interview/2005/12/albrecht.html.

[54] Cavoukian, Tag You're It, *supra* note 4, at pp. 15.

Katherine Albrecht of CASPIAN goes further and suggests that retailers would profile a customer in real-time based on an RFID read of objects carried and by cross-referencing to past buying patterns, and may offer differential service based on the 'value' of the customer to the retailer.[55] Ironically, more loyal shoppers may end up paying more for products than other shoppers as retailers develop the ability to track product desire and ability to pay. Additionally, retaining such detailed information, especially when compiled with existing databases of "customer relationship management" information,[56] poses an incredible privacy risk to customers.

Finally, if retailers do indeed institute the practice of keeping RFID tags live post-sales in order to administer exchanges/recalls, maintain warranty information, or for smart-appliance functionality, then mandatory deactivation will become difficult to enforce. It will also be difficult to formulate privacy policies that provide consumers with a meaningful opportunity to give consent to this use of RFID. [57]

Payment and Commercial Transaction Privacy Concerns

RFID systems, when used to complete transactions, are vulnerable to fraud and even identity theft. Unauthorized readers could read tags and deduct money or carry out other transactions to the detriment of the consumer.[58] While many of the issues have already been raised in the context of credit card and bank debit card use, the use of RFID may involve many more transactions and hence broaden the scope of concern. As well, if small dollar amounts are involved,[59] fraud may not be as readily noticed.

Even money could be tagged. The European Union has proposed putting RFID tags into currency.[60] The intent is to help deter counterfeiting and prevent money

---

55 See 'Total Surveillance", *supra* note 53, where Albrecht states:
> That's the retailer's dream: Instead of having to rely on all of this extremely expensive technology to follow you and watch you walk around the store, they can issue you something that you put in your wallet willingly [an RFID chipped loyalty card]. That way they could figure out how long you stood in front of the bread aisle or they could figure out how long your shopping trip took. They could identify you from the moment you walked in the door. They could identify your value to the store and then treat you differently depending on how profitable you are.

56 Cavoukian, Tag You're It, *supra* note 4 at pp. 15.

57 The issue of consent, RFID and privacy is dealt with in "RFID and Privacy Law in Canada", below pp 31 and following.

58 Symmetrically, fraudulent tags could be used to cheat businesses.

59 See Dexit micropayment system at note 13, *supra*.

60 See Kim Yon-Young, "Radio ID Chips May Track Banknotes", CNET News, May 22, 2003, online: http://news.com.com/Radio+ID+chips+may+track+banknotes/2100-1017_3-1009155.html.

laundering by recording transactional information.[61] As an additional benefit, RFID tagging could speed up routine bank processes, such as counting, because readers could sum stacks of bills in a split second.

Embedding tags in paper currency, with the avowed intent of following that currency's movements, raises a large number of serious privacy issues. These include tracking persons' movements in space and time, their purchases and where those purchases are made, when they receive money and from whom, and when and where they do their banking. Some have even speculated about currency that can be programmed to self-immolate in the hands of compulsive gamblers.[62] However, the real impact is in making a formerly anonymous transaction method, cash payment, now eminently trackable to whichever organization has access to the RFID-cash payment records.

The Electronic Privacy Information Center concludes: "RFID should never be employed in a fashion to eliminate or reduce anonymity. For instance, RFID should not be incorporated into currency."[63] Cash payments are a well-established route for anonymous payment which society has tolerated as useful for thousands of years. However, governments' desire to curb counterfeiting and money laundering and retailers' thirst for knowledge about their customers may outweigh such concerns and convenience in the long run.

---

[61] RFID tags would be the size of a grain of sand, embedded in the Euro note, and act as "digital water marks", the primary objective being the determination of authenticity. Winston Chai, CNET Asia, "Euro Notes May be Radio Tagged", ZDNet U.K. News, May 22, 2003, online: http://news.zdnet.co.uk/business/0,39020645,2135074,00.htm.

[62] See EPIC, "Radio Frequency Identification: Applications and Implications for Consumers" Comments to a FTC Workshop, June 21, 2004, at pp. 35-37. Online: http://www.epic.org/privacy/rfid/ftc-comts-070904.html. Besides being a fire and injury risk, would this not also be extremely embarrassing situation for an individual?

[63] See EPIC, "Radio Frequency Identification: Applications and Implications for Consumers" Comments to a FTC Workshop, June 21, 2004, at pp. 35-37. Online: http://www.epic.org/privacy/rfid/ftc-comts-070904.html"

Health Risks of RFID

To date, minimal effort has been expended on the possible health risks of RFID and similar "electronic article surveillance" (EAS). Exploring risks of radio wave exposure in humans will likely take a concerted effort and be difficult to state definitively. That does not mean that RFID and EAS could not pose a health risk, especially if the readers and their tags become as ubiquitous as the industry predicts.

The European Community is the first jurisdiction to address the issue directly, in EC paper, *Possible Health Risks to the General Public from the Use of Security and Similar Devices*.[64]

This document is a summary of potential problems with exposure to RFID and EAS devices. The report notes that at the frequencies used presently for low-grade passive RFID (i.e. between 100kHz and 10 MHz) that a combination of "membrane excitation" and heating can occur. Above 10MHz, "heating effects are well established".[65] However, the report concludes that generally exposure levels from high frequency security devices would be "many times below those that would induce a physiologically relevant heating".[66] The EC report therefore recommends further study of electromagnetic radiation from RFID and similar devices at the design stage.[67] The report also recommends that exposure studies to be undertaken to specifically study the effect upon children, as children will also be exposed to RFID and their potential sensitivity to electromagnetic fields.[68] It would also seem sensible to study those likely to have chronic exposure levels, such as check-out cashiers.

The EC report additionally suggests that larger problems may exist with RFID interaction with medical devices:

> The reported cases of electromagnetic interference with certain critical medical devices remain a concern. […]

---

[64] International Commission on Non-Ionizing Radiation Protection, "Possible Health Risks to the General Public from the Use of Security and Similar Devices", 2002 [***Possible Health Risks***], online: http://www.icnirp.de/documents/ExSummary.pdf.

[65] Note that the EPCglobal RFID standard protocols run at 13.56 MHz (the most common passive tags); 900 MHz; and 860 MHz – 960 MHz (EPCglobal Class 1, Gen. 2 Protocol).

[66] Possible Health Risks, s*upra* note 64 at pp.11. The report notes, however, that the mid-range frequencies (100 kHz to 10 MHz) have not been extensively studied. Some RFID applications use these frequencies.

[67] *Ibid*. at pp.13. "There is also a need to collect exposure data about RFID systems. When such technical information becomes available during the development of a new product or application, a health hazard assessment should be undertaken to identify likely problems in complying with exposure guidelines. Awareness of the magnitude of the likely exposure of people as a result of the envisaged use of a system should be an integral part of the development process."

[68] *Ibid.* at pp. 14.

> More data are needed on the emissions of EAS, RFID or metal detector systems and on the interference with all kinds of active implantable medical devices. The data must be publicly available […] to make informed choices. [69]

Certainly consumers are concerned about radio wave exposure from RFID devices.[70] However, all that can be said at present is that the issue of healthy exposure levels for RFID systems, as well as guidelines for their interaction with medical devices, has yet to be undertaken. Thus, introducing RFID technology in advance of these health studies means taking some kind of risk, whether that risk is large or small, with public health.

---

69 *Ibid.* at pp. 12 and pp.15-16.

70 See "Consumers' Perceptions of RFID Technology", below.

RFID AS SURVEILLANCE

At first glance, it may appear that RFID is not a serious tool for surveillance. Critics and vendors state that the surveillance concerns of groups such as CASPIAN and EPIC are overblown.[71] They note, for example, that:

- Most chips are not designed to be self-powered, limiting their range and thus usefulness for tracking;
- Readers are not deployed in public places, nor are they likely to be;
- At present there are no plans for businesses to read each others' chips, or for the state to monitor business' chips
- Customers may simply make a habit of removing tags;
- There are no [clearly stated] plans to make tags inaccessible, so small as to be imperceptible, to require them for warranty service, or to make devices inoperable without them.

Yet, it is worthwhile noting that there are no guarantees that these "realities" will hold for the future. Indeed, there are several trends which appear to contradict these assurances, perhaps most notably that the chips will not get smaller,[72] that readers will not become more prevalent, and that they will not become required and essentially integral to the operation of some devices. Since most chips use unencrypted protocols, the assertion that no one presently reads another's tag does not preclude someone from attempting to do so, or a retailer from being able to read the tags of another retailer. Further, as seen below, claims that the information from RFID chips will not be linked to personal information gathered in other ways (such as through loyalty cards) either by business or government is naïve.

Rather, RFID tags have the potential to play the role of an essentially low-tech tracking device in a system of distributed mass surveillance. At present, such a system is uncoordinated and patchy. However, with only a slight shift in the present reality, a shift that is already occurring, RFID devices and their readers will form the infrastructure of a massive public surveillance architecture. Only by laying down clear legal ground rules now can consumers avoid a system to be deployed to track them.

---

[71] See Mark Roberti, "New Rules of the Game" RFID Journal, March 8, 2004, online: http://www.rfidjournal.com/article/articleprint/820/-1/2/.

[72] Cavoukian, Tag You're It, *supra* note 4 at pp. 9, where she discusses the development of 'smart dust' chips that are all of 1 millimeter square.

RFID Ubiquity

It is very likely that RFID will in fact create an architecture of potential surveillance. RFID is slated to take the place of the bar code as well as function within devices where bar codes have, until now, been impractical. This means there will be potentially billions of readable tags in circulation in a few years.[73] Millions are presently circulating. This means that the tag end of the architecture is being rolled out. Now, all that is needed to complete the system is a network of readers.[74]

As an example, think of readers located at the entrances and at various key points in shopping malls. The merchants could quite conceivably agree to share data on all customers regarding all items bought and tagged in that mall. Mall management might also even participate in this reader information gathering initiative in order to study, for example, customer movements. As the information will be shared and as customers with tags will likely return to the mall with at least one recently purchased and tagged item, reader ubiquity could be an extremely easy way to monitor the movements of many customers with a minimal number of readers. One of the main criteria of surveillance architecture – ubiquity – is indeed becoming a reality with RFID.

The Soul of the Chip

RFID is not, at least at one level, *intended* in most instances to identify and track persons, but simply things. Also, the undertaking to track individuals may be a difficult or even risky strategy if it is discovered and deemed objectionable by consumers.[75] However, this attitude tends to overshadow the realization on the part of most observers that RFID is at its core about *tracking* things. This very fundamental point should not be glossed over. By it's nature, RFID is a tracking tool. What makes RFID potentially a *surveillance tool* is that people interact with

---

[73] See Cavoukian, Tag, You're It, *supra* note 4 at pp. 11: "As many as 40-billion objects could be tagged each year by the end of the decade when the market for RFID systems, software and tags could be worth $10 billion (US) a year, according to a report prepared for the MIT Auto-ID Center."

[74] Note, however, that unless tags are designed *not* to be read except by readers associated with the retail location where the item was bought, and provided the tags are not deactivated, that very few readers could potentially provide basic tracking information on an individual. Recall that tags provide exact information not only on the item but also, potentially, on the individual, if they either are so programmed at point-of-sale or can be cross-referenced with personal information gathered at the point of sale (e.g. information from a credit card or from RFID chips implanted directly in loyalty cards.

[75] See Mark Roberti, "Spychips Book Fails to Make Its Case", RFID Journal, Oct. 24, 2005, online: http://www.rfidjournal.com/article/articleview/1947/1/128/.

those things in observable and meaningful ways. [76] Employees load and manage tagged objects in stores. Customers, however, have a more long lasting and important relationship with tagged objects – they walk around with them inside stores; they buy them, take them home and out with them again.

Many consumer goods travel with the consumer outside the home. Cell phones, MP3 players and game consoles accompany many people to nearly every destination. Durable clothing such as shoes or coats are also worn frequently. What this means is that consumers will likely be unaware of the tracking capability of RFIDs in these common things, due simply to their everyday nature.

Likewise, there is no admission, and possibly no recognition, on the part of business that they are creating a surveillance mechanism not of items but of people – at least once consumers purchase a tagged item. It is this steadfast repetition of the mantra that 'RFID tracks things, not people', that makes it dangerous. This doctrine allows the architecture to be aggressively rolled out by business, and RFID tags kept live and ostensibly to be used for many 'valid business purposes' (such as warranty service or special offers), without acknowledging the associated surveillance potential.

Thus, the question must be asked: do businesses know of the surveillance potential of RFID? Even if the answer is no, and they do not yet recognize the surveillance potential of RFID, there is cause for concern. It is also worrisome to unwittingly build an architecture of surveillance by pursuing other business or government goals which incidentally facilitate mass surveillance.

---

[76] See Stephanie Perrin, "RFID and Global Privacy Policy", in *RFID: Applications, Security, and Privacy*, Simson, Garfinkel and Beth Rosenberg (eds.), Addison-Wesley Professional, 2005, [***Perrin***] online: http://idtrail.org/files/Perrin%20%20RFID%20and%20Global%20Privacy%20Policy.pdf. At p. 100, she states:

> Now RFID brings to us an "Internet of things," on which objects talk about their owners or handlers, thus feeding powerful new databases. Industry proponents protest that the chips are not big enough to be intelligent, but the chips' "chatter," even if it is only in monosyllables, which brings to a new level a world in which humans hold increasingly less power and information holds increasingly more. In discussions about "trust" and "security", the emphasis is on building trusted systems. But does this mean we no longer trust humans?

RFID and 'Lawful Access'

Consumers and citizens should also be aware of the essential similarity of the information made available by RFID chips, and the 'tracking and location' information sought to be accessed by law enforcement officials in Canada under the federal government's recent 'lawful access' proposals.[77] Those proposals recently culminated in Bill C-74, the *Modernization of Investigative Techniques Act* (*MITA*).[78] Although *MITA* died on the order paper in December 2005, there is little doubt the legislation will be re-introduced in the next Parliament.

Consumer and civil liberties groups have heavily criticized the Act, and the lawful access proposals that preceded it, for being overbroad and lacking judicial oversight and reporting mechanisms. The likelihood that RFID tags will be considered a "telecommunications facility",[79] under the Act, or that the readers will be considered part of a "telecommunications service"[80] or at the least a "transmission apparatus"[81], appears at least plausible. Equally plausible is that *MITA* would be amended slightly, given the similarity of information provided by RFID tags to the definitions of 'location information' and 'tracking information' under *MITA*. Therefore, consumers and citizens should realize that the creation of an essentially business consumer-reporting architecture could be appropriated to the "public safety" goals of the state with little difficulty.[82]

---

[77] See the Federal Government's 'Lawful Access' Consultation page at: http://www.canada.justice.gc.ca/en/cons/la_al/

[78] 1st Session, 38th Parliament 53-54, Elizabeth II, 2004-2005, First Reading: November 15, 2005.

[79] Text of definition reads: "telecommunications facility" means any facility, apparatus or other thing that is used for telecommunications or for any operation directly connected with telecommunications.

[80] Text of definition reads: "telecommunications service" means a service, or a feature of a service, that is provided by means of telecommunications facilities, whether the provider owns, leases or has any other interest in or right respecting the telecommunications facilities and any related equipment used to provide the service.

[81] Text of definition reads: "transmission apparatus" means any apparatus of a prescribed class whose principal functions are one or more of the following:

(a) the switching or routing of communications;
(b) the input, capture, storage, organization, modification, retrieval, output or other processing of communications;
(c) the control of the speed, code, protocol, content, format, switching or routing or similar aspects of communications; or
(d) any other function that is similar to one described in paragraphs (a) to (c).

[82] This is especially easy now that *PIPEDA* has been amended to permit a government security agency to request business information without notice or consent (see *PIPEDA*, s. 7(3)(c.1)(i) and (ii)) and to allow business on its own initiative to forward business records thought useful for 'national security' to the appropriate authorities without the subject's knowledge or consent (see *PIPEDA*, s. 7(3)(d)(i) and (ii)).

RFID IMPLEMENTATION

Given the potential for creation of a surveillance architecture with RFID (even if that architecture is initially patchy, or only partly used, or not coordinated between vendors), and given the likely temptation of marketers and governments to compile tracking information on individuals, it is prudent for consumers and citizens to demand the utmost in transparency and to require clear rules on the limits of the acceptable use of such information. To accept that such a high level of privacy control over RFID is required, consumers and citizens must be persuaded that RFID is indeed like other kinds of surveillance. If this can be demonstrated, the question becomes the extent to which present privacy law in Canada can be privacy-vigilant enough to halt mass surveillance use of RFID and whether privacy law should be modified considering RFID architecture and it surveillance possibilities. It is to these questions that this paper now turns.

RFID and Video Surveillance

RFID does not provide an actual visual image of a person going about their business, and so is less privacy-invasive than video surveillance. However, that does not mean that RFID cannot provide the 'observer' – that is, the person with access to RFID data – with a mental picture of the individual carrying a RFID tag. This could be achieved, for example, by associating the RFID chip with an individual, using either the individual's personal information from credit payment or loyalty card information at point of sale, or more directly, by encoding the RFID chip either at the point of sale or earlier with personal information. This is the METRO "Payback" loyalty card approach described above.

With such an identifiable RFID chip located on a person, RFID reader systems can tell things the eye can see and also, significantly, provide a detailed record of things the eye *cannot* see. One can track movements of an individual via RFID chip as with video surveillance, but one can also ascertain how long the individual took to proceed from RFID station to RFID station, and then link that to the individual at the point of sale.[83] Although no retailers admit to linking the

---

[83] See E. Murphy, "Tracking Grocery Hot Spots" Portland Press Herald, January 27, 2004:

> PathTracker consists of small sensors attached to shopping baskets and carts that allowed the system to monitor where people went through the store. / It recorded their route and timed how long they lingered in specific areas, producing printouts that look like thermal sensors. Crowded areas generated bright colors and became hot spots. Places shoppers avoided became cold spots. / At checkout, the system married the information on where shoppers went with what they bought, giving researchers a picture of how a consumer shops and what's the end result.

RFID path-tracking and timing to individual profiles,[84] there is no impediment, technologically, to doing so.

Notably, in *combination* with the video surveillance that is prevalent in a retail environment, RFID enables another, powerfully detailed dimension to video surveillance. However, even without accompanying video surveillance, RFID would allow a retailer to track customers' movements through a store and even whether they had picked up an item, regardless of whether the customer entered a camera "blind zone" or had successfully hidden an item in a pocket, bag or purse.

RFID and Location-Based Tracking Devices

Unlike RFID's somewhat haphazard tracking capabilities, there are systems that are *specifically* designed to track location. Such "location-based services" are designed to report a subject's position with incredible precision (i.e. to less than 150 metres) on a regular basis.[85]

These are cellphones and other Global Positioning System (GPS) devices that report location to computer systems that parse the signals into useful tracking information like direction of travel, speed and of course location at the time of communication with the device. Unlike RFID, these systems are designed to act over large distances and to track one device continuously. Professor Colin J. Bennett of the University of Victoria has studied the LBS technology (Location Based Service) in Canada and has concluded that:

> From the [LBS] examples listed above the potential challenges to existing regulatory frameworks, such as that framed by the […] *PIPEDA* in Canada are enormous. Locational data can be extraordinarily sensitive. It can be monitored remotely, without the individual's knowledge and consent. It may be collected continuously and stored indefinitely. The level of consumer education and experience is low. And the potential value of such information government and for business is enormous. [86]

Colin Bennett has noted that the application of *PIPEDA* to LBS may yield a requirement that explicit consent is required for tracking 'sensitive' information because the category of what is 'sensitive' personal information must be viewed

---

[84] However, see discussion of media relationship networks below.

[85] See generally regarding privacy and location-based services, Colin Bennett and Lori Crowe, "Location-Based Services and the Surveillance of Mobility: An Analysis Of Privacy Risks In Canada" A Report to the Office of the Privacy Commissioner of Canada, under the 2004-05 Contributions Program, June 2005, online: http://web.uvic.ca/polisci/bennett/pdf/lbsfinal.pdf.

[86] *Ibid.* pp. 33.

in light of the locational context that LBS makes possible.[87] He has also noted that *PIPEDA* may not fully capture the concept of "trajectory" as personal information; that is, the apparent and actual destination, as well as route taken by persons carrying LBS-equipped devices.[88] Bennett notes other problems with application of the general *PIPEDA* principles to LBS, such as the degree of accuracy required of LBS records, which are presently not able to exactly pinpoint an individual – leaving open the possibility of false inferences regarding an individual who simply passes near a 'sensitive' area.[89] Similar concerns would seem to apply to RFID, as the locational data would be quite similar to that collected under LBS systems.

What has not been examined with regard to LBS is the potential for it to be combined with RFID's short-range detailed information. One use would then be to help to "de-anonymize" RFID carriers by potentially cross-referencing them with, for example, a location-reporting cell phone. RFID can then be used to determine an individual's location when out of LBS range, but more importantly perhaps, will allow nearly microscopic sub-tracking of individuals within an RFID-reader enabled zone (such as a shopping mall). Any cross-referencing between the systems could allow the LBS provider to know what RFID tagged object the LBS subject was carrying in addition to their exact route, making for a very powerful tracking "system" indeed.

87 *Ibid*. at pp. 36-37.
88 *Ibid*, at pp. 37.
89 *Ibid* at pp. 36-37.

RFID AND PRIVACY LAW IN CANADA

Given that RFID may present privacy problems that are new and unique to consumers, how does Canadian privacy law treat it and how should it deal with RFID privacy concerns?

Privacy as a Charter Right

The right to privacy is not a constitutionally protected right in Canada on its own.[90] Rather, privacy is discussed in various constitutional law cases involving search and seizure. In these cases, a determining factor with regards to the admissibility of evidence after a search was consideration of whether the accused person had a 'reasonable expectation of privacy'. The latest Supreme Court of Canada statements on 'reasonable expectation of privacy' do not bode well for those looking to limit the permissible uses of RFID. First, in the case of *R.* v. *Wise*, [91] a tracking device was surreptitiously attached to a suspect's car. The Supreme Court of Canada concluded that the accused's expectation of privacy was lower in a vehicle than in his home and further, seemed unconcerned about the 'tracking' nature of the observation. Second, in the case of *R.* v. *Tessling*,[92] an infrared scanner mounted on a low-flying plane identified several 'hot' residences. The police used this scanner information to obtain a warrant to search the house of the accused on the theory that the accused was growing marijuana under lamps that produced more than the average heat for a house. What is truly important about the case for RFID, however, is the following statement made by Binnie J.:

> In my view, with respect, the reasonableness line has to be determined by looking at the information generated by existing FLIR [infrared scanning] technology, and then evaluating its impact on a reasonable privacy interest. If, as expected, the capability of FLIR and other technologies will improve and the nature and quality of the information hereafter changes, it will be a different case, and the courts will have to deal with its privacy implications at that time in light of the facts as they then exist. [93]

So the principle appears to be that in Canadian constitutional and criminal law at least, that when a technology is insufficiently developed to be a truly 'effective' way of putting someone under surveillance, that that surveillance will not violate

---

[90] This is in contrast to the United Nations *Universal Declaration of Human Rights* and the *European Convention on Human Rights*, which provide numerous privacy rights. See Perrin, *supra* note 76 at pp. 103-7.

[91] [1992] 1 S.C.R. 527.

[92] [2004] 3 S.C.R.

[93] *Ibid*. at para 29.

a person's reasonable expectation of privacy. Until the technology matures and becomes effective in providing a detailed profile, the subject of the surveillance will simply have to tolerate the surveillance.

However, such a legal regime appears too blunt to deal with the effects of RFID. RFID can be viewed at present as an undeveloped, low level or "dumb' technology. But, as demonstrated in the "Payback" example investigated by CASPIAN, can be easily combined with other known information collected and other technologies to track individuals. It is the equivalent of a beeper under our bumpers at nearly all times.

RFID and PIPEDA

Fortunately, the protection of *personal information* (though not 'privacy' *per se*) in a civil context is regulated by the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[94] in Canada. *PIPEDA* sets out ten principles for the protection of personal information. This regime, when applied to RFID, may set reasonable boundaries on the use of RFID that might otherwise go unmonitored long enough to generate the sort of privacy violations the Supreme Court suggested a mature technology might produce in *Tessling*. Fortunately, *PIPEDA*'s framework for the most part should protect consumers from becoming the "guinea pigs" in business' rush to roll out RFID.[95]

OPCC View

To date there has been no finding regarding RFID in the context of a *PIPEDA* complaint. The Office of the Privacy Commissioner of Canada (OPCC) has, however, expressed its concern about the issue, both funding the Scassa report (referred to elsewhere) and also in indicating the OPCC's priorities in the coming years in the most recent, 2004-2005, OPCC Report to Parliament. In this report, the OPCC states that:

---

[94] S.C. 2000, c. 5.

[95] It is interesting to note that Scassa et al., conclude in their paper, *supra* note 12, that *PIPEDA* as drafted is inadequate to properly regulate RFID use, and that specific privacy guidelines for RFID under *PIPEDA* should be developed (Recommendation #4, at 62):

> While existing private sector privacy legislation such as *PIPEDA* will apply to personal information collected, used or disclosed in the course of commercial activity involving RFIDs, existing principles and guidelines must adapt to the nature of the technology to ensure proper respect for personal privacy from the outset. Technology-specific guidelines must be established to outline the specific practices necessary to bring RFID use in line with the legislation.

> Organizations must think carefully about the legal implications of deploying RFID systems. Amidst the flurry of activity involving RFIDs, very few people fully understand the myriad of privacy implications. We are now encountering many marketplace uses of RFIDs, and expect that we will soon be investigating complaints about tracking the use of RFIDs. [96]

However, in a section entitled "Keeping Watch on Radio Frequency", the OPCC indicates that it is sensitive to claims that RFID may violate *PIPEDA* principles if implemented in certain ways, and also that the OPCC is sensitive to how RFID fits into a 'system' of data mining and other surveillance:

> We continue to monitor advances in RFID technology. In our view, companies should establish policies and standards before they implement RFID technology, not after the fact. Any use of RFIDs must comply with *PIPEDA*. Furthermore, we want to know the role of RFID applications in data aggregation and mining activities, since these depend on obtaining ever-increasing amounts of detail about individuals and what they buy or rent.
>
> We plan to send letters to selected corporations in Canada that might be introducing RFIDs, to better understand the emerging uses of RFID. Our primary interest is in learning how RFID might be used to link personal information with products and services. We want to know if the technology will be used to identify or track individuals. We also want to know if companies will do privacy impact assessments or threat/risk assessments when developing and implementing RFID applications, and how employees and customers would learn about the presence and use of RFIDs.
>
> […] We will continue monitoring developments in RFID technology to see where guidance on privacy issues is necessary. [97]

Such proactive action as asking companies to outline their privacy policies and suggesting privacy impact assessments prior to the roll out of a technology on the part of the OPCC is somewhat the exception, as the office has been more reactive in most situations. This concern, along with that expressed by provincial privacy commissioners,[98] seems to indicate that companies should take care with RFID and clearly think through its implementation and how that implementation

---

[96] Privacy Commissioner of Canada, "Annual Report to Parliament, 2004: Report on the Personal Information Protection and Electronic Documents Act", Minister of Public Works and Government Services Canada, October 2005, [***OPCC***] at p. 10, online: http://www.privcom.gc.ca/information/ar/200405/2004_pipeda_e.pdf.

[97] *Ibid*. at pp. 76-77.

[98] See, for example, Cavoukian, Tag You're It, *supra* note 4.

will be treated under *PIPEDA* before investing heavily in potentially non-compliant RFID systems.

We turn therefore to a detailed consideration of the likely requirements of *PIPEDA* on an RFID system aimed at consumers both pre- and post-sales.

PIPEDA's "Privacy Commandments"

Subsection 5(1) of *PIPEDA* requires organizations to comply with Schedule 1. Schedule 1 generally requires prior consent of the individual for the collection, use or disclosure of personal information. Subsection 5(3) of *PIPEDA* also contains an overarching "reasonableness" test and provides that: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances."

Schedule 1 contains most of the detailed requirements regarding the collection, use and disclosure of personal information. These are organized into ten sections. They can be summarized as follows: [99]

1. Accountability: Organizations must designate an individual to be accountable for their compliance with the principles. They must also ensure that third parties to whom they transfer data for processing provide a comparable level of protection.

2. Identifying Purposes: Organizations must identify the purposes for which they collect personal information at or before the time of collection.

3. Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Consent to secondary marketing purposes may be obtained via negative option (also referred to as "opt-out") as long as the sensitivity of the information and the reasonable expectations of the individual do not suggest otherwise. But organizations cannot, as a condition of the supply of a good or service, require an individual to consent to information collection, use or disclosure "beyond that required to fulfil the explicitly specified and legitimate purposes."

---

[99] This description is taken from Phillippa Lawson, "Techniques of Consumer Surveillance and Approaches to their Regulation in Canada and the USA", March 2005, a paper presented at the tenth annual International Consumer Law Conference in Lima, Peru, May 4-6, 2005, at pp.14-15, online: http://idtrail.org/files/Techniques%20of%20Consumer%20Surveillance%20w%20footnotes.pdf.

4. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6. Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Regarding RFID, the greatest challenge for compliance comes from the Identifying Purposes principle (Principle 2), the Consent principle (Principle 3), and also by limiting collection, use and disclosure of personal information (Principles 4 and 5). There are other, less serious but still important questions around the other principles, notably safeguards (Principle 7).These main principles shall be examined in the context of RFID below.

While it is important to note what *PIPEDA* requires, and acknowledge that the OPCC seems intent on using proactive measures to encourage compliance, ultimately it is up to consumers to ensure companies comply with *PIPEDA* through individual privacy complaints.[100] It is equally important to be clear that any conclusive decisions regarding Canadian privacy requirements and RFID will

[100] See J. Lawford, "Consumer Privacy under *PIPEDA*: How are We Doing?", PIAC, 2004, online: http://www.piac.ca/privacy/report_consumer_privacy_under_pipeda_how_are_we_doing/.

need to be aligned with U.S. standards for RFID implementation.[101] There will certainly be pressure to align Canadian privacy law for RFID with the law in the U.S. on RFID use. However, since there is no overarching personal information protection legislation in the U.S., the pressure naturally will be to "dumb-down" the Canadian rules involving RFID to the U.S. standard. Canadians therefore must be very clear on what *PIPEDA* (and similar provincial privacy legislation) requires of RFID systems.

Identifying Purposes

Principle 2 of *PIPEDA*, the 'Identifying Purposes', provision, requires organizations to identify the purposes for which they collect personal information at or before the time of collection. Indeed this is the first of many ways in which RFID chip systems will fail to comply with *PIPEDA*. Most commentators have either assumed,[102] or offered,[103] that a notice should be posted in retail establishments regarding RFID tracking in light of *PIPEDA* and similar privacy legislation. Such a notice should be prominent and explain in sufficient, understandable detail, how information collected will be used,[104] as well as identify the items being tracked. Similarly, it is said that consumers should be notified of the presence of RFID tags on tag bearing items themselves.[105]

Although this may seem a convenient solution to ensuring that consumers are given notice, there are three problems with relying solely on this approach. First and most important is that the purposes identified in such a notice are unlikely to reveal unplanned collections and possible uses and disclosures of the information on an RFID tag.[106] For example, it is very unlikely that a retailer will believe it necessary to identify the possibility of another retailer's potential ability to read tags when the consumer visits a different store as a 'purpose' of RFID

---

[101] According to Decima Reports ICT Update Industry Canada has adopted new rules regarding RFID (RSS-210), making it easier for the deployment of RFID equipment in both Canada and the United States. The rule changes involve modifications to RSS-210 that will align with the technical standards currently in force in the U.S., and that will permit the development of RFID devices, which can operate in other countries. Source: blog*on*nymity: "Industry Canada makes RFID deployment easier",
posted by: Philippa Lawson // 12:26 PM // September 19, 2005 // Digital Democracy: law, policy and politics (online:
http://www.anonequity.org/weblog/archives/cat_digital_democracy_law_policy_and_politics.php).

[102] Scassa, *supra* note 12 and Cavoukian, Tag You're It, *supra* note 4.

[103] Derren Bibby, "Squaring the Circle with RFID and Privacy", CRM Buyer, November 29, 2004, online: http://www.crmbuyer.com/story/Squaring-the-Circle-with-RFID-and-Privacy-38385.html.

[104] Scassa, *supra* note 12 and Cavoukian, Tag You're It, *supra* note 4.

[105] See EPIC, "Comments submitted in consideration of the Article 29 Data Protection Working Party "Working Document on Data Protection Issues related to RFID Technology"" at p. 9, online: http://www.epic.org/privacy/rfid/comments_art29.pdf

[106] See Perrin, *supra* note 76 at pp. 113.

use. However, based on the discussion below regarding the consent requirement for RFID use and the danger of leaving tags readable to outside readers, this (unintended) "purpose" should indeed be revealed.

Second, simply posting a sign or statement on a tag noting the presence of RFID does not provide consumers with a real opportunity to understand the proposed uses and disclosures of personal information via RFID. The adequate standard for consent for RFID or similar surveillance-friendly technology may be higher. The purposes identified must be explicitly brought to the attention of the person to get true consent to the proposed purposes.

Third, it is possible that a retailer will not think it necessary to include potential data matching purposes, for example, that RFID information may be matched against other personal information systems to produce a more detailed overall customer profile, in their notice to consumers. Instead it is likely that the retailer may treat the RFID information as a discrete activity, although the ultimate goal is to combine it with information gathered from, for example, loyalty card programs or video surveillance footage.[107]

The argument above regarding what is required of a 'purposes identifying', document or procedure relies on the argument below as to the adequate level of consent required from consumers. It does not seek to undermine the requirement of notice on tags and posted in-store. Rather, this view questions the extent to which notice can prop up a situation in which true consumer consent to RFID use may not be practicable or even permissible.

Consent

Consent is the largest and most difficult problem facing RFID technologies. The consent issue applies to both the pre-sales and post-sales contexts, but with varying results. However, for both pre-sales and post-sales contexts, the legal standard mandated by *PIPEDA* is the same: informed consent.

The highest court interpretation of *PIPEDA* consent requirements is the Federal Court of Appeal decision in *Englander* v. *TELUS Inc,*[108] where the Court made it clear that the appropriate standard under *PIPEDA* is informed consent.[109] This clear requirement to explain, at or before the time of collection, all the uses to which personal information will be put is the essence of informed consent. Commentators have downplayed this clear direction issued by the Federal Court

---

107 This is discussed for fully in the section on consent, below.

108 [2004] FCA 387

109 "Principles 2, "Identifying Purposes," and 3, "Consent," are at the heart of this appeal. Principle 3, I hasten to add, despite its name, "requires 'knowledge and consent' " (clause 4.3.2). ***In other words, Principle 3 requires <u>informed consent</u>.*** [Emphasis added.]"

of Appeal, possibly because it does not sit comfortably with automatic information collection technologies like RFID.[110]

To the extent that *any* information is collected in-store prior to this full and informed disclosure, the consent burden would not be met. In the out-of-store context, such full disclosure would be non-existent, as readers belonging to other retailers, mall owners, parking operators etc. would be tracking the RFID by chance or by stealth. Even if the readers outside the original retailer acknowledged that they intended to 'spy' on any chips passing by, it may be impossible to meet the criteria for full disclosure outlined in *Englander*. Thus, based on this interpretation of the present law of consent under *PIPEDA*, RFID tags would be virtually barred post-sales and severely restricted pre-sales.

A "strict liability" standard will be applied to RFID readers (whomever they may be) for RFID violations. Strict liability is legal shorthand for responsibility for the results of one's actions, whether there was any carelessness or not. RFID retailers who do not disable tags can be viewed as strictly liable for putting out a product that can be used as a promiscuous tracking device. The rationale being that that when it comes to protecting privacy, and specifically the consent principle, the release of live RFID tags is akin to the release of a dangerous

---

[110] This report assumes that RFID readers will 'collect' personal information when the tags' information is scanned and stored, even absent. It has been pointed out that the Federal Court Trial Division in the case of *Eastmond* v. *Canadian Pacific Railway*, [2004] FC 852 ('Eastmond") appears to have established the principle that an electronic recording of information is not a "collection" under *PIPEDA* until viewed by a human being. See I. Kerr, "If Left to Their Own Devices … How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy", note 104, pp. 194 (online: http://idtrail.org/files/Kerr%20-%20If%20Left%20to%20Their%20Own%20Devices....pdf):

> "Consider, for example, the video camera surveillance system used in *Eastmond* v. *CPR*, [2004] F.C.J. No. 1043. CPR used video cameras to record activities in its Toronto yard, keeping the recordings in a locked area in order to ensure that they were never viewed by anyone unless an incident took place in the yard. If no incidents were reported, the recordings were automatically destroyed within 96 hours. According to the court, no "collection" of personal information occurred until such time as an incident was reported and the videotape viewed. In other words, automated systems that do not involve human observers are not collecting information and therefore not in violation of *PIPEDA*. This decision, if upheld, could have significant ramifications for DRM [digital rights management], since its automation usually does not require human intervention."

However, this principle appears absurd in the context of RFID, where the readers are by their nature collecting vast quantities of information, which is then transferred to a "back office" application for processing into intelligible data streams. However, to deny that the RFID reader was "collecting" information would mean that unless a consumer could show that a human had interacted with the RFID information that there never could be any application of *PIPEDA* to RFID use. This appears to fly in the face of reality, for if a system were developed that was utterly automated, but that still tracked individual users via RFID purchases and then provided in-aisle 'suggestions' of 'companion products' to the consumer in realtime it would be easy to imagine embarrassing privacy violations. This is the point also made by Kerr – "This decision [*Eastmond*], if upheld, could have significant ramifications for DRM, since its automation usually does not require human intervention."

substance. One view of fully "informed consent" would be a requirement that such a 'dangerous' situation required revelation that the tag could be read by any external reader. Promiscuous tracking would require the highest informed consent standard. The standard according to *Englander*, informed consent, in medical contexts, for example, requires identification of dangers or "risks" posed by the treatment.[111] In this case (live post-sales RFID tags) it could also mean identifying the risks to which such a technology exposes customers (i.e., tracking by others – retailers, criminals, police/security services).[112]

Note that even "in-store" or "on site" tracking (such as in a mall) may require a more obvious display of the terms *to the individual* than a simple sign at the door. This "is a notice board enough?" question has not been thoroughly examined by the OPCC. However, it seems to be assumed by some privacy commentators that it is sufficient to post a notice stating there is video surveillance in order to warrant conducting video surveillance of customers in-store. However, a basic question to answer should be: Should *PIPEDA* allow in-store tracking of persons by camera or RFID *at all*? That is, should it be possible to consent such activity by glancing at a general message that video surveillance (or RFID tracking) is being employed? This type of 'consent' approaches that of 'deemed' consent, since it is unlikely that many customers will read or pay attention to such signs. At best, it is a form of implied consent that is "informed" by the notice. At worst, it cannot be considered consent at all. This type of consent based on a cursory notice board that may not even identify risks of RFID surveillance, or the various uses to which data collected will be put, and which may not even be read by consumers, places too little importance on the surveillance aspect of the activity.[113]

Other researchers have raised the spectre of RFID as a surveillance technology. Dr. Teresa Scassa concludes:

> RFID technology raises privacy concerns in terms of the information gathered. If their full tracking and monitoring capabilities materialize, RFIDs will constitute a form of surveillance. […] It is as if we might be constantly shadowed by an increasingly comprehensive 'data body' that does more than follow us. It can also precede us: before we arrive somewhere, we have already been measured and classified. Thus, upon arrival, we are treated according to whatever criteria has been connected to the profile that represents us. […] Regardless of the nature and quality of the information obtained, this is surveillance: systems are used to

---

111 *Reibl* v. *Hughes*, [1980] 2 S.C.R. 880.

112 Note here also *PIPEDA* principle 4.3.3 "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes."

113 It is worth noting that the *Englander* 'informed consent' requirement for consent under *PIPEDA* necessarily telescopes *PIPEDA* Principle 2 'Identifying Purposes' with Principle 3 'Consent'.

> monitor people's actions or communications; and their ability to define, determine and control the parameters of their space is diminished. In this way, the privacy interest individuals have in sustaining personal or physical space free from intrusion is potentially compromised. [114]

It is interesting to apply the "4 point test" developed by OPCC Commissioner George Radwanski (one still endorsed by the OPCC and approved by the Federal Court) to both workplace surveillance and surveillance in a retail environment, whether by video surveillance or RFID tracking.[115] It appears that the surveillance made possible by either video cameras or RFID does differ from one another, but may also be equally privacy-intrusive, albeit in different ways.

The four-point test to assess and justify (video) surveillance under *PIPEDA* was developed by the OPCC in response to a complaint by a railway employee about video surveillance of the rail yard.[116] This test requires that for surveillance to be of sufficient importance to overcome the general principle against surveillance in any private place:

1. Is the camera demonstrably necessary to meet a specific need?

2. Is it likely to be effective in meeting that need?

3. Is the loss of privacy proportional to the benefit gained?

4. Is there a less privacy-invasive way of achieving the same end?

Accepting for the moment that RFID tracking is analogous to video surveillance, is the situation of a shopper in a retail store all that different from that of an employee? If anything, a shopper should have more freedom from surveillance, even within a private store, than an employee, since the shopper owes the storekeeper no duties (besides those not to trespass or shoplift) as does the employee.

It is therefore instructive to note that the OPCC has generally found against constant video surveillance for employee monitoring purposes. Generally, the four-part test will not be satisfied in this circumstance. For example, in a 2005

---

114 Scassa, *supra* note 12 at p. 47.

115 Note that public video surveillance is not permitted under *PIPEDA* except for very serious public safety applications (see *PIPEDA* Finding #1) or narrow workplace uses (*Canadian Pacific* v. *Eastmond*). The more RFID is considered, therefore, to be acting like (or is being used together with) video surveillance, the more likely is should be to fail to pass muster under *PIPEDA* too. This is discussed further below.

116 *Eastmond* v. *Canadian Pacific Railway*, [2004] FC 852 ["***Eastmond***"].

OPCC Finding ("Finding 290"),[117] the Assistant Commissioner applied the factors listed above. It was noted that a *specific* need must be met, and that a general wish to "monitor" was insufficient. In that case, the cameras were not powerful enough to monitor the actual meat cutting, and as such were not "demonstrably necessary" to meet the stated need of "food hygiene".

In the case of RFID tracking from readers in-store, the stated purpose, or "specific need", then would therefore have to be "tracking shoppers". It could also possibly be "inventory control" if a smart shelf were deployed with an RFID reader. However, there is no "inventory" purpose in tracking the progress of items through the store, provided it is eventually purchased at the register, except if that tracking is a form of consumer surveillance. Only cash-register RFID readers would need to be deployed for the more basic purpose of "identifying items at check-out". However, retailers appear to be contemplating placing readers throughout the store.[118]

Finding 290 went on to consider if the video surveillance were 'likely to be effective' in meeting the stated need. Since the cameras were not sufficiently powerful to actually capture any 'wrongdoing', and since there were actually inspectors working on the meat-cutting floor, the OPCC found this ground had not been met.

With respect to RFID readers in-store, it would appear they could be very effective at checkout for their stated purpose (i.e. their bar code, identification, function) and also inventory control. However, retailers would be unable to claim that RFID chips were "effective", if readers were deployed throughout the store, unless they admitted that the readers were being used for customer surveillance. Retailers would then be required to explain the end to which this surveillance was being used. For instance, consumer surveillance could be useful for tracking patterns of customer flow, or for targeted advertising in-store.[119] Additionally, RFID tracking could also be used to detect and deter shoplifting. However, many shoppers would probably resent being suspected of shoplifting, and therefore monitored, by virtue of entering a store.

The next factor to consider under the OPCC's test is whether "the loss of privacy [is] proportional to the benefit gained". This factor is difficult to evaluate due to the dearth of surveys examining consumers in retail environments where RFID has been fully implemented. However, one preliminary survey completed in 2003 supports the contention that consumers find in-store RFID tracking more privacy-invasive than useful. The Cap Gemini-Ernst & Young Internet-based

---

117 *PIPEDA* Case Summary #290, "Video surveillance cameras at food processing plant questioned", January 27, 2005, [***Finding 290***] online: http://www.privcom.gc.ca/cf-dc/2005/290_050127_e.asp.

118 See E. Murphy, "Tracking Grocery Hot Spots", *supra* note 2, 78.

119 Note that while the first example of consumer surveillance would not necessarily identify individual shoppers, while the second example of targeted advertising in-store would identify individual consumers.

study: *RFID and Consumers: Understanding Their Mindset*, was performed in October 2003 in the U.S. on 1000 adults.[120]

> According to the survey results, the RFID-enabled benefits that consumers value are not necessarily the same ones currently determining RFID deployment by retailers and CPG manufacturers. Although some retailers such as Metro Group have used trial deployments of RFID as a way to help merchants combine individual consumer identification and purchasing history with RFID-prompted selections and sales suggestions, consumers are wary of such developments. The survey found that the benefits of RFID least important to consumers were increased access to more products, instant recognition of preferences that can lead to faster/better service, and instant in-aisle suggestions for companion products.
>
> The survey also asked consumers about their apprehensions related to RFID. From a list of issues that had the potential to make respondents feel "extremely concerned," the three most frequently chosen were (1) the use of consumer data by a third party, (2) an increase in targeted direct marketing and (3) the potential for tracking consumers via their product purchases.
>
> [. . .]
>
> Consumer support for RFID mostly involves security and safety. The survey found that the top two benefits most important to respondents were the potential for faster recovery of stolen items (rated as "extremely important" by 71 percent of respondents) and improved car anti-theft capabilities (70 percent of respondents). In third place was savings stemming from reduced product costs (rated as "extremely important" by 66 percent). Improved security (such as protection from tampering or counterfeiting) of prescription drugs came in fourth (65 percent), and faster, more reliable product recalls ranked as the fifth (62 percent).

It is therefore conceivable that in Canada, both at present and in the future, even with retailer confidence that consumers will be pleased with targeted advertisements in-store, product suggestions in-aisle and so on, that consumers will instead regard in-store tracking as privacy-invasive to the point of

---

120 See Jonathan Collins, "Consumers Voice Opinion on RFID", RFID Journal, February 2, 2004, online: http://www.rfidjournal.com/article/articleview/780/1/1/. The original survey is available from the pollster at http://www.us.capgemini.com with e-mail registration. See also the survey by Cap Gemini "RFID and Consumers: What European Consumers Think About Radio Frequency Identification and the Implications for Business" also available from the pollster with e-mail registration.

outweighing any useful product suggestions or other stated conveniences.[121] It is also possible, based on these rough results, that many consumers will find that privacy should trump continued expansion of RFID use out of the store (e.g. for warranty service or recalls) if RFID chips used can be read by other retailers, the police, or another third party. More surveys of consumer attitudes should be done before retailers solidify assumptions.

The last factor in the OPCC test is: "Is there a less privacy-invasive way of achieving the same end?" If this question is applied to in-store tracking for inventory purposes, the answer would appear to be yes, there is a less privacy-invasive way of controlling inventory in-store. The old barcode scanning system, and any other manual system of tagging items and taking inventory, remains effective. Similarly, an RFID system without readers throughout the store, and one that killed tags at checkout could also be effective in controlling inventory. The question at this point is whether barcodes, or such a "plain vanilla" RFID system, are so inferior that it is not a fair comparison to state they are an alternative to RFID chips. Yet, experience shows that retailers have survived with barcodes for inventory control and in-store re-stocking until now. What RFID promises is lower cost for inventory control to retailers. Yet, if this is indeed the case, retailers should under this test provide a clear breakdown of the cost savings and a rationale for why the 'last mile' from the shelf to the cash register must be monitored by RFID chips.

If this question is instead asked of tracking in-store for promotions and monitoring consumer purchasing habits in real-time, the answer would appear to be no; there is no less privacy-invasive way of 'serving customer needs'. However, this negative response would not militate for the use of the technology; it would only confirm that the plan was unprecedented. The only close substitute is a scheme where every shopper is constantly monitored via video surveillance, which is an overly intrusive privacy violation.[122]

In sum, retailers seeking true consent required by *PIPEDA* from consumers to permit in, and out-of-store RFID 'tracking' face many challenges. First, they must

---

[121] See Cap Gemini survey on European Consumers, *supra*. This survey appears to demonstrate the relative lack of importance of in-store preference and tailored advertising (see chart p. 8 noting low levels of importance of 'increased access to more products', 'instant recognition of preferences' and 'in aisle companion product suggestions' as compared to high consumer concerns (see chart p. 11) with 'tracking of consumers via product purchases'; 'targeted more with direct marketing' and 'consumer data used by third party'.

[122] See "Total Surveillance' *supra* note 50, 52, where Katherine Albrecht suggests that the surveillance of shoppers is widespread and a large industry, into which RFID will naturally fit easily:

> There are things that have been going on long before RFID became available to retailers that are quite revolting. They've got shelf cameras that can zoom in and capture your customer expression as you look at a shelf. They've got fake shoppers who can literally follow you around and record what you say to the people you're shopping with. It's a $10 billion per year industry. And it's almost entirely invisible to the average consumer.

inform consumers in advance of collecting data, and provide details of how the data will be collected and the uses to which information collected will be used. Retailers will have to strive for informed consent. Second, retailers may, as a result of acquiring informed consent, be obliged to warn consumers that the tags may be read by third parties once the consumer leaves the store. Finally, it seems that in-store, and by extension out-of-store, tracking will be foiled by the principle against surveillance as expressed by the OPCC under the four-part surveillance test - despite efforts to obtain wide consent.

Limiting Collection

The principle of "limiting collection" under *PIPEDA*, like the justification for the "surveillance" aspect of RFID technology under the OPCC 4-part surveillance test, is dependent upon the stated or eventual use of the personal information collected. Principle 4.4 of *PIPEDA* states:

> The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Therefore, as noted above, if the retailer claims that the purpose of the collection is only inventory control, then collection of information "in-aisle" would be excessive and in violation of principle 4.4. If the retailer admits instead to collection for customer profiling, or shoplifting control, then the retailer would have to detail the extent of the profiling or suspicion of stealing. Under principle 4.9 (Individual Access) shoppers therefore should be able to see a copy of this profile. Retailers may be reluctant to pursue such profiling if they must reveal these purposes and make these records available.

However, by far the largest challenge faced by retailers using the present RFID tag technology would be the collection of personal information that their RFID tags would permit for other retailers, law enforcement or third parties. It is not clear from the wording of *PIPEDA* principle 4.4 that the original retailer is responsible for third party collection.[123] However, on the theory of strict liability for releasing a dangerous substance outlined above (that is, a live, unencrypted RFID tag) such an obligation would be reasonable. It would be burdensome to the consumer to protect all his or her purchases from readers after leaving a

[123] However, Principle 4.4.1 of *PIPEDA* does state in part; "4.4.1Organizations shall not collect personal information indiscriminately". Further, in Principle 4.4.2, it is noted, collection should not be performed by misleading the consumers and that "consent with respect to collection must not be obtained through deception". Not revealing that third parties may also read the personal information (i.e. RFID tags) may be misleading, and third party collection without any notice, and therefore without any consent, would seem by it's nature to be deceitful in the sense intended by this paragraph.

store. In contrast, a retailer could easily "kill" a tag at checkout. This theory assumes that if the retailer planted the device to permit automatic collection of a certain type of personal information for its own purposes, that it has a duty to ensure that the device is used only to further those stated purposes. By definition, a third party's collection of the information would not be serving the original retailer's purposes. The 'limiting collection' principle therefore also argues in favour of retailers killing or encrypting RFID tags at point of sale.

Limiting Use and Disclosure

The final major principle of *PIPEDA* that would be possibly compromised through RFID use is that of "Limiting Use and Disclosure" (Principle 4.5). This principle is somewhat circular in that it only requires personal information to be used or disclosed for the purposes for which it was originally collected.[124] Therefore, there could be no use or disclosure of information collected unless proper consent had been acquired in the first place. Assuming, however, that the retailer has obtained consent for limited use, such as inventory control, or has persevered and obtained full consent to a profiling-type RFID system, the retailer would still encounter problems limiting use and disclosure. First, and most obviously, unless the tag were deactivated or reasonably well encrypted, there would be the risk of inadvertent disclosure to third parties and consequences arising from their use of that information. Again, the responsibility for ensuring that third parties do not read live, unencrypted tags, would appear to more reasonably fall upon retailers than consumers. This argument gains some additional force in environments like shopping malls where retailers congregate, and where it is reasonable to expect consumers to frequent many retail establishments.

However, the larger problem with RFID and the "limiting use and disclosure" principle is profiling by the original (and possibly affiliated or even third party) retailer. There will be an irresistible pressure to link RFID information to loyalty cards or other forms of personal information to permit profiling. This indeed was exactly the system that was created when METRO 'Payback" loyalty cards were fitted surreptitiously with RFID chips in Germany.[125]

It is very likely however, that retailers will be tempted ***not*** to provide this level of detail about use or disclosure, or will provide completely inadequate disclosure. This assumption is based on the experience of the METRO store, where even

---

[124] Principle 4.5 reads:

> Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

[125] See "A Real Retail Scandal", above, pp.17.

the possibility of linking loyalty card information with RFID information right on the card was hidden from consumers. If retailers take the view that they are not responsible for third parties reading RFID tags that leave their premises, then they will not bother to disclose that risk to consumers. Again, disclosure of this risk should be mandatory, as should disclosure of all the possible uses to which that information may be applied.

Safeguards

PIPEDA is based on a standard prepared by the Canadian Standards Association, and as such is written in generalist language that avoids specific requirements. One area where this non-legal drafting approach appears inadequate is with regard to Schedule 1, art. 4.7 of *PIPEDA*. This provision only requires those handling personal information to implement security measures "appropriate to the sensitivity of the information".[126] This weakness is particularly noticeable with regard to RFIDs.

This report has argued that the risk of 3rd party reading, and the burden of preventing such activity, should not fall on the consumer. The only remedy, it appears, is killing tags, or using a secure method for reading tags such that only the original retailer, with the consumer's consent, can read the tags. The obvious candidate for such security measures is encryption of tags. Nothing else will satisfy privacy law in this context, nor will it be fair/safe for consumers.

However, it appears that retailers are not demanding and more importantly manufacturers are not implementing encryption of tags. The EPCGlobal Inc. conglomerate, that is setting U.S. and international RFID standards, has undertaken work on encryption which have not yet been implemented as a retail-level RFID encryption standards.[127] Interestingly, the 'kill switch' protocol has been in the EPC standard for some time.

---

[126] Principle 4.7.3 of *PIPEDA* categorizes the possible steps that should be taken to secure personal information:

> (a) physical measures, for example, locked filing cabinets and restricted access to offices;
> (b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
> (c) technological measures, **for example, the use of passwords and encryption**. [emphasis added.]

[127] This is the "EPCglobal UHF Generation 2" standard. See online: "Fact Sheet" http://www.epcglobalinc.org/news/FINAL_Gen2_Ratification_Fact_Sheet.doc which notes that this generation of the standard for retail RFID will "better protect data stored on the tags and corresponding databases, products built to the UHF Generation 2 standard will feature, among other improvements, advanced encryption technology, password protection and authentication.". However, a different document, the "Implementation Notes; How EPCglobal Works – EPCglobal Action & Working Groups" online; http://www.epcglobalus.org/SubscriberResources/IN_3_ActionGroups_072205.pdf notes only that

Yet, the idea that encryption protects consumers from unintentional disclosures to third parties would seem a simple solution to the problem and a specific requirement to meet the general safeguards requirements of *PIPEDA*.[128] A bill recently introduced in California requires contactless card systems, but also RFID on, or that links to an "identification document",[129] to meet the following requirements:[130]

> The document's RFID tag must not transmit anything other than a unique ID number. **Encryption must be used to protect the data on the RFID chip from unauthorized reading**. The reader and document's chip must use mutual authentication. The ID holder must authorize the reading of the ID's data and be notified in writing that the ID uses RF to transmit information, and that he or she can use a shield to prevent the data from being transmitted through RF. In addition, the ID holder must be informed of the locations of all devices intended for use in reading the ID.

The point made by the proposed bill is that any unencrypted transmission for the RFID tag exposes the bearer of the tag to identification by anyone with a reader. This is precisely the linkage that *PIPEDA* is attempting to protect with its safeguards "proportionality" principle. A seemingly innocuous device like an RFID can effectively broadcast personal information whose sensitivity is determined by the context or the item being purchased.[131] This risk is virtually impossible for the original retailer to gauge, so the only method to ensure a live tag would not transmit sensitive information or information that was sensitive given the context, would be to encrypt the data.

---

the 'Hardware Action Group' is studying whether the additional Class 2 features "may include encryption". At present there is no encryption in the EPCGlobal standard for RFID devices.

[128] As noted, Principle 4.7.3 of *PIPEDA* suggests that encryption is an effective technological protection measure.

[129] See Senate Bill 682, Introduced by Senator Simitian, February 22, 2005: "An act to add Article 4 (commencing with Section 1798.9) to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, relating to privacy" [***SB 682***]. Latest amended version: http://info.sen.ca.gov/pub/bill/sen/sb_0651-0700/sb_682_bill_20050815_amended_asm.pdf.

[130] See description of Bill SB 682 in Mary Catherine O'Connor, "Calif. Bill Allows RFID in More IDs" RFID Journal, online: http://www.rfidjournal.com/article/articleprint/1686/-1/1.

[131] Note that *PIPEDA* recognizes that information that might seem innocuous in one situation might be destructive of personal privacy in another. See *PIPEDA* Principle 4.7.2 which reads;

> **The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage.** More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4. [emphasis added.]

PRIVACY MEASURES

Given the forgoing discussion of Canadian privacy law, it appears there are relatively few applications of RFID at the consumer (item) level that will pass muster. In fact, for any retail application, the primary purpose for which is simply logistics and inventory control, there appears to be no other answer than that tags must (a) not be read within store to track individuals and (b) must be killed (at the latest) at checkout. These restrictions are difficult to ensure without fairly bright line rules. These rules could be OPCC guidelines that clarify the interpretation of *PIPEDA* in relation to RFID, or they could form the basis of RFID-specific privacy legislation. We deal with the easiest first.

Killing Tags

Disabling or 'killing' RFID tags at the retail level is both possible, simple and effective in reducing or eliminating privacy violations and associated risks such as surreptitious surveillance by third parties. The EPC standard specifies an 8-bit header that can be reset to disable the tag. Generally, the tag is magnetic and the object is "swiped" in proximity to a de-magnetizer.[132]

Retailers may object that killing tags involves extra time and expense. However, stores already use magnetic tags to combat shoplifting, and are already in the habit of routinely disarming these at point of sale. This does not seem to place a major burden on those retailers. By extension, killing RFID tags should not, therefore, place an additional strain on retailers who are already in the practice of disarming magnetic and similar tags. Killing tags should be routine procedure at checkout and only an explicit consent, based on full information about uses and disclosures, should suffice to allow the tag to live past the point of sale.

Retailers wishing to use RFID for returns, warranties or extended functionality will have to clearly explain the rationale for a 'live' tag to a consumer. Under the informed consent standard, it also appears retailers should both inform consumers of the risk of third-party RFID reading and possibly even bear the losses associated with that risk (on a strict liability theory). Alternatively, consumers should be offered an alternate method of returning products or obtaining warranty service, should they refuse to take the risk of leaving with a live tag.

---

[132] A kill code of 8, 24, or 32 bits, unique to the RFID tag, would require the "killer" to have access to a secure database to transmit the proper "kill" key. Reactivation of RFID tags would also require access to the database, 'the key', and should be impossible without such access or information. Note that some systems allow tags to be accidentally or purposely reactivated. If such reactivation were to be a real risk, the original retailer should not be considered to have actually "killed' the tag.

Some retailers have offered the idea of tag "blockers" as an alternative to killing tags that they wish to have active after sale. One such blocker has been developed by RSA Laboratories.[133] These could be embedded in a shopping bag, purse, wallet, or watch that is carried or worn near live tags with information that consumers want blocked. These blocker tags would "jam" any readers trying to read the consumer's live tags.[134] Jamming is said to be selective, and very short range so as not to jam tags that other consumers want active, affecting only readers without the proper authorization. Thus, they can prevent unwanted scanning of purchased items, without affecting the scanning of shop inventories. Consumers also have the choice of turning their blocking tag off, if RFID monitoring is desired.

The Electronic Frontier Foundation (EFF) is quite critical of tag "busters" or blocker tags.[135] EFF argues: (1) blocker tags could encourage the proliferation of RFID by giving consumers a false sense of security; (2) blocker tags could be banned by governments, for reasons of national security; (3) blocker tags could be banned by stores if they might circumvent security measures or hinder the collection of marketing data (4) busy consumers might forget to carry their blocker tags; (5) blocker tags don't protect items once they are separated from the blocker tags; (6) reliance on blocker tags shifts the burden of protecting privacy from the retailer to the customer.

However, none of these concerns will be present if the simple step of killing tags effectively is required by *PIPEDA* guidelines or specific legislation (and provided there is fining power and adequate enforcement by the OPCC or a similar body).

---

[133] RSA Laboratories, "Protecting Consumer Privacy" (2004), online: http://www.rsasecurity.com/rsalabs/node.asp?id=2119.

[134] The Blocker Tag manipulates the reading protocol to make the reader think that RFID tags representing all possible identifier numbers are present, thereby 'confusing', the reader.

[135] See EFF, "Position Statement on the Use of RFID on Consumer Products" (November 14, 2003), Attachment 2, online: http://www.eff.org/Privacy/Surveillance/RFID/rfid_position_statement.php.

Encryption

The 'live tag past checkout' problem could be solved by communications between tags and readers being encrypted. Depending on the level of encryption employed, this will block eavesdropping by third parties.[136] In a retail environment, such eavesdropping could potentially collect data for marketing purposes or, in extreme cases, for misrepresenting oneself as the rightful owner of a purchased object. However, given the emphasis on low cost for tags used in the retail environment, encryption will likely be low grade, or perhaps non-existent.[137]

However, *PIPEDA*'s security principle, as well as good business sense, dictates that, once collected, consumer information should be protected from hackers and other abuses.[138] The amount of information collected and stored on tags should therefore be the strict minimum necessary to perform the function, and the data should be deleted as soon as possible, given the objectives. However, for RFID tags, this level is not enough; encryption of the tag information is required to avoid third-party eavesdropping on the chips and potential data-matching with (for example) other retailers' customer profiles.[139] This would be easily achieved through encryption.

The international standards setting body, the ISO, and EPCglobal Inc., though stating that encryption can form part of the next standard, are not making it mandatory. The simple reason is cost – encrypted tags cost (at present) more than the retail industry is willing to spend on security. Nonetheless, the encryption of RFID information would appear to solve the third-party access problem that *PIPEDA* clearly would not permit.

---

[136] To prevent eavesdropping by unauthorized third parties, some higher-end tags use access control mechanisms. The reader must furnish a proper code before the tag will transmit any information. But, this mechanism is unlikely to be used by the low-cost tags common in retail.

[137] Applications involving tracking location, identifying people, and especially completing transactions, pose a much greater threat of third-party interception, including mimicking fraudulent transactions and outright identity theft. Here, encryption will be much more sophisticated and more difficult to "crack". RFID tags are more likely to be active, rather than passive, with more memory and significant processing power.

[138] Several relevant OPCC findings involve the adequacy of password systems. See for example, the contrasting results in OPCC Finding #5 and OPCC finding #315 where the difference in the outcomes appears to turn on the user's control over the password system. In an RFID system, short of employing a "tag buster" or wrapping all purchases in tinfoil, a consumer would have little control over the system and therefore should have little or no obligation to compensate for security risks in the system.

[139] Another way to achieve a similar result is through "mutual authentication". Access to tags can be controlled through software. A reader would have to present an authorization code that the tag would validate before transmitting any information. Such an approach would require some processing by the tag, but notably, less processing than encryption would require. Theoretically, if the consumer had control of the tag's access code, he or she could selectively choose the category of readers that will be permitted to read the tag. However, consumers likely would not take the time to so tune their RFID chip communications.

Prohibition on Linking RFID Info with Loyalty Card Info

In-store tracking is not affected by killing tags or encryption. How then will retailers who do not obtain full, informed consent to track in store be constrained in accordance with *PIPEDA* from tracking individual shoppers rather than simply aggregating anonymous shopper information? One course could be to forbid in-store RFID readers placed between the shelves and the cash register. However, such a solution would not permit 'smart shelves' (as these shelves could report on customer movement with other objects) to assist a retailer in replenishing and tracking inventory.

The only practical way to enforce the restriction on in-store tracking without consent is to make RFID information anonymous. This can only be done, legally, in forbidding the association of any RFID information in-store with a particular individual. For the most part, this prohibition will mean forbidding the retailer from associating their loyalty card or similar consumer profile database with any information from the RFID database gathered from the sales floor.

Contrary to the view that such a system would not stop retailers from associating RFID with shoppers, it in fact could be highly effective, provided the prohibition stipulated fines per occurrence (which could be levied by either a beefed up OPCC or perhaps by a municipal by-law officer) and consumers were provided a statutory right of action under *PIPEDA*, with statutory damages set high enough per occurrence to dissuade flouting of the law. Businesses generally respect a specific law that forbids a course of action and provides for penalties and risks a major class proceeding.

Only retailers that claimed to have a complete system for obtaining prior, informed consent to full consumer tracking via RFID in store would have a "due diligence" defense to an action or fine under this new law.

Other Safeguards (U.S. Proposals)

It is interesting to contrast these proposed safeguards with those developed in a jurisdiction without a comprehensive private-sector privacy law. In the U.S., several organizations have suggested a set of such limitations. The Electronic Privacy Information Center (EPIC) provides a good example.[140] The salient points of EPIC's guidelines are summarized as follows:

1. **Notice:** The most important measure is notice of the presence of RFID tags.[141] The notice should be reasonably conspicuous, and should identify the type of information that will be collected via the tag, and the uses to which that data will be put. Furthermore, notice should also be given of the presence of readers, as well as reader activity, whether through a tone, a light, or other readily observable signal whenever the reader is interacting with a tag.

2. **Removal:** In a retail environment, customers should have the right to have RFID tags removed or deactivated upon purchase. Customers may choose to maintain live tags so as to benefit from various post-sales functionalities. However, unless those functionalities are an essential part of the product, the customer's consent must be obtained before the tag is allowed to remain live beyond the point of sale.[142] Furthermore, a live tag must be easily removable by the customer later if they decide no longer to have a live tag.[143]

3. **Anonymity Priority:** To the greatest degree possible, RFID systems should avoid or minimize the collection of personal information (as opposed to the product information). This should be routine in a retail environment. RFID systems should not be employed to collect or use information outside of the publicly stated objectives. In particular, it should not be used to track customers to obtain individual shopping habits or to build any other personal profiles. When personal information is collected, the consumer's informed consent should be obtained beforehand, and

---

[140] Electronic Privacy Information Center, "Guidelines on Commercial Uses of RFID Technology", July 9, 2004, online: http://www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf.

[141] This could be extended to all objects with which the customer comes into contact, whether ultimately purchased or not.

[142] Deactivating tags should not be an undue burden on retailers. Security tags are in widespread use today, and their deactivation is a routine activity.

[143] CASPIAN, *supra* note 42, has also been critical of killing tags at point of sale as a solution to the privacy issues raised by RFID. They claim: (1) killing tags after purchase doesn't address in-store tracking of consumers; (2) tags can appear to be killed when they are really "asleep" or dormant and can be reactivated; (3) the tag killing option could be halted by government directive, so as to create a "surveillance society"; (4) retailers might offer incentives or disincentives to consumers to leave tags active, e.g. loss of discounts, long wait for deactivation.

data uses restricted to those consented to.[144] In any case, individuals should not be coerced or forced to keep tags live after purchase, if they choose not to.

4. **Security:** There should be no disclosure of personal information to third parties without the consent of the person involved. Measures should be taken to keep such data secure, whether contained in large databases or in any other form. Essentially, data should be confined within a "closed system", accessible only to those within the system or acting pursuant to a court order.[145]

5. **Openness:** Persons whose personal information has been collected via RFID systems should have the right to access this data, and the opportunity to make any corrections.

6. **Accountability:** Users of RFID systems should make public, and readily available to interested individuals, specific information about their policies and practices relating to handling of personal information. They should also designate someone who is accountable for compliance with these policies and practices.

Such general principles governing privacy issues are useful. However, the mapping of these guidelines to *PIPEDA* requirements is the necessary first step. At best, these suggestions can only inform the Canadian retailers' actions in meeting the necessary burdens required by *PIPEDA*, notably the requirement of informed consent to surveillance via RFID, whether in-store or later.

---

[144] Obtaining individual consent is likely to add significantly to retailers' costs, and fierce resistance can be expected. An important issue will be clearly defining the standard that will qualify as adequate notice.

[145] CASPIAN is critical of this proposal as well. They claim that (1) one of the reasons closed systems remain closed today is that coding schemes vary across systems; with the standardization of product level tagging, there will be more incentive to share (2) closed systems lack transparency and make it difficult for consumers to assess privacy risks and protect themselves. See CASPIAN, *supra* note 42.

CONSUMERS' PERCEPTIONS OF RFID TECHNOLOGY

It is interesting to compare the above analysis of the requirements of Canadian privacy law with the privacy concerns enunciated by consumers themselves about RFID. Although no large-scale surveys of Canadian attitudes to RFID presently exist, work has been done on the issue in the U.S. and Europe. Capgemini, a business consultant, has conducted several surveys focusing on the issue of RFID and Consumers.[146]

The first notable result of their 2005 survey, "RFID and Consumers" is that awareness of RFID technology is low among both American and European consumers: 23% of U.S. consumers, and 18% of European consumers had heard of RFID technology.[147]

The second significant finding, however, was that privacy was the most relevant and pressing concern among consumers in all countries surveyed, with between 60% and 70% of consumers in each country stating they were "concerned or extremely concerned' with RFID. Health and environmental issues also raised alarm.[148]

Further, most (between 66% and 76%) of consumers in these countries thought RFID would have the same or more impact on their privacy than: mobile phones, debit cards, credit cards, ATMs, frequent shopper/loyalty cards, access-control badges, smart cards and camera phones – all technologies in which consumers are now well-versed.[149] Similarly, a survey conducted by Artafact LLC and BIGresearch,[150] indicates that 63% of RFID aware consumers are concerned about invasion of privacy. The study conducted by BIGresearch/Artafact

---

[146] The European survey, done in November 2004, involved more than 2,000 consumers in the U.K., France, Germany and the Netherlands using an Internet panel. Consumers were asked to complete a questionnaire that included a brief explanation of RFID and a wide range of questions about the technology. The European research is a follow-up to a similar study conducted in October of 2003 in the U.S., in which more than 1,000 consumers were surveyed. Capgemini, "RFID and Consumers", February 2005, Online: http://www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf [***Capgemini European Study***]. The Capgemini study of US consumers, "RFID and Consumers: Understanding Their Mindset", is also available online: http://www.nrf.com/download/NewRFID_NRF.pdf.

[147] The latest wave of RFID Buzz Reseach, conducted by BIGresearch /Artafact, indicates that consumers are much savvier about RFID now than they were a year ago. In September of 2005, more than two out of every five adults (42.4%) claim to have heard of RFID technology. Awareness grew most dramatically late in 2004 and early in 2005, with awareness levels peaking in June of 2005 (43.6%). BIGresearch Press Release, "Consumer Awareness of RFID Technology Now Stands at 42.4%, Up Dramatically From 28.2% Just One Year Ago", November 15, online: www.bigresearch.com/news/big111505.htm.

[148] Capgemini European Study, *supra* note 137, at pp. 11.

[149] Between one-third and almost half of European respondents expect the impact of RFID to be greater than these other technologies. *Ibid*. at pp. 12.

[150] BIGresearch Press Release, "Who's Afraid of the Big Bad Wolf?", October 26, 2004, online: www.bigresearch.com/news/big102604.htm.

surveyed over 8,000 U.S. consumers also reveals that only 35% of respondents concerned about protecting their personal information believe that RFID is a "good idea", and are concerned with the potential for misuse, given the "lack of safeguards".[151]

Respondents were also asked directly how application of relevant privacy principles, such as: notice, record use, retention and security, and consumer choice, might influence their willingness to buy RFID-enabled products.[152] Both American and European consumers indicated that legislated privacy protection is the key feature that would make them more likely to buy such products, mentioned by 62% of Americans and 57% of Europeans. Further, the ability to disable tags at the time of purchase (58% of Americans and 53% of Europeans), clear labeling informing consumers that products bear RFID tags (53% of Americans and 51% of Europeans), and a customer choice as to what is done with the information collected via RFID tags (54% of Americans and 44% of Europeans), would also serve to quell privacy concerns among respondents.[153]

While one of the main purposes of introducing RFID into the retail environment is the reduction of cost, consumers disagreed that this would be the effect: 41% of Americans and 39% of Europeans thought that RFID would increase the cost of goods, 17% of Americans and 11% of Europeans thought it would lower the cost, while 18% of Americans and 24% of Europeans thought it would have no impact on costs.

When asked what benefits RFID might offer, the top of the list for European consumers was improved car anti-theft capabilities (70%), faster recovery of stolen items (69%), improved security of prescription drugs (63%), and improved food safety and quality (58%). As noted earlier in this paper, at the bottom of the list were reduced out-of-stocks (43%), increased access to more products (36%), instant recognition of preferences (28%), and in-aisle product suggestions (19%).[154]

Significantly, the leading consumer concern was access to consumer data by third parties, mentioned by 69% of Americans and 59% of Europeans. Almost as important was consumer tracking via product purchases, of concern to 65% of

---

[151] See also above note regarding consumers rating the claimed convenience factors of RFID in-store as significantly less important than privacy concerns around in-store tracking.

[152] Capgemini European Study at pp. 13.

[153] For a detailed consideration of consumer attitudes and comments regarding RFID and privacy, refer to "RFID Applications and Implications for Consumers", A Workshop Report from the Staff of the Federal Trade Commission, March 2005, at pp. 13-15, online: http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

[154] Note that the most popular consumer benefits require RFID tags to stay active after purchase. By contrast, those features that can be achieved with tags that are killed upon purchase are among the lowest ranked. This suggests consumers can be approached for proper consent to continued "live" tags, provided there are clear consumer benefits and provided adequate security measures (such as encryption) are in place.

Americans and 55% of Europeans; and being targeted more with direct marketing (67% of Americans, 52% of Europeans). Other concerns included the environmental impact of RFID systems (45% of Americans and 44% of Europeans), health issues stemming from RFID (56% of Americans and 35% of Europeans) and RFID tags that can accidentally be ingested or those that might dissolve (43% of Americans and 31% of Europeans).

The Capgemini report recommends that consumers be included in the RFID discussion, because it is a 'game-changing', technology that has the potential to fundamentally alter the global supply chain and the store experience in the coming years".[155] They also recommend that greater consumer education be put at the top of the list of priorities for RFID manufacturers and retailers as it is argued that "debunking myths" and "communicating the potential benefits" of RFID is key to acceptance of the technology.

[155] Capgemini Eurpopean Study, *supra* note 137 at pp. 17.

CONCLUSIONS AND RECOMMENDATIONS

PIPEDA appears to require that retailers use RFID at the retail level only for inventory purposes. Further, consumers appear very uncomfortable with the retail surveillance and associated aspects of RFID. Therefore, from both a legal and policy perspective, any additional use of RFID that may identify an individual would make RFID data "personal information" and subject to consent and other requirements of *PIPEDA*.

As Dr. Scassa et. al. advance in their paper:[156]

> Guidelines for the appropriate use of RFIDs should be promulgated before the technology is widely used. Further, such guidelines may influence the development of the technology, in particular through technological configurations that support privacy initiatives.

Such guidelines or *PIPEDA* amendments should, at the least, include the following six requirements.

1. Informed Consent for RFID Surveillance

Where retailers wish to use RFID for consumer surveillance purposes in-store (usually by cross-referencing a customer loyalty card with RFID information) or where there is a risk that a 'live' RFID tag may be read by third parties post-sales, informed consent of the individual consumer for this use is required.

The specific criteria that will satisfy the informed consent standard for RFID in this context has not yet been established. However, it appears that a consumer will have to be fully informed of the fact of surveillance, how it works, where readers are located and whether RFID readers are integrated with video surveillance. Retailers must also state the purposes for which the information collected will be used, who will use it, and identify the circumstances under which this information may be shared or disclosed. Additionally, any data aggregation and cross-referencing of RFID information with a retailer's customer relationship management data (whether obtained from a loyalty card, credit card or otherwise) must be revealed. Customers also must be told of safeguards in place to protect this information. They must also be given the right to examine their personal record, contact the retailer and obtain, and if necessary correct, the information, as well as the right to withdraw their consent to the use of the information. It is also important that consumers have the right to challenge the retailer's dealings with this personal information as not being in accordance with

[156] Scassa, *supra* note 12 at pp.57.

PIPEDA. Importantly, such information must be provided to the consumer, and consent actually indicated, prior to the commencement of RFID surveillance.

The manner in which retailers intend to implement these ideas, and especially the manner in which retailers intend to secure consent may vary. As noted previously, it will be difficult to show true informed consent if the only effort the retailer has made is to post a notice near the entrance of the store, even if it details all of the requirements listed above. Ultimately, the consumer must provide positive consent to the surveillance. Retailers under this standard will assume the burden of demonstrating that the consumer was fully informed of RFID use. Thus, obtaining written or similar express consent may be the only real course of action to avoid privacy complaints.

Recommendation #1: *PIPEDA* be amended, or OPCC guidance issued, regarding the requirements of informed consent to RFID surveillance in-store and post-sales.

2. Killing RFID Tags for Routine Sales

Retailers who do not claim to track shoppers with RFID (that is, use it as a glorified barcode or potentially also as a generator of aggregated anonymous shopping flow data) will have to routinely kill tags at checkout, or face privacy complaints that they are: (a) in fact tracking individuals, either using in-store readers, or failing to kill tags and identifying customers on return trips to these retailers; and (b) risking the identification of the individual or release of his or her personal information to third parties.

Thus, Retailers who intend to track customers in-store via RFID must also routinely kill tags, unless the consent they obtain is informed by the revelation that they intend to leave tags live past check-out for tracking a customer's return.[157] The only other exception to routinely killing tags may be for warranty service, repairs or returns. However, in order to avoid coercing consumer consent for continued live tags, retailers must provide the option of such services with a simple receipt, or other non-RFID system.

[157] As noted above, if retailers do this they must also fully inform the customer, and obtain their consent, to taking a risk with third party disclosure. As noted, there is an arguable case that in such circumstances (risk of third party disclosure) that the original retailer may bear some portion of any resulting liability.

Recommendation #2: *PIPEDA* require, or OPCC guidelines state, that RFID tags should be routinely killed for all retailers who claim to use RFID for inventory purposes only, as well as for retailers using RFID for surveillance, unless the continued surveillance is explained. Tags also may be left live if the retailer obtains informed consent of the customer for such uses as warranties, repairs and returns, provided such consent is not coerced by making live RFID chips a requirement for warranties, repairs or returns.

3. Encryption

Third-party access to RFID tags is a gross privacy violation of consumers. Retailers should bear the responsibility, on a strict liability basis, for such "data leaks" as occur through unencrypted RFID tags. Encryption of any tags that are live post-sales should therefore be an absolute requirement for all retailers, even where the tag is intended to stay live for warranty, repair, return or recall purposes.

Recommendation #3: *PIPEDA* should be amended, or OPCC guidance issued, to require encryption of all 'live' tags post-sales.

4. Prohibition on Associating RFID with Consumer Profiles

Unless a retailer has sought and obtained informed consent to associate consumer profiles, for example gathered from loyalty card data, with RFID information, any association of RFID information with a pre-existing customer profile amounts to surveillance. Retailers must be made aware that such surreptitious surveillance is not permitted under *PIPEDA* without informed consent. As the temptation to combine such data sources will be overwhelming to retailers, it must be flatly prohibited unless informed consent is obtained. Retailers who violate this prohibition should be subject to specific fines and possible legal actions, brought by aggrieved consumers.

Recommendation #4: All association of RFID information with loyalty cards or other consumer profiling information should be prohibited, unless the retailer has sought and obtained informed consumer consent. This will require an amendment to *PIPEDA* that also provides the OPCC with fining power. In addition, a private right of action, with statutory damages per violation, should be created as a parallel enforcement mechanism.

5. U.S. RFID Recommendations

Other suggested recommendations such as warnings on items carrying RFID tags that they are 'chipped', or mandating the right to remove RFID chips are useful but secondary. Most of these recommendations, including those suggested by EPIC above, are simply manifestations of practices that retailers could or should be taking to adequately inform consumers about RFID to obtain the level of consent required for the proposed use.[158] It must be remembered that the United States does not have overarching privacy legislation. Thus, recommendations from this market may be more targeted to specific abuses than to a coherent philosophy of limiting RFID surveillance. These "trees" should not obfuscate the clear duties of Canadian retailers not to monitor their customers without consent.

In this regard, the Office of the Privacy Commissioner of Canada should be encouraged to pursue its stated goal of closely questioning the intentions of Canada's retailers with regard to RFID and should forge ahead quickly with guidelines and proposed amendments to clearly establish *PIPEDA* requirements for RFID.[159]

Recommendation #5: That the Office of the Privacy Commissioner of Canada immediately establish appropriate RFID specific guidelines for use that respects the requirements of the Personal Information Protection and Electronic Documents Act and encourage provincial privacy commissioners to do likewise. The OPCC should also propose RFID-specific amendments to *PIPEDA* and ensure it obtains the order making and fining power required to police *PIPEDA*.

6. Other Recommendations

Certain other recommendations, though not required by *PIPEDA*, could help reduce the risk of future privacy violations due to RFID by reducing practices that border on the retail environment or encroach upon the informed consent of the customer to appropriate RFID use.

---

[158] Numerous ideas could be suggested to alert consumers to the presence or functions of RFID such as having readers flash or beep when within range of a live tag but these may themselves create problems (such as screens set to display the identity of the carrier of a nearby tag that could be read by others).

[159] Note that *PIPEDA* is under Parliamentary review in 2006, so the time is ripe to suggest substantive amendments – indeed, the OPCC has already intimated it requires order-making power.

Recommendations #6:

a. **Tags used in the manufacturing process should normally be deactivated before the finished product is offered for sale to consumers. If tags on some parts are intended to stay alive post-purchase, e.g. for warranty purposes, the retailer should be made responsible for ensuring the customer's informed consent.**

b. **Governments encouraging use of RFID in the supply chain should require privacy impact assessments if those RFID tags will reach the retail level or are likely to increase RFID use at the retail level.**

c. **Even in a retail store where informed consent to consumer surveillance is obtained, the RFID identifiers of objects picked up but not ultimately purchased should never be linked to the personal information of a shopper.**

d. **If a retailer chooses to link RFID data to customer profiles, and that retailer acquires another retailer or a data aggregator,[160] the original retailer would have to notify its customers and seek consent to use the original RFID data, or customer profile, and the new RFID data or customer profile, before data-mining of this consolidated RFID and customer profile data.**

[160] See, for example, 'retail media networks' discussion above.

Conclusion

Radio Frequency Identification (RFID) technology holds modest promise for consumers of increased convenience and functionality but great risks of privacy loss. RFID's real value is to retailers. However, RFID offers retailers a Faustian choice: between sticking to improved logistics (looking at themselves) and constant consumer surveillance (looking at others). To the extent that *PIPEDA* and similar privacy law empowers consumers to demand retailers to look only inwards and not spy on them, they should ensure retailers are made to choose the right path. If not, consumers may well find they have shopped themselves into surveillance.

POSTLUDE

Since this paper was originally drafted, the Office of the Information and Privacy Commissioner of Ontario issued privacy guidelines focusing on RFID information systems.[161] These guidelines intend to serve as privacy "best practices" for organizations when designing and operating RFID information technologies, and were intended to apply to any organization that used RFID technology on consumer products involving or potentially linking to, personally identifiable information.[162]

Ten guidelines were issued addressing many of the topics covered in this paper. To summarize the guidelines issued: (1) accountability; (2) identifying purposes for collecting and linking personal information; (3) consent; (4) limiting collection; (5) limiting use, disclosure and retention of personal information; (6) accuracy of information retained; (7) safeguards to protect personal information appropriate to its sensitivity; (8) openness between consumers and those gathering information; (9) providing consumers with individual access to information retained; and (10) complaint mechanisms that provide consumers with means to challenge breaches to compliance of privacy standards. Additionally, the Office

---

[161] Ann Cavoukian, "Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)", Information and Privacy Commioner/Ontario, June 2006 [***RFID Guidelines***], online: http://www.ipc.on.ca/docs/rfidgdlines.pdf.

[162] Note the broad interpretation of the term 'personal information' intended by these guidelines.

> "Personal information" refers to any recorded information about an identifiable individual. IN addition to one's name, contact and biographical information, this could include information about individual preferences, transactional history, record of activities or travels, or any information derived from the above, such as a profile or score, and information about others that may be appended to an individual's file, such as about family, friends, colleagues, etc. In the context of item-level RFID tags, the linkage of any personally identifiable information with an RFID tag would render the linked data as personal information". *Ibid*, at pp.2.

of the Information and Privacy Commissioner of Ontario has also provided practical tips for businesses to implement these guidelines.[163]

Of particular relevance are the tips about providing notice of RFID use. While it is advised that collection, use and disclosure of RFID-linked personal information be confined to purposes that a 'reasonable person' would consider appropriate,[164] use of signs to inform consumers of RFID readers on the premises is also advised.[165] It is also recommended that organizations have a "clear policy for obtaining consent to collect, use and disclose RFID-linked personal information".[166] As noted above, using signs to warn consumers about RFID tracking does not address the pressing *PIPEDA* requirement of obtaining consent prior to the collection, or use, of personal information.[167] Thus, the inconsistency between these two practices has not been addressed by the guidelines or tips issued by the Information and Privacy Commissioner of Ontario. We encourage additional discussion and consideration of the above in order to prospectively limit privacy violations for the benefit of consumers.

---

163 Ann Cavoukian, "Practical Tips for Implementing RFID Privacy Guidelines", Office of Information and Privacy Commissioner/Ontario, [***RFID Tips***] online: http://www.ipc.on.ca/docs/rfidtips.pdf.

164 *Ibid*. at pp.1.

165 "Organizations should notify consumers of RFID readers on their premises, using clearly written signage, prominently displayed at the perimeters". Additionally, "Signs at the perimeter should identify someone who can answer questions about the RFID system, and include their contact information". *Ibid*. at pp.1-2.

166 *Ibid*. at pp.2.

167 See pp.36-38, above, for example.