Consumer Privacy and Radio Frequency Identification Technology

TERESA SCASSA, THEODORE CHIASSON, MICHAEL DETURBIDE AND ANNE UTECK*

Radio Frequency ID tags are poised to replace the UPC barcode as a mechanism for inventory control in the wholesale and retail contexts. Yet the tiny chips offer a range of potential uses that go beyond the bar code. In this paper the authors define RFID technology and its applications. They explore the privacy implications of this technology and consider recent attempts in the U.S. and European Union to grapple with the privacy issues raised by the deployment of RFIDs at the retail level. The authors then consider the extent to which Canada's *Personal Information Protection and Electronic Documents Act* ** will apply to RFID technology, before making recommendations for initiatives to proactively address the privacy issues that RFIDs will raise.

Les étiquettes d'identification par radiofréquence (IRF) sont sur le point de remplacer les codes à barres CUP en tant que moyen de contrôle de l'inventaire dans le contexte de la vente au détail et en gros. Déjà les petites puces offrent plus de possibilités d'utilisations que les codes à barres. Dans cet article, les auteurs définissent la technologie IRF et ses applications. Ils en explorent les répercussions sur le droit à la vie privée et examinent les efforts récents faits aux États-Unis et dans l'Union européenne afin de résoudre les problèmes de respect de la vie privée que soulève la mise en place de cette technologie dans le secteur de la vente au détail. Les auteurs étudient ensuite dans quelle mesure la *Loi sur la protection des renseignements personnels et les documents électroniques* *** du Canada s'appliquera à la technologie IRF, puis recommandent des mesures proactives afin de répondre aux questions de respect de la vie privée que soulève cette technologie.

---

* Teresa Scassa is Director of the Law and Technology Institute, and Professor at Dalhousie Law School. Theodore Chiasson is Assistant Professor at the Faculty of Computer Science, Dalhousie University. Michael Deturbide is Associate Professor and Associate Director of the Law and Technology Institute at Dalhousie Law School. Anne Uteck is an Associate of the Law and Technology Institute at Dalhousie Law School.
The research for this paper was generously funded by the Office of the Privacy Commissioner of Canada under their Contributions Program, 2004. We would like to thank research assistants Jennifer Hefler, Marie McNamee, Wen Liu, Donna Davis and Lindsay Bailey. Thanks also to Dr. Thomas Trappenberg of the Faculty of Computer Science of Dalhousie University and Fred Carter of the Office of the Information and Privacy Commissioner of Ontario. We are grateful to Lynda Corkum of the Law and Technology Institute for her administrative assistance with the project.

** S.C. 2000, c. 5 [PIPEDA].

*** L.C. 2000, c. 5 [LPRPDE].

Table of Contents

Consumer Privacy and Radio Frequency Identification Technology

TERESA SCASSA, THEODORE CHIASSON, MICHAEL DETURBIDE AND ANNE UTECK

I. INTRODUCTION

In the not too distant future, it is likely that most, if not all, consumer items will contain a tiny, possibly imperceptible chip. This chip, known as a Radio Frequency Identification (RFID) tag, is poised to replace the UPC barcode as a mechanism for inventory control. Yet the tiny chips offer all businesses in the supply chain, from manufacturer to retailer, with a range of potential uses that go beyond the bar code. RFID technology promises to provide each product item with a unique identifier that can be read from a distance. The data encoded on RFIDs can be matched with other information in databases to offer superior inventory control, the potential for tags to interact with store shelves or home appliances, and the potential for a new wave of consumer data-matching activities.

In this paper we begin by defining the technology and defining its applications. We then explore the privacy implications of this technology and the first attempts by legislators in the US and the European Union to grapple with the privacy issues raised by the deployment of this technology at the retail level. We then explore the extent to which Canada's *Personal Information Protection and Electronic Documents Act*[1] will apply to RFID technology, before making recommendations for initiatives to proactively address the privacy issues that RFIDs will raise.

II. AN OVERVIEW OF RFIDS IN THE COMMERCIAL CONTEXT

An RFID system has three integral parts: a tag, a reader and a database. The tag consists of an antenna attached to a microchip. Tags can be classified in a variety of ways based on their power source, frequency range, and processing and storage capabilities. Tags are classified as active if they have a battery power source. Active tags

---

1. S.C. 2000, c. 5 [PIPEDA].

have a range of up to several kilometres, whereas the range for passive tags is restricted to less than five metres. Semi-passive tags contain a battery, but still rely on the reader field for communication since they do not have an integrated transmitter. The maximum range for semi-passive tags is about 100 metres. Due to cost considerations, only passive tags are candidates for massive wide-scale deployment at the retail item level for low-cost commodity goods tracking.[2] This paper will therefore focus primarily on passive RFID tags, which do not have a battery and must rely on the reader field as a source of energy and for communication from and to the reader.

A reader or "transceiver" activates an RFID tag through the transmission of a signal. It "reads" the data transmitted by the tag, decodes it and communicates it to a computer for processing. The reader must use the same radio frequency as the tag it is reading, but, by using multiple readers, a system could communicate with tags that operate at different frequencies. Readers can be hand-held or fixed at specific locations. They can be obvious or hidden. In a recent report on RFIDs, the Ontario Privacy Commissioner noted that emerging technology would allow readers to be hidden in such furnishings as floor tiles or carpets, as well as such fixtures as counters or shelves.[3]

Once a conversation between an RFID reader and a tag has been established, the tag's ID is known to the reader. The ID, in and of itself, is not very useful without an associated database of information. Thus, the third component of an RFID system is typically a computer system that is attached to the reader and that has access to a database of information in which the ID on the tag is an index. This will typically be an inventory control database, but one can envision a variety of data stores indexed by RFIDs. For example, the database may house account information for RFIDs used in a toll highway or transit system. Alternatively, it could be a list of "stolen merchandise" IDs, so that passing individuals are automatically scanned for possession of stolen goods.

Although RFID tags used in the consumer context have been compared to the UPC barcode, there are key differences between them. The data storage capacity of even the smallest tags offers the commercial private sector significant advantages over current product tracking devices, such as the UPC barcode. It is possible to assign a unique code to each RFID tag. Thus, it is possible to provide a unique identifier for each product item on a store shelf. Further, the UPC barcode must be held close to a reader to be scanned, and only one item at a time may be scanned in this way. By contrast, an RFID tag need not be on the surface of a product to be read. A tag can

---

2. Active tags are also 1000 times more expensive than passive tags, costing as much as $200 US each.
3. Ontario, Information and Privacy Commissioner, *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology* by Ann Cavoukian (Toronto: Information and Privacy Commissioner, 2004) at 17, online: <http://www.ipc.on.ca/docs/rfid.pdf> [*Tag, You're It*].
4. Michael Burns, "Retailers discover venerable radio technology" *The Bottom Line* 20:15 (November 2004), online: 180 Systems <http://www.180systems.com/RFID.pdf>.

be read even if it is embedded in clothing or hidden by an outer layer of clothing, inside a box or within a shopping bag. A tag may even be read through a layer of skin. Substances and signals that interfere with RFID signals, including some metals, liquids, cell phone transmission towers, walkie-talkies and even bug-zappers, can be used effectively to "block" RFIDs.[4]

A. *Commercial Uses of RFIDs*

A recent study found that over 50% of Canadian retailers plan to be using RFID technology within the next two years. The study also found that a majority of these retailers (71%) have already taken active steps to implement the technology, yet "very few" claimed to be extremely familiar with it.[5]

Inventory tracking is the most immediate planned use of RFID technology in the commercial sector. Its potential use in tracking inventory from the point of manufacture to the retail store shelves, using the tags attached to pallets or crates,[6] could give companies constant awareness of where goods and shipments are and immediate knowledge of delays.[7] The recent US Federal Trade Commission Staff Report on RFIDs anticipated major cost savings from the use of RFIDs in the supply chain.[8] The potential of RFIDs as tools for organizing and monitoring the supply of goods and services is extensive.[9]

The next phase of private sector RFID deployment is expected to be the widespread tagging of individual consumer items. This use depends on the technology becoming sufficiently inexpensive, which may not happen until 2008,[10] although pilot projects are under way in various contexts. Gillette has, for example, experimented with "smart shelves"[11] which are equipped with a reader, while each individual item

---

5. Deloitte Canada, News Release, "Nearly half of Canadian retail and consumer corporations anticipate using RFID technology within two years–reveals Deloitte study" (11 November, 2004), online: <http://www.Deloitte.com/dtt/press_release/0,1014,cid%3D65794%26pv%3DY,00.html>.
6. Jeffrey Silva, "ACLU says RFID in passports leaves Americans vulnerable" *RCR Wireless News* (29 November 2004), online: <http://rcrnews.com/news.cms?newsId=20582>.
7. Barnaby J. Feder "Keeping Better Track From Factory to Checkout" *The New York Times* (11 November 2004) G7, online: <http://www.nytimes.com/2004/11/11/technology/circuits/11howw.html?ex=1142053200&en=471e79ecac2ca0bd&ei=5070>.
8. U.S., Federal Trade Commission, *Radio Frequency Identification: Applications and Implications for Consumers* (2005) at 9, online: <http://www.ftc.gov./os/2005/03/050308rfidrpt.pdf> [FTC Report].
9. Analogous to supply chain uses is the deployment of RFIDs to monitor or track larger items. For example, airlines and airports have been experimenting with RFID-equipped baggage tags to improve baggage-handling services, and at least one airport is using RFIDs as part of a system to control the order and supply of taxi cabs to waiting consumers. See e.g. Andy McCue, "Heathrow Airport to get taxi-tracking RFID system" (22 January 2004), online: <http://networks.silicon.com/mobile/0,39024665,39117915,00.htm>.
10. FTC Report, *supra* note 8 at 11.
11. Carl Zetie, "RFID: The Good, the Bad and the Ugly" *Information Week* (15 December 2003), online: <http://www.informationweek.com/story/showArticle.jhtml?articleID=16700081>. See also: Mark Baard, "Lawmakers Alarmed by RFID Spying" *Wired News* (26 February 2004), online: <http://www.wired.com/news/privacy/1,62433-0.html>. This experiment ended prematurely when it was discovered that Gillette was also photographing customers using hidden cameras as part of the experiment.

on the shelf contains an RFID tag. As consumers remove products from the shelves, the tags are read and the information is communicated to an inventory control system that lets workers know when shelves need restocking. Such a system could also be designed to automatically re-order inventory when supplies of a particular item fall below a certain level. Applications in retail clothing stores include linking handheld devices to real-time inventory systems that could provide sales personnel with precise and immediate information about items in stock, including sizes, colours and other relevant details.[12]

RFIDs may also be instrumental in advancing a range of consumer-oriented technologies, including "smart appliances" equipped with RFID readers. A reader-equipped refrigerator would read the RFID tags on grocery items stored within it and communicate to the homeowner when items had reached their expiry dates. A smart fridge could also provide inventory updates, letting consumers know when they were running low on certain items. Similarly, a smart washing machine would read tags on items of clothing and alert the operator when, for example, a delicate item is accidentally added to a regular load. Smart appliances offer consumers the "next generation" of in-home technology. Significantly, however, from a privacy perspective, they also increase the disadvantages to customers of deactivating tags contained in various commodity items.

Retailers are also interested in how RFIDs could improve the efficiency of operations, of customer service, or of both. For example, exchanges and refunds would be accomplished easily if each item contained a unique identifier that could be matched to the store's information on when and where it was purchased and how much was paid. Customers need never retain receipts, but could return or exchange any item, even one received as a gift. RFIDs could also be used to verify warranty protection.[13] Although convenient in some ways, these customer-oriented benefits concern privacy advocates because they disadvantage consumers who remove or deactivate their tags. They also raise issues from a policy development point of view: if these uses of RFIDs become widespread, it will be difficult to choose legislative or regulatory options that provide for mandatory deactivation of tags at the point of purchase.

Privacy advocates have raised concerns that 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 throughout a store, a business could garner information about how customers move through the store, which areas are most

---

12. The Gap has experimented with such a system. See Jerry Brito, "Relax, Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature" [2004] 5 UCLA J.L. & Tech. 1, online: <http://www.lawtechjournal.com/articles/2004/05_041220_brito.pdf>.

13. Wal-Mart has stated: "Consumers may wish to keep RFID tags on packaging to facilitate returns and warranty servicing". See Electronic Privacy Information Center, "EPIC Questions to RFID Industry", online: <http://www.epic.org/privacy/rfid/survey.html>.

heavily browsed, and so on. The potential use of RFIDs on customer loyalty cards raises privacy concerns as well. Cards embedded with RFID tags can be read through clothing, purses or wallets. In this way, the store that issued the card, or an affiliated store, could identify any cardholder who enters the store without the cardholder's knowledge.[14] Shoppers could be monitored to ascertain their habits or preferences, regardless of whether they actually make any purchases on any given visit to the store.[15]

B. *RFIDs and Databases*

The collection and storage of information related to product items, and the matching of this data with customer information, is at the heart of many privacy concerns regarding RFIDs. The information contained in a database is only as secure as the database itself. To the extent that RFIDs enable even more detailed customer profiles to be created, they exacerbate general privacy concerns about the security of data in the hands of private sector companies. In a recent US consumer survey, two thirds of those surveyed indicated that their top concern with RFID technology was "the likelihood that RFIDs would lead to their data being shared with third parties, more targeted marketing, or the tracking of consumers via their product purchases."[16]

Data matching with RFIDs could arise, for example, where a customer uses a credit card or loyalty card during the purchase of items bearing RFID tags. The information about those purchases can be matched with the customer's personal data to create a customer profile of increasing complexity and detail. While to some extent loyalty cards are already used to match data about purchases to personal information, the use of RFIDs adds another dimension. For example, even before he or she has made a purchase, a repeat customer can be identified when a reader accesses RFID tags in his or her clothing, which was previously purchased in the store, and then matches the data to the customer's personal information and profile.

It is not clear whether these concerns about data matching are exaggerated.[17] However, the collection of vast amounts of personal information relating to consumption habits through devices such as loyalty cards is already a widespread practice. One study found that "eight of the top ten U.S. grocery retailers own at least

---

14. In Germany, the grocery store Metro implanted their "Payback Loyalty" consumer cards with RFID tags, without notice to customers. The cards could be read from a distance, through wallets or clothing, to identify shoppers. See Jo Best, "Supermarket cans RFID trials in Germany" (1 March 2004), online: <http://networks.silicon.com/lans/0,39024663,39118760,00.htm>.
15. EC, Data Protection Working Party, "Working document on data protection issues related to RFID technology" (Brussels: Working Party, 2005) at 5-6, online: <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf> [Working Document].
16. FTC Report, *supra* note 8 at 12.
17. *Ibid.* at 15.

one supermarket chain with a [loyalty] card program" and that they used these programs to track "unprecedented amounts of . . . information on consumer purchase and eating habits."[18] This study also noted that "the most egregious privacy violations in the commercial sphere occur far from the average consumer's experience and awareness," but that cards used by grocery stores are linked to a "host of complex strategies to watch, record and control consumers on an enormous scale."[19]

C. *Secondary Uses: Government Use of Private Sector Data*

Secondary uses of RFID data are a major privacy issue. A secondary use can be defined as a use other than that for which the data was collected. One concern is that the government may be able to obtain from the private sector RFID data matched to personally identifiable consumer information. Concerns about information falling into the hands of government are heightened in the post-September 11 environment, as there are already examples of incidents in which private sector companies have voluntarily furnished government with consumer information.[20] This concern is not unique to data collected via RFID technology, however.

Information gathered through the use of RFIDs might be called upon in legal contexts as well. Data collected by RFIDs on bridge toll systems have been subpoenaed in divorce cases.[21] RFIDs in the clothing or personal effects could be used to assist in the identification of victims of crimes. Similarly, RFIDs in consumer items left at crime scenes could be used to track and identify individuals connected to them. RFIDs could also be used to identify "hot" goods at flea markets or in other contexts. While there is a public interest in crime detection and law enforcement, there is also a range of privacy concerns about such uses.

D. *Illegitimate Uses*

Undoubtedly, RFIDs could be deployed in ways covert and illegitimate. A commonly cited concern is that if consumer goods are tagged with RFIDs, potential criminals could scan one's home with a hand-held reader to detect the nature and value of the goods stored within.[22] Other forms of surveillance may also be possible. For example, if RFID tags are used to store personally identifiable infor-

---

18. Katherine Albrecht, "Supermarket Cards: The Tip of the Retail Surveillance Iceberg" (2001-2002) 79 Denv. U.L. Rev. 534 at 534.
19. *Ibid.* at 535.
20. See Jennifer Stoddart, "Privacy in a New Era: Challenges, Opportunities and Partnerships" (Address to the Public Voice Symposium, September 2004), online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/speech/2004/sp-d_040913_e.asp>.
21. See e.g. Mark Baard, "Watchdogs Push for RFID Laws" *Wired News* (5 April 2004), online: <http://www.wired.com/news/privacy/0,1848,62922,00.html>.
22. See e.g. Brian Dipert, "Reading Between the Lines: RFIDs Confront the Venerable Bar Code" *EDN* (14 October 2004), online: <http://www.edn.com/article/CA468418.html>; Eric Jacksch, "Why You Should Care" *Monitor Magazine Online* 11:11 (June 2004), online: <http://www.monitor.ca/monitor/issues/vol11iss11/feature3.html>.

mation, as they may be in a loyalty card, a public transit pass or a driver's licence, surreptitious scanning of these chips could give third parties access to important personal information. As the EU Working Party on Data Protection noted: "As they work non-line-of-sight and contactless, an attacker can work remotely and passive readings will not be noticed."[23]

III. Regulating RFIDs: An Overview of Developments Outside of Canada

Before conducting an assessment of privacy law and RFIDs in Canada, it is useful to look at developments in jurisdictions outside Canada. The discussion below focuses on law and policy developments in the United States and in the European Union.[24]

A. *International*

In November 2003, the Resolution on Radio-Frequency Identification[25] was adopted at the 25th International Conference of Data Protection and Privacy Commissioners. The Resolution on RFID noted that "[although] this technology can have positive and benign effects, there are also potential privacy implications."[26] Specific concerns identified were the potential to link product information with customer credit card information and the potential to use RFIDs "to locate or profile persons possessing tagged objects."[27] The potential of this technology to be used to link product information with existing databases was emphasized.

The Resolution on RFID stated the need to observe the basic principles of data protection and privacy law in relation to the use of RFIDs. The particular principles set out in the Resolution on RFID are as follows:

---

23. Working Document, *supra* note 15 at 6.

24. While it is clear that privacy commissioners around the world are alert to the issues raised by RFIDs, there has been relatively little legislative or other policy making in relation to this new technology. The Information Commissioner's Office in the United Kingdom has published reports on several topics that address RFIDs, although they do so in a relatively minor manner. See e.g. U.K., Information Commissioner's Office, *Public Attitudes to the Deployment of Surveillance Techniques in Public Places* (Qualitative Research Report) (2004), online: <http://www.informationcommissioner.gov.uk/cms/DocumentUploads/cctv report.pdf>; U.K., Information Commissioner's Office, *Technology Development and its Effect on Privacy and Law Enforcement* (Qualitative Research Report) (2004), online: <http://www.informationcommissioner.gov.uk/cms/DocumentUploads/report parts 1&2.pdf>. A recent presentation by the Assistant Privacy Commissioner of New Zealand raised concerns about the use of RFIDs and recommended compliance with New Zealand's private sector privacy legislation, the development of global initiatives, and public education. See Blair Stewart, "EPC/RFID—The Way of the Future? A Privacy Perspective" (Address to GS1 New Zealand/EPCglobal New Zealand "EPC/RFID-The Way of the Future" Conference, February 2005), online: <http://www.privacy.org.nz/EPCRFID.doc>.

25. "Resolution on Radio-Frequency Identification" (Resolution adopted by the International Conference of Data Protection & Privacy Commissioners, November 2003), online: <http://www.privacyconference2003.org/resolutions/res5.DOC> [Resolution on RFID].

26. *Ibid.*

27. *Ibid.*

> a) any controller—before introducing RFID tags linked to personal information or leading to customer profiles—should first consider alternatives which achieve the same goal without collecting personal information or profiling customers;
>
> b) if the controller can show that personal data are indispensable, they must be collected in an open and transparent way;
>
> c) personal data may only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve (or carry out) this purpose, and
>
> d) whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags.[28]

The Resolution on RFID also noted that "[t]he remote reading and activating of RFID tags, without any reasonable opportunity for the person in possession of the tagged object to influence this process, would raise additional privacy concerns."[29] This statement seems to address both the use of readers by stores to gather information from RFID tags at points other than the checkout, as well as the use of readers by other parties in other contexts.

Overall, the 2003 Resolution on RFID takes a very measured approach to RFIDs, noting their potential benefits and focusing almost exclusively on their use in the commercial context. Parts (a), (b) and (c) of the recommendations focus on the adaptation of personal information protection principles to the context of RFIDs. Part (d) seems to address a further issue: the potential for consumers to disable any tags that come into their possession.

B. *The United States*

It is not surprising, given the role that American corporations play in driving the development and deployment of RFIDs, that there are significant concerns about

---

28. *Ibid.*
29. *Ibid.*
30. U.S., Bill H.R. 4673, 108th Congress, 2d Sess., 2004, s. 2(c) [*Federal Bill 4673*], introduced in the House of Representatives in June 2004, required warning labels to be placed on any consumer products containing RFID devices. The label would have to inform consumers that the device could be used in tracking the product before and after purchase. Labelling requirements feature prominently in state bills as well. See e.g. U.S., S.B. 867, *An Act to amend chapter 407, RSMo, by adding thereto one new section relating to radio frequency identification tags (RFID)*, 92d Gen. Assem., Reg. Sess., Mo., 2005 [*Missouri Bill*]; U.S., H.B. 251, *Radio Frequency Identification—Right to Know Act*, 2004, Gen. Sess., Utah, 2004 [*Utah Bill*]; U.S., S.B. 181, *An Act Relative to Consumer Protection and Radio Frequency Identification Systems*, 2005, Reg. Sess., Mass., 2005 [*Massachusetts Bill*]; U.S., H.B. 215, *An Act relating to Consumer Protection; requiring removal of radio frequency identification tags on consumer goods at points of purchase; requiring limits on business release of personal information; prescribing penalties*, 47th Legis., Reg. Sess., N.Mex., 2005 [*New Mexico Bill*]; U.S., H.B. 1136, *An Act to regulate the use of radio frequency identification tags*, 80th Legis. Ass., Reg. Sess., S.Dak., 2005 (defeated) [*South Dakota Bill*]; U.S., S.B. 699, *An Act to amend Tennessee Code Annotated, Title 47, Chapter 18, relative to consumer protection*, 2005, Reg. Sess., Tenn., 2005 [*Tennessee Bill*]; U.S., H.B. 300, *An Act to amend Tennessee Code Annotated, Title 47, Chapter 18, relative to consumer protection*, 2005, Reg. Sess., Tenn., 2005; U.S., S.B. 264, 2005, Reg. Sess., Nev., 2005.

RFIDs and privacy in the US. These concerns have led to the introduction of a number of bills at the state and federal level that attempt to establish parameters for the use and deployment of RFIDs. While a few of these bills have died, and only one to date has been signed into law, a number still remain under active consideration.

A few trends or points are worth noting with respect to these early legislative initiatives. Labelling requirements are the focus of a number of these legislative initiatives.[30] They recognize that consumers are entitled to notice when personal information is being gathered. Notice may appear on the specific product item or, more generally, near the product shelf or at the checkout.[31] A general labelling requirement, where the chip contains only product information and not personal information, would draw the consumer's attention to the fact that the product is capable of conveying information about itself, and by extension its purchaser.

Labelling requirements in the US bills typically stipulate that RFIDs be deactivated at the point of sale or that consumers be given the option of deactivating them.[32] Such provisions, potentially protective of consumer privacy, will likely run into problems as technology advances and as the continued activation of RFIDs becomes essential to the functioning of warranty and return systems or of smart con-

---

31. See U.S., H.B. 203-FN, *An Act relative to the regulation of tracking devices and establishing a commission on the use of tracking devices*, 2005, Reg. Sess., N.H., 2005, which would require retailers to notify consumers, orally or in writing, that an RFID tag is embedded in a product. In contrast to other bills with labelling requirements, this one is much less specific about the location, visibility or contents of any label or notice given to consumers. S. 2 of the *Tennessee Bill*, *supra* note 30, would amend s. 47-18-104 of the *Tennessee Code Annotated* to make it an offence to sell "any good containing a radio frequency identification tag that does not bear a label on the good or the good's packaging". The label must state that the good or its packaging contains an RFID tag and that the tag can transmit information about the item both before and after purchase. The label must be "in a conspicuous type-size and location". The *Utah Bill*, *supra* note 30, s. 2(2)(s) would have made it an offence for retailers to sell a product containing an RFID tag to a consumer without providing notice on the product or packaging that the product contained an RFID. Labels would have to inform the consumer that the RFID can transmit information to a reader both before and after purchase. The bill also contained specifications relating to the visibility and readability of such labels. The *Massachusetts Bill, supra* note 30, s. 3 would require multi-level warnings. Retailers using RFIDs in their stores would have to "display a sign placed in a conspicuous location printed in a conspicuous type size" to warn consumers that the store uses RFID technology and that products are equipped with tags containing information that can be read before and after purchase. All products using RFID tags would have to bear labels, in a conspicuous location on the packaging, which state that the product contains an RFID tag, and that the information on the tag can be read both before and after the item is purchased.

32. *Federal Bill 4673*, *supra* note 30, mandated that the consumer be given an option to have the chip removed from the product or deactivated following purchase, and that the label provide this information. Under the *Massachusetts Bill*, *supra* note 30, s. 3, "RFID tags that are not components essential to the tagged item's operation shall be attached in such a way as to allow individuals to remove the tag after the item has been purchased without damaging the item". The *Utah Bill*, *supra* note 30, s. 2(2)(t) required any supplier to disable the RFID prior to the completion of the sale "unless the consumer chooses to leave it active". The *New Mexico Bill*, *supra* note 30 ss. 3-4 would have required retailers using RFIDs to provide notice that RFIDs are being used, to label products containing RFID tags, and to remove or deactivate tags at the point of purchase. The bill would also have sanctioned businesses that coerce consumers into keeping tags active (s. 4), and that match consumer personal information with tag information "beyond what is required to manage inventory" and share information gathered from RFID tags with third parties (s. 5). The *New Mexico Bill* faced fierce opposition from the retail and high-tech sectors and was ultimately defeated. It is expected to be reintroduced in 2006. The *South Dakota Bill*, *supra* note 30, s. 5 required that tags be deactivated before consumers left a store in which they had purchased any tagged item.

sumer products. Tags in clothing may be designed to communicate information to washing machines, to wash the article more efficiently. Tags in grocery items may communicate with refrigerators to report their expiry dates. Deactivation removes this utility and may increasingly be seen as an ineffective or suboptimal option.[33]

Bills addressing labelling requirements often specify the size, location and format of the label to ensure clear visibility.[34] In some cases, additional notification is required in retail stores.[35] Generally, labels must go beyond informing consumers that an RFID tag is present, to informing them of the tag's ability to transmit unique identifier information before and after purchase.[36]

The success or failure of these bills is tied to the demands they make on commercial interests. The bills that have been defeated, such as the *New Mexico Bill*[37] and the *South Dakota Bill*,[38] provided such strict limitations on the use of RFIDs, however, that the advantages to retailers of using such tags were largely negated. This is an important lesson to be drawn from the US experience: the protection of consumer privacy must be balanced against commercial interests in deploying useful technologies.

C. *The European Union*

The European Union has perhaps been the most active in responding to the privacy issues raised by RFID technology. In a Working Document released in January 2005, the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (Working Party) issued guidelines for the use of RFIDs in the private sector.[39] The Working Document was followed by a call for comment on the proposed guidelines, with a deadline of March 31, 2005.

Acknowledging that RFID technology could have a number of advantages to businesses, individuals and governments, the Working Party nonetheless issued this very stern caution:

> The ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and

---

33. FTC Report, *supra* note 8 at 21.
34. For example, the *Missouri Bill*, *supra* note 30, s. 4(1) required mandatory labelling of products containing RFIDs to inform consumers that the product in question contained an RFID tag, and that "the tag can transmit unique identification information to an independent reader both before and after purchase". The bill also stated that labels must be clear and readable. There was no requirement that consumers be given the option of having the tag removed or deactivated at the point of purchase. The bill has passed second reading and was referred to the Commerce, Energy and the Environment Committee in January of 2005. See also the discussion of labelling requirements, *supra* notes 30-31.
35. This is the case in the *Massachusetts Bill*, *supra* note 30, which requires notification on the product and also in the store itself.
36. This was the case in the *Utah Bill*, the *Tennessee Bill* and the *Missouri Bill*, *supra* note 30.
37. *Supra* note 30.
38. *Supra* note 30.
39. *Supra* note 15.

> accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns. The problem is aggravated by the fact that, due to its relative low cost, this technology will not only be available to major actors but also to smaller players and individual citizens.[40]

The Working Party is clearly aware that RFIDs have both privacy-neutral and privacy-invasive uses and that privacy-neutral uses could impact on personal privacy in cases of illegitimate use of tag data.

The EU's *Data Protection Directive*[41] sets out basic norms relating to the processing of personal data. Personal data is broadly defined as "any information relating to an identified or identifiable natural person."[42] The Working Party notes that whether or not the *Data Protection Directive* will apply to data collected from RFID tags will depend on each particular RFID application: where RFID data is not matched with personally identifiable data, for example, there will be no privacy implications.[43] In the retail context, RFIDs are likely to contain data about the specific products in which they are embedded, but it is possible to link this data to customer information. As the Working Party notes,[44] the *Data Protection Directive* itself is instructive about whether or not it should apply: parties should take account "of all the means likely reasonably to be used either by the controller *or by any other person to identify the said person*."[45] Thus, it may be possible to consider the potential to link RFID tag data to other personal data beyond the context of a particular in-store transaction.

Aside from these grey areas, the Working Party notes that in many contexts it will be clear that the Directive and its norms apply.[46] Thus, where RFID data is matched with customer data on credit or loyalty cards, the RFID data will become information about an identifiable person and the Directive is engaged.

Because it would be difficult to establish how the Directive's requirements should apply in every conceivable context, the Working Party attempts to provide general guidelines for dealing with RFID data. Significantly, it does not place sole responsibility for complying with the Directive on the data collector at the end of the RFID chain. It states that "manufacturers have a direct responsibility in ensuring that privacy compliant technology exists to help data controllers to carry out their obligations under the [*Data Protection Directive*] and to facilitate the exercise of an individ-

---

40. *Ibid.* at 2.
41. EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J.L. 281/31, online: EurLex <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett> [*Data Protection Directive*].
42. *Ibid.* at 38.
43. Working Document, *supra* note 15 at 8.
44. *Ibid.*
45. *Data Protection Directive*, *supra* note 41 at 33 [emphasis added].
46. Working Document, *supra* note 15 at 8.

ual's rights."[47] This is distinct from the approach taken in the various US state bills described earlier. They place the onus largely on the retailer at the point of transaction with the customer, while the EU charges manufacturers of the technology to produce technology that can be used in compliance with the Directive and that gives consumers more privacy options.

In emphasizing data controllers' mandatory compliance with the Directive, the Working Party's guidelines single out particular principles: limiting the purposes of data collection, avoiding the collection of irrelevant data, and storing data only for as long as is necessary to meet the purposes of collection. Further, RFID data can be processed only if there is a legitimate basis to do so. This may mean that consent to the data collection by the data subject will be required in some circumstances, possibly where loyalty card data will be matched with RFID data from consumer items. In such cases, the consent provisions of the Directive will be applicable.[48]

The Working Party indicates that data controllers must provide notice to data subjects about a range of issues. First, controllers must inform consumers of the presence of RFID tags on products or packaging and of RFID readers on the premises. This latter requirement is an important one that has not commonly appeared in the US bills. Since readers can be hidden, and can operate silently and invisibly, it is important to alert consumers to their locations. Second, consumers must understand the link between the presence of RFIDs and data collection, and they must know that tags and readers can operate without their knowledge or awareness. They must be told the purposes for collection, what data matching will take place, and whether or not data will be shared with third parties. Third, the identity of the data controller must also be disclosed, which can be significant in the context of RFIDs. For example, although the customer may be shopping in a particular supermarket, other companies may have installed readers as part of a test-marketing program for their products. Fourth, data subjects have a right to access data collected through RFID technology and matched with their personal information, and to check the accuracy and currency of the information. They also have this right with respect to RFID tags containing their own personal data, such as tags embedded on loyalty cards or other identification documents. The normal requirements of data security also apply in the context of information gathered using RFID technology.[49]

The Working Party also emphasizes the role that technology can play in protecting privacy. RFID technology designed according to standardized initiatives, such as those of EPCglobal (discussed below), can incorporate technological responses to privacy concerns. The Working Party is open to the use of pictograms or logos to identify the presence of tags or readers. Beyond that, the Working Document con-

47. *Ibid.* at 9.
48. *Ibid.* at 9-10.
49. *Ibid.* at 10-11.

templates technological developments that will signal when RFID components are operating; for example, a light that flashes when a reader is active or an audible tone that sounds when a reader reads a tag. Other devices could block, erase or scramble tag information or delete content by sending a "kill" command to the tag. As tags are difficult to read through metal, sheathing items in aluminum, for example, could block signals from RFIDs embedded in those items. The Working Party recommends additional research and development on technical measures to protect data.[50]

IV. APPLICATION OF THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT* (*PIPEDA*)

A. *Application to the Commercial Use of RFID Technology*

Unlike the US or the EU, Canada has not yet attempted to develop RFID-specific privacy norms. Instead, it is currently dependent upon the application of general private sector privacy legislation such as *PIPEDA*[51] and its provincial counterparts.[52] *PIPEDA* applies where an "organization collects, uses or discloses [personal information about its clients or customers] in the course of [its] commercial activities."[53] It also applies to personal information about employees of an organization that "the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."[54] Personal information of those employed by organizations strictly within the private sector is not generally governed by the Act. *PIPEDA* broadly defines the term "organization" to include an association, a partnership, a person (which includes a corporation) or a trade union.[55] Most, if not all, private sector individuals or bodies carrying on commercial activities are captured by this definition. Therefore, the application of *PIPEDA* to the use of RFIDs in the private sector will depend, first, on whether or not the information collected, used or disclosed by means of RFID technology is personal information and, second, on whether or not the organization's collection, use or disclosure of such information using RFID technology occurs in the course of commercial activities.

---

50. *Ibid.* at 14-15.
51. *Supra* note 1.
52. For reasons of space, we discuss only the federal privacy legislation here. Private sector privacy legislation in British Columbia, Alberta and Quebec will also require interpretation to consider whether and to what extent it applies to RFIDs.
53. *Supra* note 1, s. 4(1)(a).
54. S. 4(1)(b).
55. S. 2(1).

1. *"Commercial Activity"*

There is little doubt that in most cases the collection of information via the use of RFID tags on purchased goods occurs in the course of a commercial activity. *PIPEDA* defines "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character. . . ."[56] Any commercial organization that sells products containing RFID tags is carrying on a commercial activity and is subject to *PIPEDA*. However, when commercial organizations employ RFID tags in the course of non-commercial activities that are beyond the organization's ordinary conduct, these transactions may not be governed by *PIPEDA*. Similarly, non-commercial organizations that employ RFID technology are subject to *PIPEDA* if the activities in which RFID tags are employed could be considered commercial in nature and, therefore, could be classified as "commercial activity."

In all these cases, the placement or use of the RFID tag is not a particularly relevant consideration; rather, it is the characterization of the activity as "commercial" that is determinative. Many, if not most, activities in which the private sector uses, or plans to use, RFID technology to gather information are commercial in nature and consequently would be "in the course of commercial activities" governed by *PIPEDA*.

2. *"Personal Information"*

PIPEDA applies where an organization collects, uses or discloses "personal information" in the course of commercial activities. "'Personal information' means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[57] These exceptions have been the subject of findings made by the federal Privacy Commissioner,[58] whose office has recently signalled that it will take a strict interpretation of these exceptions.[59]

The definition of "personal information" implies that such information must be about a human being, as it uses the word "individual" rather than "person." The issue, then, with respect to RFID technology, is whether or not an organization employs RFID tags to collect, use or disclose personal information (other than information listed as excepted) that is about an identifiable individual.

---

56. S. 2(1).
57. S. 2(1).
58. For example, the Commissioner has found that "under normal circumstances, an unlisted home telephone number is information about an identifiable individual and would be deemed personal information for purposes of the Act." See Office of the Privacy Commissioner of Canada, *PIPED Act Case Summary #230: Bank accused of improperly disclosing unlisted phone number to another financial institution* (Commissioner's Findings) (2003), online: <http://privcom.gc.ca/cf-dc/2003/cf-dc_030916_05_e.asp>.
59. The Assistant Privacy Commissioner recently concluded that e-mail addresses of employees are not captured by the exceptions in the definition of "personal information". See Letter to Prof. Michael Geist (1 December 2004), online: < http://www.mgblog.com/resc/GeistPCCSpamdecision.pdf>.

To determine this issue, one must examine the information that organizations engaged in commercial activities have embedded in RFID tags. Passive RFID tags deployed for inventory control communicate information about the particular product to a reader. An individual who purchases a product with an attached or embedded RFID tag may have such information communicated to a reader at, for example, a store checkout. For such information to qualify as "personal information," it would have to be linked to and be about an identifiable individual. If the information on the RFID tag is read and used by an organization solely to determine sales and inventory levels, and is not linked to a particular customer (i.e. an identifiable individual), then such information does not qualify as "personal information." Similarly, employment of a smart-shelf system, where products containing RFID tags are tracked for inventory control purposes, would not usually raise concerns about collecting or using personal information, as the association of the information with an identifiable individual would typically be absent. Even the monitoring of a customer's browsing and purchasing habits, through the use of RFID tags on products and the installation of readers throughout a store, would not usually constitute the collection of personal information, unless the customer was an identifiable individual.

In other circumstances, the information collected, used and disclosed through unique identifier RFID tags is clearly personal information. For example, organizations that offer RFID tags to customers to track movements or credit purchases are plainly collecting and using information about an identifiable individual. Organizations that use RFID tags for baggage tracking and locating, or for recording individual purchases that are charged to a hotel room account, for example, will be subject to *PIPEDA* and its privacy principles.

The potential for organizing and monitoring the supply of goods and services through the use of RFID tags is considerable. Whether or not the information communicated by RFID tags constitutes "personal information" will depend, in most cases, on how the organization uses and integrates such information with other data. If such use or integration results in the collection, use or disclosure of information about an identifiable individual, *PIPEDA* will apply.

In making this assessment, one may consider decisions from the federal Office of the Privacy Commissioner and from the courts on what constitutes "personal information." One of the federal Privacy Commissioner's first decisions rendered under *PIPEDA* dealt with a complaint that an organization had collected information about an individual that, in the circumstances, amounted to personal information, although the information collected did not *per se* identify the complainant.[60] The

60. See Office of the Privacy Commissioner of Canada, *PIPED Act Case Summary #4: Musician objects to collection of salary information by professional organization* (Commissioner's Findings) (2001), online: <http://privcom.gc.ca/cf-dc/2001/cf-dc_010723_04_e.asp>. A professional organization that collected copyright dues for its members had collected personal information about a member (his annual salary) from the member's employer. Because the complainant was the only musician at the establishment where he worked, and therefore the only employee who was a member of the professional organization, he alleged that his salary could be easily ascertained.

Commissioner applied a strict interpretation of what constituted "personal information" and did not discuss the particular context of the information collection. The Commissioner concluded that the collection did not involve personal information about an identifiable individual and found that the collection was therefore not subject to *PIPEDA*. In another controversial case, the federal Privacy Commissioner ruled that the prescribing habits of physicians did not meet the definition of "personal information," but were simply their "work product". The Commissioner concluded that "the meaning of 'personal information', though broad, is not so broad as to encompass all information associated with an individual."[61]

In the context of RFID technology and information collection, use and disclosure, these findings may indicate superficially that only highly specific information that identifies an individual meets the definition of "personal information," and that a purchase may not constitute personal information about the purchaser.[62] However, it would be risky to draw and rely on such conclusions. With respect to the latter finding, the Commissioner was careful to limit the analysis to work activity. The earlier findings were made under the administration of the previous Privacy Commissioner, and it is unclear whether the current administration will always agree with the previous one. For example, the Assistant Privacy Commissioner recently indicated that if the circumstances render an individual identifiable, then the information at issue would be considered personal information under *PIPEDA*, notwithstanding the fact that the individual is not specifically named.[63] In any event, exactly how much precedential value these findings should be accorded is questionable, as the Federal Court has indicated that they are not binding.[64]

In another finding, the Privacy Commissioner concluded that what a business may consider to be "business information" could also, in some circumstances, constitute personal information under *PIPEDA*. The Commissioner found that although the "sales statistics of individual employees are information that the company itself generates, records, and processes for reasonable and legitimate business purposes," such information could also constitute "personal information" under *PIPEDA* since "sales records attributed to the complainant in order to indicate her on-the-job performance relative to that of others constitute information about her as an identifiable indi-

---

61. Office of the Privacy Commissioner of Canada, *PIPED Act Case Summary #14: Selling of information on physicians' prescribing patterns* (Commissioner's Findings) (2001), online: <http://privcom.gc.ca/cf-dc/2001/cf-dc_010921_e.asp>.

62. Consider the former Privacy Commissioner's statement: "It is certainly diffficult [*sic*] to discern how an individual prescription can constitute personal information about the physician who wrote it." Office of the Privacy Commissioner of Canada, *PIPED Act Case Summary #15: Privacy Commissioner releases his finding on the prescribing patterns of doctors* (Letter from Privacy Commissioner to complainant) (2001), online: <http://www.privcom.gc.ca/media/an/wn_011002_e.asp>.

63. Office of the Privacy Commissioner of Canada, *PIPED Act Case Summary #270: Bank agrees to modify automated message* (Commissioner's Finding) (2004), online: <http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040504_e.asp>.

64. *Englander v. TELUS Communications Inc.* (2004), [2005] 2 F.C.R. 572 at para. 48, 247 D.L.R. (4th) 275, 2004 FCA 387.

vidual."[65] The Commissioner found nothing in *PIPEDA* that would suggest business information and personal information must be mutually exclusive.[66] By analogy, a business might consider inventory information on an RFID tag to be information gathered for business purposes, but it may also be deemed personal information if it can be considered information linked to an identifiable individual.

Inventory information captured on an RFID tag would not likely constitute personal information, as it is not about an identifiable individual. *PIPEDA* clearly does not apply to data about consumer items until such time as it is matched or linked to other personally identifiable information. For example, when a consumer makes a purchase at a store, the cashier is able to visually link the product being purchased with the individual making the purchase. Where a credit card is used, the cashier also knows the actual name of the purchaser. Currently, when a consumer walks into a store, clerks can make a visual assessment of the kind or quality of clothing, shoes or jewellery worn by the consumer, and can draw inferences about the person from these items. In some contexts, RFIDs do little more than facilitate the gathering of information that is already largely available through observation.

However, that information, coupled with other information such as that on a credit card, results in the collection of information about an identifiable individual, which, *prima facie,* should be subject to *PIPEDA*. If the two sources of information are combined and collected at the checkout, it would seem that *PIPEDA* should apply. However, inventory information on an RFID tag, even if matched to customer data, might not, in fact, be personal information, as there may not be a reasonable expectation of privacy about such mundane information gathered through technological means. If a reasonable expectation of privacy is the relevant test, presumably the *type* of inventory information on the RFID tag that is matched with an identifiable individual would be relevant. For example, linking the purchase of a piece of clothing with one's name (particularly when one's clothing is normally visible to the public) might not engender a reasonable expectation of privacy, whereas the purchase of a pornographic magazine might.[67]

Such an approach in the commercial sector creates concerns for the purchaser and difficulties for the vendor, who must ascertain whether there exists a reasonable expectation of privacy with respect to any particular product and who, consequently, must decide whether or not to apply the principles under *PIPEDA*. This reasoning would also seem to preclude *PIPEDA*'s application in situations where data

---

65. Office of the Privacy Commissioner of Canada, *PIPED Act Case Summary #220: Telemarketer objects to employer sharing her sales results with other employees* (Commissioner's Findings) (2003), online: <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030915_e.asp>.

66. *Ibid.*

67. A recent Supreme Court of Canada decision that might have some bearing on these issues will be discussed in detail below: *R. v. Tessling*, [2004] 3 S.C.R. 432, 244 D.L.R. (4th) 541, 2004 SCC 67 [*Tessling*], rev'g (2003), 63 O.R. (3d) 1, 171 C.C.C. (3d) 361 (C.A.) [*Tessling* cited to O.R.].

from multiple RFID tags linked to an identifiable individual is matched and analyzed for purchasing patterns or other information. Fundamentally, clarification of how "personal information" under *PIPEDA* relates to a "reasonable expectation of privacy" in the commercial context is required before vendors and purchasers can fully assess *PIPEDA*'s application to the expanding use of RFID technology.

PIPEDA's relevance to the use of RFID technology in the private sector will depend both on the degree to which this technology is used to link business information (e.g. inventory information) to information about an identifiable individual, and on whether or not individuals have a reasonable expectation of privacy with respect to such information stored on RFID tags. The latter requirement is not explicitly articulated in the legislation but may be implicit, depending on whether the courts view privacy as a protean concept that is context-specific, or whether a reasonable expectation of privacy test applicable to *Charter*[68] interpretation will be relevant to our understanding of the "personal information" definition in *PIPEDA*. This is an issue that affects our understanding of *PIPEDA* generally; it is not peculiar to RFID technology. However, because the type of information that, thus far, is typically included on RFID tags would not usually be classified as particularly sensitive, the application of *PIPEDA* to RFID technology may depend on whether a reasonable expectation of privacy test is indeed a relevant consideration.

3. *Reasonableness in PIPEDA*

Subsection 5(3) of *PIPEDA* contains a statement generally applicable to all instances of personal information collection:

> An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.[69]

This "reasonableness" provision gets beyond the organization's stated purposes for collecting personal information to require that those purposes be reasonable in the circumstances. The relevance of subsection 5(3) to RFIDs turns on the extent to which data collected from RFID tags is considered "personal information." It is hard to say that it would be "unreasonable" to gather information that parallels what is normally available through observation.

B. *The Normative Provisions of* PIPEDA

Subject to certain exceptions and requirements,[70] every organization that is subject to *PIPEDA* must comply with the obligations set out in Schedule 1 to the

---

68. *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.
69. *PIPEDA*, *supra* note 1, s. 5(3).
70. Ss. 6-9.

Act.[71] Schedule 1 incorporates the Principles and Commentary of the *Model Code for the Protection of Personal Information* adopted by the Canadian Standards Association.[72] The Principles do not refer to specific technologies, and therefore do not address the particular or peculiar challenges that the application of new information-gathering tools, such as RFIDs, present with respect to the privacy of personal information. The following section examines the requirements of these Principles in the context of RFID use in commercial activities. In particular, it focuses on those Principles for which the use of RFIDs raises specific questions or uncertainties.[73] It also assumes that there would be a reasonable expectation of privacy with respect to *any* purchasing information about an identifiable individual—an assumption that, as suggested above, is not patently clear in Canadian law.

1. *Principle 2: Identifying Purposes*

An organization must identify the purposes for which personal information is collected at, or before, the time it is collected. If such information is used for another purpose not previously identified, the new purpose must be identified prior to use, and consent must be obtained before the information can be used for that purpose.

As previously discussed, an organization that tracks inventory without reference to an identifiable individual would not likely be subject to *PIPEDA*, in which case there would not be a normative requirement to identify the reasons for the product placement of an RFID tag. However, if the information that is gathered through the use of the RFID tag is coupled with other information, such that the information qualifies as "personal information," the purposes for which that personal information is collected will have to be identified. In a commercial context, this would normally occur at the checkout, but it could occur at other times (e.g. in the recording of purchases to a hotel room account). Principle 2 requires the identification of the purpose for which the personal information is collected at or before the time of collection.[74] Practically, this would entail in-store signage and/or product labelling to notify customers that products contain RFID tags that enable the collection of personal information and to explain the purposes for which the information is collected.

---

71. S. 5.

72. Canadian Standards Association, *CSA Standard CAN/CSA-Q830-96: Model Code for the Protection of Personal Information*, online: <http://www.csa.ca/standards/privacy/code/Default.asp?language=English>.

73. The four Principles that are highlighted raise specific issues with respect to the employment of RFIDs in commercial transactions. The remaining Principles, such as the requirement for adequate security safeguards, the requirement that an organization be open about its policies and practices relating to the management of personal information, and allowing individuals to access and challenge the accuracy and completeness of information gathered by an organization will, of course, also apply to personal information gathered by the use of RFID tags.

74. *PIPEDA*, *supra* note 1, Sch. 1, s. 4.2.

2. *Principle 3: Consent*

Generally, individuals must have knowledge of and consent to the collection, use or disclosure of their personal information. Signage and/or labelling could fulfil the notice requirement of Principle 3. However, consent will not necessarily be deemed by simply giving notice, and an organization cannot, as a condition of the supply of a product, require an individual to consent to the collection, use or disclosure of personal information beyond that required to fulfil explicitly specified and legitimate purposes.[75] The form of consent may vary, depending on the sensitivity of the information.[76] Express consent will be required where the information is likely to be considered sensitive.[77] Also, an individual may withdraw consent at any time.[78]

With respect to the use of RFIDs, the form of consent will depend on the type of product being purchased. If the purchase of the particular product by the customer could be considered sensitive information, express consent will be necessary. Because written consent may not be practical in the retail environment, some other measure, such as mandatory deactivation of tags at the checkout, may be appropriate.

Where the information is less sensitive, implied consent might be acceptable in a situation where the customer is adequately notified of the option of deactivation but chooses not to make that request. However, in the absence of clear legal authority, it could be difficult for the retailer to discern the circumstances in which the information regarding any particular purchase could be considered sensitive.

An organization might seek consent to collect, use or disclose a customer's personal information through the application form that a customer completes for that organization's loyalty or credit card. By completing and signing the form, customers could agree to the matching of their prospective purchases with their identity on the card. However, the organization should not generally be able to require the customer to consent in this way as a condition of receiving the card. Customers should be given the option on the application form of refusing to have their personal information collected, used or disclosed in this way.

An individual may also withdraw consent at any time, subject to contractual restrictions and reasonable notice.[79] The organization must then inform the individual of the implications of such withdrawal. In the case of product matching with identifiable individuals through the use of RFID tags, such consequences could include interference with the ability to return products or access warranties.

---

75. Sch. 1, s. 4.3.3.
76. Sch. 1, s. 4.3.4.
77. Sch. 1, s. 4.3.6.
78. Sch. 1, s. 4.3.8.
79. *Ibid.*

3. *Principle 4: Limiting Collection*

Information cannot be collected indiscriminately, but must be limited to that which is necessary for the purposes specified.[80] Therefore, the collection of information must be limited to the identification of the purposes reflected in Principle 2.

If the purposes of the collection of the personal information by means of RFID tags are inventory control and customer service (for example, by allowing a customer to easily return or exchange merchandise), then the collection of information that tracks the customer's movements throughout a store, or the indiscriminate reading of RFID tags on a customer's person, do not serve such a purpose. In most cases, the limited information required for the identified purpose will be collected only at the point of purchase, in conformity with Principle 3.

4. *Principle 5: Limiting Use, Disclosure and Retention*

Once information is collected for the purpose identified, it cannot be used or disclosed for any other purpose, except with the consent of the individual or as required by law.[81] In situations where information has already been collected and an organization wishes to use or disclose such information, consent is required from the individual to use the information for a purpose that was not previously identified.[82]

The application of this Principle to the use of RFID tags does not really raise uncertainties peculiar to this technology. However, it is worth emphasizing that the use of RFID tags in collecting information for inventory and customer service purposes will not allow the organization to share the information with unaffiliated third parties without the express consent of the customer, or to use the information in any way for its own benefit other than for the purposes previously identified to the customer and to which the customer has consented. Similarly, any personal information obtained through the use of RFID technology, like information obtained by any other means, will be subject to the minimum and maximum retention periods necessary for the purposes for which the information was collected and to allow the individual to access the information pursuant to Principle 9.

C. *Collection, Use and Disclosure Without Consent*

PIPEDA provides for a number of contexts and situations in which information can be collected, used or disclosed without an individual's consent. Each activity, collection, use or disclosure is treated separately in section 7 of the Act. These exceptions are extremely important in the context of RFID technology. Our discussion in this part is limited to those aspects of the exceptions that are of particular relevance to RFIDs.

---

80. Sch. 1, s. 4.4.
81. Sch. 1, s. 4.5.
82. Sch. 1, s. 4.3.1.

Paragraph 7(1)(b) states that information may be collected without an individual's consent where:

> (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province. . . . [83]

This provision raises certain concerns in relation to RFIDs where personal information is stored on an RFID chip in, for example, a loyalty card or a government-issued document such as a driver's licence. The collection of this information without the individual's knowledge or consent may be permitted in a broad range of contexts where there exist possible breaches of agreements or contraventions of the laws of Canada or a province.

It is the possibility of *disclosure* without knowledge or consent that is most worrisome. Subsection 7(3) of the Act provides:

> (3) . . . an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is . . .
>
> > (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records. . . . [84]

Clearly, an organization could be compelled by a court to produce information in its possession without the knowledge or consent of the data subject. This may occur in the context of civil actions.

In addition to disclosure under court order, there is also the possibility that organizations may be required to, or may voluntarily choose to, disclose information to government institutions in response to requests and in relation to national security or law enforcement. In the post-September 11 environment, there is reason to be concerned about such provisions and the scope they give to private sector companies to "cooperate" with government through large-scale transfers of data.[85] Similar concerns have been raised in the United States.[86] Paragraph 7(3)(c.1) of *PIPEDA* permits disclosure by an organization of personal information without an individual's knowledge or consent, where it is

> (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

---

83. S. 7(1)(b).
84. S. 7(3).
85. See e.g. John Schwartz, Micheline Maynard & Eric Lichtblau "Airlines Gave F.B.I. Millions of Records on Travelers After 9/11" *The New York Times* (1 May 2004) A10.

> (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
>
> (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
>
> (iii) the disclosure is requested for the purpose of administering any law of Canada or a province. . . . [87]

These provisions give an enormous scope for data collected in the private sector to be disclosed to government without the knowledge or consent of the individual. Privacy commentators in Canada have stated: "Only information that is of a relatively innocuous nature will be collected by these means, since the collection of information in which the individual has a reasonable expectation of privacy would require the *Charter* protection of a warrant."[88] However, as discussed earlier, the scope of these provisions in relation to data collected from RFIDs is more troubling.

Paragraph 7(3)(d) of *PIPEDA* permits organizations, on their own initiative, to disclose information to an investigative body, a government institution or part of a government institution, where the organization:

> (i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or
>
> (ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs. . . . [89]

To the extent that RFID technology has the potential to allow private organizations to collect and compile data about individuals that is unprecedented in both volume and nature, there is good reason to be concerned about these provisions. Allowing private sector organizations to act as government informants places ordinary individuals in a vulnerable situation.

---

86. These concerns have been raised with respect to broad powers of government in the US under the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272. See Waseem Karim, "The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring" (2004) 14 Wash. U.J.L. & Pol'y 485 at 512.

87. *PIPEDA*, *supra* note 1, s. 7(3)(c.1).

88. S. Perrin *et al.*, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law, 2001) at 75.

89. *PIPEDA*, *supra* note 1, s. 7(3)(d).

D. *The Conundrum of Secondary Uses of Personal Information*

The potential for secondary uses to be made of data gathered from RFIDs and matched with personal information has already been addressed. Secondary uses may include use by government in a variety of contexts where information can legally be collected, used or disclosed without the consent of the data subject. The recent Supreme Court of Canada decision in *Tessling*,[90] combined with the potential for secondary uses of personal information, raise unique concerns.

Tessling involved a claim, under section 8 of the *Charter*,[91] that the warrantless use of a thermal imaging device violated the rights of the accused. The RCMP flew in an airplane over the house of the accused and used a thermal imaging device to take a "heat" picture of the house. Based on the heat emanations and other information, the RCMP obtained a search warrant for the accused's home. They found a large quantity of marijuana and several guns.

The Court ruled that the fly-over heat imaging did not violate the accused's *Charter* rights. In doing so, Binnie J identified three main privacy interests: personal privacy, territorial privacy and informational privacy. Territorial/spatial privacy is rooted historically, legally and conceptually in property. There is a physical domain, specifically the home, wherein a claim to be left alone is recognized. Protecting beliefs, thoughts, emotions and sensations became the majority's focus in *Katz v. United States*: what is protected is people, not places.[92] Adopting *Katz*, Canada's *Hunter v. Southam Inc.*[93] "ruptured the shackles that confined these claims to property."[94] Thus, territorial/spatial privacy protects physical privacy, but it has been de-physicalized so that its protection extends to people. Personal privacy, like territory, is spatial: the person is deemed to be surrounded by a space but, unlike physical property, it is not necessarily bounded by tangible barriers. Its realm "transcends the physical and is aimed essentially at protecting the dignity of the human person."[95] Personal privacy can be said to relate to a sphere of the self—a zone of privateness surrounding the individual, which should not be invaded without justification by either unwarranted physical contact or by unwarranted observation. This zone of informational privacy also surrounds personal information and data about an individual.[96] Therefore, a rea-

---

90. *Supra* note 67.
91. *Supra* note 68.
92. *Katz v. United States*, 389 U.S. 347 (1967).
93. [1984] 2 S.C.R. 145, 11 D.L.R. (4th) 641.
94. *R. v. Dyment*, [1988] 2 S.C.R. 417 at 428, 55 D.L.R. (4th) 503 [*Dyment* cited to S.C.R.].
95. *Privacy and Computers: A Report of the Task Force Established by the Department of Communications/Department of Justice* (Ottawa: Information Canada, 1972) at 13, cited in *Dyment*, *ibid.* at 429.
96. *Dyment*, *ibid.* at 429-30.
97. The reasoning of Binnie J in *Tessling*, *supra* note 67 (S.C.C.), illustrates this point. By contrast, in the Court of Appeal, Abella JA (as she then was) evaluated the privacy issues from a territorial/spatial perspective with focus on safeguarding the home. As a result, she found a violation of s. 8. Binnie J takes a different perspective by evaluating the issue from an informational perspective with a focus on the nature and quality of the information. In the result, he finds no violation or unlawful intrusion.

sonable expectation of privacy may relate to a place or a space, to the person or to information. Whether or not a particular technological device violates privacy may depend on the court's analytical approach to assessing the privacy interest.[97]

In the case of thermal imaging of one's home, Binnie J noted that "the privacy interest is essentially informational (i.e., about the respondent's activities) but it also implicates his territorial privacy because although the police did not actually enter his house, that is where the activities of interest to them took place."[98] In the view of Binnie J, the distinction between territorial and informational privacy can be used to determine where one should draw the "reasonableness" line on the facts before the Court. He characterized the fly-over thermal imaging search as "an external search for information *about* the home which may or may not be capable of giving rise to an inference about what was actually going on inside, depending on what other information is available."[99] This shifts the focus from the individual's personal privacy to the privacy of the individual's home, construing what was gathered as just some information about the home, which could be combined with other information so as to draw inferences about activities in the home. Abella JA had characterized the thermal imaging activity differently: in her view, it amounted to a search of the accused's home.[100]

Binnie J concluded that there was no reasonable expectation of privacy with respect to the thermal image created by this technology.[101] Due to the nature of the current technology, the process produces information that is useful only when combined with other known information to draw inferences that might justify a search warrant. It is not sufficiently sophisticated to pinpoint or identify the particular activities giving rise to the heat signature. The decision of Binnie J placed great emphasis on the current state of the technology:

> External patterns of heat distribution on the external surfaces of a house is not information in which the respondent had a reasonable expectation of privacy. The heat distribution, as stated, offers no insight into his private life, and reveals nothing of his "biographical core of personal information." Its disclosure scarcely affects the "dignity, integrity and autonomy" of the person whose house is subject of the FLIR image.[102]

The Supreme Court's *Tessling* decision is disturbing in its implications for personal information privacy in general and for technologies such as RFID in particular. Like a thermal imaging camera, the reader of an RFID tag captures information that is not, in and of itself, personal information, but rather is information about the object in which the tag is embedded. Although the collector can match this information with

98. *Tessling, supra* note 67 at para. 24 (S.C.C.).
99. *Ibid.* at para. 27 [emphasis in original].
100. *Tessling, supra* note 67 at para. 76 (C.A.).
101. *Tessling, supra* note 67 at para. 63 (S.C.C.).
102. *Ibid.* [citations omitted].

other gathered data so as to allow the collector to draw inferences about a particular individual, the Supreme Court seems unwilling to make a privacy link between the collection of individual pieces of data and the practice of data matching and inference drawing. This approach is clear in other cases in the criminal context as well. In *R. v. Plant*, the Supreme Court held that electricity consumption patterns are not part of the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."[103]

While *Tessling* deals with the constitutional right to privacy in the form of the right to be free from unreasonable search and seizure, and thus would not be directly relevant in the context of private sector data collection and data matching, it does indicate an unwillingness to view individual data collection technologies as part of a larger system raising privacy concerns. The Supreme Court of Canada's approach is one of seeing no reasonable expectation of privacy, at least in the criminal context, with respect to information about one's clothing or other personal effects. One critic has noted that "stripped to their essence, these tests are fundamentally circular. They tell us that s. 8 will only protect the privacy of information if the information is inherently private."[104] This same author also identifies data mining as a major threat to privacy in the case of criminal investigations.[105] Another author argues: "When state surveillance uses ubiquitous technologies, constitutional privacy protection may be diminished as social conventions have already adapted to them."[106] It is significant that the more ubiquitous the use of a technology, the lower the threshold for a reasonable expectation of privacy. The widespread deployment of RFIDs in the retail sector could well have the effect of diminishing individuals' reasonable expectations of privacy with respect to the data transmitted by these devices embedded in their personal property.

Conceivably, the use by law enforcement officials of RFID readers to read information about a person's clothing or other personal effects, or about items stored within the individual's home, will simply be another form of data gathering through technology, which, viewed in isolation, does not trespass upon a reasonable expectation of privacy. This alone should be a matter of real concern for privacy advocates. When combined with the prospect that governments might introduce identification cards containing RFID chips embedded with personal information, or even drivers' licences equipped with RFIDs, the impact on citizen privacy could be intensified. A view of information collection that discounts the inferences to be drawn from that data raises concerns for the interpretation and application of *PIPEDA*.

---

103. [1993] 3 S.C.R. 281 at 293, 84 C.C.C. (3d) 203.

104. Renee M. Pomerance, "Shedding Light on the Nature of Heat: Defining Privacy in the Wake of *R. v. Tessling*" (2005) 23 C.R. (6th) 229 at 233.

105. *Ibid.* at 234-35.

106. James A.Q. Stringham, "Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core for Section 8?" (2005) 23 C.R. (6th) 245 at 251.

E. *RFIDS and Cookies: Analogous Technologies?*

Although RFIDs are relatively new, the privacy issues they raise are not necessarily novel. In some ways, the "cookie," a technology used in the online context, operates like an RFID tag. In this regard, lessons learned in relation to cookies and privacy may be relevant to RFIDs.

A cookie is a small amount of text or binary data that can be placed or "set" on a user's computer by the web browser on behalf of a website. Cookies may be either "session" cookies or "permanent" cookies. A session cookie is active only for a particular session (i.e. one visit to the website) and disappears after the session is complete. This sort of cookie may be useful in keeping track of the visitor's activity on the website for banking purposes and other transactions. A permanent cookie remains on the user's hard drive. Whenever the user returns to the site, the browser sends the cookie text to the site, thus linking the user to previous activities. Cookies may be used by a website to customize the view for returning visitors. In the simplest model, the website's host server may maintain a log that matches the stored text along with the user's IP address, thus linking the visitor to personal information. However, cookies may also be linked to other more precise personal information, which the user provides to the website.

Third-party cookies are cookies that are set on a web user's hard drive by a site other than the one being visited by the user. Commonly, third-party cookies are set by companies that monitor the website use patterns of individuals in order to tailor advertising content for them. The entire process of setting cookies, and the communication of cookie information, can take place without the computer user even being aware that this technology is active, or that it even exists.

In many ways, cookies are analogous to RFIDs from a privacy point of view. A cookie is a unique identifier that is automatically reported to the originating web server when it is revisited. While the unique identifier is not, in and of itself, personal information, the identifier can be collected and stored and can be matched with other data to create complex profiles. Cookies can be stored and read without consumers necessarily having any idea that this is taking place. Similarly, without labelling, an RFID can be placed on a product and can communicate the information stored on it to readers, all without the consumer's knowledge.

Cookies have been in use for some time now, and the privacy responses that have emerged may be useful in thinking about approaches to RFIDs. With respect to cookies, technology clearly plays a role in protecting privacy: web browsers can be configured to reject all cookies, to reject particular kinds of cookies or to prompt users to notify them that the site is attempting to set a cookie. These technological solutions raise some of the same concerns as technological solutions related to RFIDs: they depend on consumers being aware of the problem and they rely to some extent on consumers knowing enough to make use of the technology to prevent cookies from being stored on their computers. As with RFIDs, there are circumstances in which consumers can benefit from the use of cookies, and the functionality of many e-commerce websites depends on the ability to identify and track user

activity on the sites. Beyond basic functionality, cookies may offer users an enhanced experience. For example, an online bookstore can use cookies to create customer profiles that allow the site to recommend book purchases based on the online shopper's personal purchasing patterns, or based on the purchasing patterns of consumers who have bought products similar to those viewed or selected by the online shopper.

The EU Working Party on Data Protection acknowledges the parallels between cookies and some applications of RFIDs. Using the example of shopping carts enabled by tokens provided to consumers to be reused each time they visit the store, the Working Party notes that, as with cookies:

> . . . even if the individual is not immediately and directly identified at the item information level, he can be identified at an associative level because of the possibility of identifying him without difficulty via the large mass of information surrounding him or stored about him. Furthermore, the data collected from him can influence the way in which that person is treated or evaluated.[107]

While legislation in the United States has not expressly addressed cookies, it is generally considered that Canada's *PIPEDA* will apply to personally identifiable information gathered by the use of cookies.[108] Assuming that the information gathered through the use of cookies is "personally identifiable" information, a website privacy policy would have to state that information was being collected in this manner, and it would have to specify the purpose behind the collection. A cookie that reported only website traffic patterns would not be collecting personal information; a cookie that linked this traffic information to specific identifiable users would be. In this regard, the impact of *PIPEDA* on cookies is analogous to that on RFIDs: the information collected from the RFID is not personal information, it is information about a product. But it becomes personal information when it is matched with other data that can identify the purchaser of the particular product and link him or her to the purchase. Use of the technology, therefore, does not inherently give rise to the application of privacy legislation—it is only certain uses that bring the technology under the scope of the Act.

Under the EU *Directive on Privacy and Electronic Communications*,[109] the European Union has directly addressed the privacy concerns raised by the use of cookies. The preamble to this Directive recognizes that while cookies raise serious privacy concerns, they may also serve useful functions:

---

107. Working Document, *supra* note 15 at 7.

108. See e.g. Stephen Luciw, "Website Data Collection Raises Many Privacy Issues" *Lawyers Weekly* 21:7 (15 June 2001) 17.

109. EC, *Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, [2002] O.J. L. 201/37, online: EurLex <http://europa.eu.int/servlet/portail/RenderServlet?search=RefPub&lg=en&nb_docs=25&domain=Legislation&in_force=NO&year=2002&month=&day=&coll=JOL&nu_jo=201&page=37>.

> Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment.[110]

The passage goes on to indicate that this should be carried out in as user-friendly a manner as possible.

The European approach to cookies is interesting and instructive. Clearly, it is contemplated that general privacy principles can apply to this new form of technology and can provide some level of protection. However, the EU has seen fit specifically to address this technology in order to clarify certain issues in relation to its use. The *Directive on Privacy and Electronic Communications* states explicitly that, used properly, cookies may offer increased website functionality and should be permitted. However, it also makes clear that consumers need to be provided with specific information as to the purpose and function of cookies and that they should have the option of refusing a cookie.[111]

While it is true that in Canada, these norms could be derived from the interpretation of the basic normative provisions of *PIPEDA*, it is useful specifically to articulate that *PIPEDA*'s principles apply to data transmitted by RFIDs when it is matched with personally identifiable information, and to illustrate what the application of *PIPEDA* means in practical terms. Further, it may also be useful to articulate what compliance with individual principles will entail, for example, whether and what kind of notice is required when RFID tags are used, and whether or not the privacy principles require a realistic option for consumers to have tags removed or deactivated at the business's expense or initiative.

V. Conclusion

It is clear that although RFID technology is currently not widely used at a product level in commerce, it is already deployed in a variety of other contexts. It is also clear that the technology is becoming smaller and less expensive, and it will likely be economically feasible for manufacturers, distributors and retailers to deploy this technology at the product level in the near future. Considered at the level of individual product tagging for inventory control purposes, the privacy implications of this technology may seem trivial. However, it is clear that this technology can easily be used in conjunction with other data-bearing instruments (such as loyalty cards or

---

110. *Ibid.* at 39. Art. 6, *ibid.* at 43, sets specific requirements for the collection, use and disclosure of "traffic data," which would include data gathered through the use of cookies.

111. *Ibid.* at 39.

credit cards) to match product data with personal information in a way that allows for the compilation of highly detailed personal profiles of consumers. RFIDs also raise concerns in that the simultaneous development of private and public sector uses of RFIDs may lead to further privacy consequences: an RFID-enabled driver's licence may provide personal information about an individual that can be matched with other data from RFID tags contained on their person or among their personal belongings. The easy flow of information from the private sector to government is also a matter of concern, as data collected in the private sector may migrate into government hands without the data subject's awareness.

The relationship between public and private uses of RFID data poses a serious concern for personal privacy. Realistically, data collected in the private sector may easily migrate, often without consumer awareness, into the hands of government agencies or departments. The resultant problems are not unique to RFIDs, but where emerging technologies allow for increasingly detailed consumer profiling, increased public awareness of the potential scope and implications of private sector data collection is important. Consumers must know that beyond an organization's stated purposes for data collection, there may also be secondary uses that occur without their knowledge or consent. In turn, private sector organizations should limit their collection of personal data and their degree of consumer profiling in order to secure their customers' privacy within their organizations and with respect to potential secondary uses.

A number of technological measures can effectively protect personal privacy as it relates to RFIDs. RFID tags equipped with "kill switches" would allow deactivation, but, to the extent that any benefits attach to allowing tags to remain active, this option is impractical. In fact, the US bills that faced the stiffest opposition were ones that advocated, among other things, mandatory tag deactivation or removal. Allowing deactivation to be optional is not ideal either, as it places an onus on checkout clerks to inform customers about RFID tags and deactivation or, alternatively, on consumers to inform themselves. The problem remains that, short of owning and operating their own readers, consumers can never know for sure if a tag has truly been deactivated.

RFID tags can also be blocked. Tags do not communicate well through liquids or metals, so lining purses, bags or knapsacks and sheathing loyalty cards in aluminum, for example, will block signals from tags contained within and prevent surreptitious reading. Nonetheless, this measure places the onus on the consumer to take action to block tags and, in many cases, to spend money on blocking devices.[112] Further, the blocking of tags may ultimately also be regulated because of its potential to interfere with legitimate uses of RFIDs.

While it is reasonable to state that existing privacy norms and rules (most notably, the applicable private sector privacy legislation such as *PIPEDA*) should apply to RFID technology, it may not be sufficient simply to rely upon norms drafted in general terms for more conventional forms of data collection and data management. In many ways, RFID technology requires separate consideration, and distinct regula-

tions or guidelines may be necessary to fully address the implications of this technology. While RFID data may be matched with customer data in a way that parallels existing loyalty card practices, RFIDs raise distinct issues that need to be separately considered. Unlike product barcodes or loyalty cards, RFIDs can be read without the consumer's knowledge, both inside the store and after the consumer leaves the store. An RFID tag can conceivably be read by a wide variety of individuals in a variety of different contexts. The potential for surreptitious information gathering or surveillance gives unique dimensions to this inventory control device that set it apart from UPC bar codes.

Although RFID technology is not currently deployed as widely as was anticipated, it will likely not be long before RFID tags become ubiquitous. It is, therefore, crucial for legislators and privacy advocates to be proactive in addressing issues raised by RFID technology. 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. If formulated early enough, such guidelines may influence the development of the technology, in particular through technological configurations that support privacy initiatives. Also, it should not be overlooked that in some cases, the use of RFIDs may be regulated by legislation other than privacy legislation. For example, provincial consumer protection legislation could conceivably mandate that RFIDs, where possible, should be contained only in removable tags or removable packaging and should not be embedded in consumer items.[113] Enough is currently known about the technology to support sensible proactive regulation, and there is little excuse for Canadian policymakers at either level of government to ignore the implications for personal privacy of RFID technology in the commercial sphere.

---

112. See e.g. *Tag,You're It*, *supra* note 3 at 19.

113. In many of the US bills discussed above, the legislators opted for consumer protection-type measures, such as notice, labelling and mandatory deactivation requirements. These privacy-friendly measures could fall within the scope of provincial government jurisdiction over property and civil rights in the province.