An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies

by
Dr. Teresa Scassa
Dr. Theodore Chiasson
Professor Michael Deturbide
and Anne Uteck

Prepared for the Office of the Privacy Commissioner of Canada

April 28, 2005

Acknowledgements

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.

We would like to particularly acknowledge the Office of the Privacy Commissioner of Canada for the funding of this research. Thanks also to the Law and Technology Institute of Dalhousie University for its support.

Table of Contents

Introduction

Canadian consumers have become increasingly aware that personal information may be embedded into objects to facilitate aspects of commerce. Many use debit and credit cards to purchase goods and services, and most realize that the act of swiping such a card transmits information about them and their purchase to the credit card company or bank that provides the service. Consumers maintain some control over this personal information in choosing whether or not to acquire such a card, from which company and, to a limited extent, under which terms of service. Further, they choose where and when not to use these cards, how to store them and, ultimately to destroy them. The cards can be read only if swiped, and consumers control when that will happen.

What consumers are much less likely to be aware of is the existence and planned deployment of Radio Frequency Identification (RFID) tags. RFID technology, which dates back to the Second World War, is being refined and developed for use in a wide range of contexts. One such context is in every day commercial activities, where RFIDs are now being touted as a superior means by which companies can track inventory from the point of manufacture to the point of sale and beyond. Current deployment of RFIDs is at the crate or pallet level but, as the cost of the technology decreases, it will become feasible for each product or item in the economy to contain a unique identifier which can be used to track the product from point of manufacture, through shipping routes, from wholesalers to retailers, and ultimately into the hands of the consumer. In such a system, fungible goods are fungible no longer: each item has its own history separately traceable and identifiable from all other like items. Significantly, the information embedded in this tiny tag can be retrieved by anyone with a retrieval device, at any point in the item's lifespan. Conspicuous "swiping" is unnecessary; a reader can pick up the signal from an RFID at some distance, through a variety of materials, including shopping bags and clothing. The technology has potential uses beyond inventory control and may be integrated with broader commercial data collection activities. As a result, it has attracted the attention of privacy advocates. What was conceived of as a superior inventory control device has the potential to become a powerful data-matching technology and, ultimately, a technology of surveillance.

Recent media attention has focused on consumers' concerns about the uses many private sector companies will make of RFID technology, and especially the ways in which it could be used to satisfy the ever-increasing demand for personal information in exchange for goods and services in the ordinary retail marketplace. However, privacy concerns extend far beyond the commercial context. RFIDs have virtually limitless applications and are being considered for use or are already deployed in a range of contexts from the delivery of health care, the management of library collections and the control of the safety of food supplies, to employee monitoring or government surveillance as a part of national security initiatives.

The Underlying Technology

One of the difficulties in coming to terms with RFID technology and in mounting any kind of privacy response is the very broad range of technology encompassed by the term "RFID". The simplest RFID tag may pose relatively little threat to personal privacy but the more sophisticated tags can store significant amounts of data, including biometric information, and may have both read and write capability. Further, RFID technology is only one part of the privacy equation. The ability to match even small amounts of data from RFID chips to already collected stores of personal information or to data simultaneously collected from customer loyalty or credit cards gives new dimensions to privacy concerns. To the extent that databases of consumer personal information are vulnerable to illicit access, any technology that increases the amount and detail of that information in the hands of third parties is also a concern. To properly identify and address the privacy implications of RFIDs, the technology needs to be defined and understood. This is the objective of Part I of this Report.

Use and Deployment of RFIDs

It is unlikely that RFID technologies will be derailed; their use in consumer goods can be expected to expand in the near future; not just in volume, but in variety of applications. In fact, a European Union Working Party on Data Protection has stated that RFID technology is expected to be "one of the main 'bricks' of the future ambient intelligence environment."[1] Currently, RFIDs are used in "speed passes" for highway tolls and toll bridges.[2] They have been used on a trial basis with respect to a range of consumer items including razors,[3] clothing[4] and tires,[5] and major retailers such as Wal-Mart[6] are considering them for adoption across a broad range of consumer goods. RFID technology is deployed in public libraries[7] and may someday be used in relation to food products,[8] and even currency.[9] Their current deployment as a means of ensuring health

---

[1] Article 29 Data Protection Working Party, "Working document on data protection issues related to RFID technology", January 19, 2005, 10107/05/EN. Online: http://www.europa.eu.int/comm/privacy (Working Document), at 3.

[2] Such tags are in use on the toll bridges across Halifax Harbour (online: http://www.macpass.com/). They are also in use on the 407 toll highway north of Toronto (online: http://www.407etr.com). Their deployment elsewhere is widespread. See online: http://www.highway61.com/Top/Recreation/Roads_and_Highways/Toll_and_Automated.

[3] RFID Journal, "Gillette Confirms RFID Purchase", January 7, 2003. Online: http://www.rfidjournal.com/article/articleprint/258/-1/1/.

[4] Electronic Privacy Information Center, *supra* note 3, at 4.

[5] *Ibid*.

[6] ECT News Syndication Desk, "Wal-Mart's Muscle Advancing Use of RFIDs", July 21, 2004. Online: http://www.crmbuyer.com/story/35006.html.

[7] David Molnar and David Wagner, "Privacy and Security in Library RFID Issues, Practices and Architectures", June 8, 2004. Online: http://www.cs.berkeley.edu/~dmolnar/library.pdf. See also: Information and Privacy Commissioner of Ontario, "Tag You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology", February 2004. Online: http://www.ipc.on.ca/docs/rfid.pdf (Tag You're It).

[8] Jonathan Collins, "Safeguarding the Food Supply", RFID Journal, 2004. Online: http://www.rfidjournal.com/article/articleprint/691/-1/1/.

security in hospital systems[10] and their possible deployment for public health or security purposes raise unique concerns.[11] The present use and deployment of RFID technology is explored in Part II of this Report.

Privacy and RFID Technology

RFID technology is of significant relevance to a growing number of powerful interest groups from industry to commerce, and to governments at all levels. They will exert enormous pressure to advance the development and deployment of these technologies. Companies eager to benefit from RFID commercial applications such as inventory control, can justify their investment in the technology on that basis alone,[12] not to mention the use of RFIDs to facilitate customer returns, warranty use, and the development of so-called "smart appliances" [13] and other RFID enabled technology. At the same time, RFIDs allow businesses to collect significant amounts of data about consumers and their practices, and then to match that data with other data about specific consumers, potentially creating complex profiles of identifiable individuals. In addition, government may show substantial interest in either requiring the use of RFID technology in contracts with their suppliers[14] or in the regulation of certain sectors.[15] Since September 11, 2001, growing reliance of governments on data collected in the private sector raises concerns that information gathered in one context may be surreptitiously used in another.

The rapid development and deployment of RFID technology is troubling from a privacy point of view. Privacy law can either be formative or reactive in addressing this issue. In other words, legal privacy norms can be developed in advance of the technology so as to direct the development and deployment of conforming technologies, or they can be developed in response to already deployed technology. While existing data protection legislation, such as the *Personal Information Protection and Electronic*

---

[9] Junko Yoshida, "Euro Bank Notes to Embed RFID Chips by 2005", EETimes, December 19, 2001. Online: http://www.eetimes.com/story/OEG20011219S0016 (Euro Bank Notes).
[10] Electronic Privacy Information Center, "Radio Frequency Identification (RFID) Systems", Washington, D.C., August 11, 2003, at 3. Online: http://www.epic.org/privacy/rfid/.
[11] See "Tag, You're It", supra note 7, at 18.
[12] *RFID: Applications and Implications for Consumers: A Workshop Report from the Staff of the Federal Trade Commission*, March 2005. Online: http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf (*FTC Report*).
[13] A "smart appliance" is a household appliance such as a refrigerator or washing machine that is equipped with an RFID reader. A smart fridge, for example, would be able to read a tag on a carton of milk, and could alert the owner of the appliance to the fact that either the milk was about to pass its best before date, or that the carton is almost empty.
[14] The U.S. Department of Defence has implemented a policy requiring the use of RFIDs as a means of improving the tracking of supplies. See: Matthew French, "For DOD logistics tags are it!", July 27, 2004, FCW.COM newsletter, online: http://www.fcw.com/fcw/articles/2003/1103/pol-dod-11-03-03.asp.
[15] For example, the European Union is moving forward with plans to embed RFIDs in currency notes. See Euro Bank Notes, *supra* note 9. In the United States, the use of RFIDs is being implemented by the Department of Agriculture as a means of improving the traceability of meat products. See: USDA, Food Safety Research Information Office, "Animal Identification Pilot Program", March, 2004. Online: http://www.nal.usda.gov/fsrio/research/fsheets/fsheet12.pdf.

Documents Act (*PIPEDA*)[16] may well be interpreted to apply to RFIDs in many circumstances, other issues raised by RFIDs might be better addressed by more technology-specific regulation. For example, failed bills in the U.S. have proposed that RFIDs be removed or deactivated at the point of sale.[17] Other proposals have suggested control measures linked to the operation of the technology itself. To the extent that such measures would affect the development and deployment of the technology, they would need to be in place prior to any wide scale deployment or use of RFIDs in a commercial context. Once the technology becomes commonplace, it will be much harder to impose technical or practical limitations.

Privacy Initiatives at Home and Abroad

Part III of this report explores national and international privacy initiatives in relation to RFIDs with a view to identifying the range of current normative responses to the emerging technology. We will consider legal initiatives in other jurisdictions, as well as activity by consumer and privacy activists. Part IV examines the current Canadian legal landscape. Using *PIPEDA* as a focus, we will consider the extent to which existing private sector privacy legislation in Canada sets norms that are useful or practical in addressing RFID technology, and we will identify any gaps in the current legislation.

While this report will focus on private sector use and deployment of RFID technology, some attention will be paid to the broader public context. The adoption or use of RFIDs by government departments and for government programs will support private sector deployment of these technologies, and may play a role in limiting government response. Further, in the post-September 11 environment, the potential for personal information to migrate with relative ease from the private sector to government officials adds a public dimension to private sector developments. Therefore, this report will explore the use of RFIDs in the contexts of employment and law enforcement.

Conclusions and Recommendations

RFID technology is already so well advanced that it is impractical to speak of banning or unduly limiting it. Indeed, it represents a potential cost savings to the commercial sector through dramatically improved inventory control and management, and through reductions in inventory shrinkage through loss and theft. Likely we will have to live with and adapt to the growing use of these technologies, so it is important to consider the means by which their impact on personal privacy can be minimized. In the final part of this report, we recommend legal and policy options for addressing the privacy risks posed by RFIDs.

---

[16] S.C. 2000, c. 33. Other private sector personal data protection legislation exists in Canada. See, for example: Quebec's *Act respecting the protection of personal information in the private sector*, L.R.Q., chapter P-39.1; British Columbia's *Personal Information Protection Act*, S.B.C. 2003, c. 63; and Alberta's *Personal Information Protection Act*, S.A. 2003, c. P-6.5. It is beyond the scope of this report to consider each of these statutes in addition to *PIPEDA*.

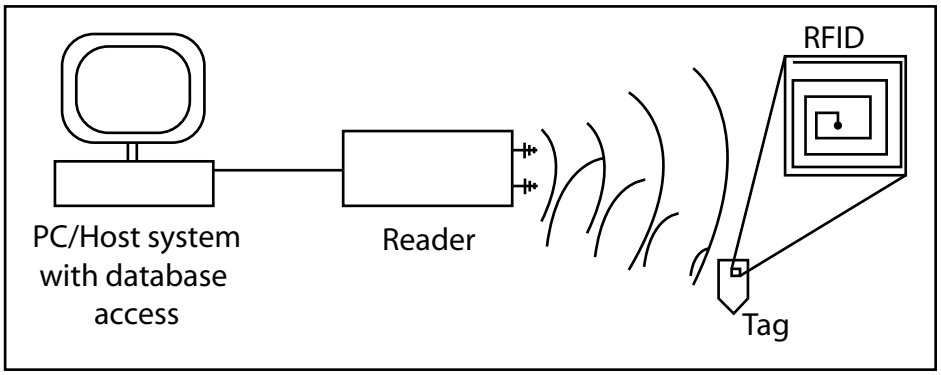
[17] See, for example, New Mexico H.B. 2003, and South Dakota H.B. 1136, discussed *infra* in Part III(2).

Part I – Defining RFID Technology

The term "radio frequency identification" (RFID) describes a range of technologies with widely differing privacy implications. While in general terms, an RFID uses radio frequencies to communicate information about the item in which it is embedded, the types of RFIDs are many.

Radio frequency identification was first deployed during the Second World War, when the Royal Air Force used "Identify Friend or Foe", or IFF to reduce incidents of friendly fire.[18] Since then, the uses of radio frequency identification have expanded to encompass diverse applications. Steady advances in microchip design has reduced the of RFID chips as well as their cost, now as low as $0.20 for bulk purchases.[19] Eventually the price will be low enough to render RFIDs a viable alternative to present-day UPC barcodes. Barcodes currently cost about $0.02 US to produce in bulk, but RFIDs could be considered cost-competitive at $0.05 US due to the additional functionality and anticipated resulting cost savings of an RFID-based inventory control system.

An RFID system has three integral parts: a tag, a reader and a database. The tag consists of an antenna attached to a micro-chip. 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 have a range of up to several kilometers, whereas the range for passive tags is restricted to less than 5 metres. Active tags are also on the order of one thousand times more expensive than passive tags, costing as much as $200 US each. 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. 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.



[18] Royal Air Force. History: 1940. http://www.raf.mod.uk/history/line1940.html.
[19] RFID Journal FAQ. Online: http://www.rfidjournal.com/faq/20/85.

As stated, passive tags have no battery and must receive energy from the field generated by the reader. They also rely on the reader field as the communications channel to receive and send messages. Passive tags can be classed as near field or far field tags, based on the way in which they receive energy from the reader field. Near field tags operate in the low frequency (LF) or high frequency (HF) spectrum, and have a very limited effective range (less than 1 metre). The near field tags induce power from the magnetic field of the reader. In contrast, ultra high frequency (UHF) tags (which are likely to see use in the retail context) use the far field (or electric field) generated by the reader to receive power, and use backscatter reflection by coupling with the electric field. While UHF passive RFIDs have a maximum range of about 5 metres, legislative controls on UHF spectrum further restrict the maximum power a reader can emit, resulting in a range limitation of under 3 metres in some jurisdictions.

Table 1. Reader ranges and typical applications for types of passive RFID tags.

	LF	HF	UHF	Microwave
Typical Read Range	Less than ½ metre	Approximately 1 metre	Approximately 4 – 5 metres	Approximately 1 metre
Application areas	Access control, animal tagging	Access control, smart cards, retail item tagging, libraries, transport	Speed passes, supply chain (pallet tagging)	Speed passes
Comments	Large antenna (high cost)	Smaller antenna (lower cost than LF tags) Most widely deployed tags	IC advances yielding cheap production cost, likely to replace HF tags for retail item tagging	Highly susceptible to interference, Not applicable for retail item tagging

The reader in a passive RFID tag system has to generate a relatively strong signal to ensure the tag will have sufficient power to operate and communicate back to the reader. Thus, the signal from the reader could be detected from a distance, typically up to 100 metres for a UHF system. When a reader produces a signal, any tag within range will "power up" and begin a handshake process with the reader. If more than one tag responds, a collision will result.

One technique for resolving collisions is the "tree walking" protocol, which makes the reader process one bit of the tag's ID at a time. When a collision occurs, the reader begins the protocol by transmitting a request to the tags asking that only tags with a "0" in their first bit respond. If more than one tag responds, another collision will occur, and the reader will proceed to ask for tags with an ID that starts with "00". Eventually, either one tag or no tag will respond to the reader's request. If only one tag responds, the tag has been "singulated" and the reader and tag can communicate. If no tag responds, the reader will change the last "0" bit to a "1" and try again (i.e., ask for all tags

whose ID starts with "01" to respond). A fairly straightforward algorithm can be used to ensure that the reader will eventually "singulate" all tags in range, and so be able to communicate with each tag in turn.

While the signal from a tag cannot be detected by a distant eavesdropper, listening to one side of the conversation can be enough to decode what is happening. This is particularly problematic when the "tree walking" protocol is employed. Although an eavesdropper cannot hear the responses from the RFID tags, it can easily detect each bit transmitted by the reader querying the tags, thus constructing the complete ID of the RFID that is responding to the reader.

One way to overcome this eavesdropping problem is to modify slightly the algorithm used by the reader, so that it queries tags within range for their "next bit" and transmits only a differentiating bit when bit collisions occur. In this way, an eavesdropper can obtain only those bits that induced a bit-wise collision, which will likely occur only in the high order bits of the tags. Alternative algorithms for overcoming this problem are a subject of research at the EPCglobal (formally known as the MIT Auto-ID centre).[20]

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.

Because RFIDs encompass many technologies that have evolved independently and that serve different application functions, a variety of standards have resulted. This is further complicated by the differences in frequency spectrum allocations in different regions. The lack of a global RFID standard is seen as a major barrier to RFID adoption and deployment. EPCglobal has produced the Electronic Product Code (EPC) Tag Data Standards,[21] which, if adopted, could serve as a standardized way of representing data within an RFID tag. Since WalMart has adopted this standard, it will likely become the *de facto* standard for inventory control and supply chain management systems.

Although RFID tags used in the consumer context have been compared to the UPC barcode, there are key differences between them. For one thing, RFIDs are capable of uniquely identifying each consumer item, while barcodes are more generic. Further, the UPC barcode must be held close to a reader to be scanned, and only one item at a

[20] Weis, Stephen August, 2003, "Security and Privacy in Radio-Frequency Identification Devices", Masters Thesis, MIT. Online: http://theory.lcs.mit.edu/~cis/theses/weis-masters.pdf.
[21] EPC Tag Data Standards Version 1.1 Rev.1.24, standards specification, April 1, 2004. Online: http://www.epcglobalinc.org/standards_technology/ EPCTagDataSpecification11rev124.pdf.

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 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. [22]

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.[23]

RFIDs vary in terms of how they are regulated, how much information they can store and how they might be disabled. Low and high frequency RFID tags can be used without a licence anywhere in the world, unlike UHF tags, for which there are no global standards. Instead, each country sets its own limits for UHF frequencies that may be used without licence. High frequency tags have a greater transmission range than low frequency tags, but they "are less likely to pass through nonmetallic materials than low-frequency tags are and generally require an unobstructed path to the transceiver."[24] 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.

Passive RFID tags can be designed with a "self destruct" function to be activated at the time a product is purchased. The EPCglobal standard includes provision of a kill command (including an 8-bit password needed to activate self-destruction). While such an approach could help allay privacy concerns, retailers or consumers may want to keep their tags alive to facilitate returns and to allow communication with smart appliances. Moreover, supplying kill switches does not guarantee that all tags will be disabled. Without a tag reader (relatively expensive at $200 to $2000 U.S.), a consumer cannot check to see that a tag has been disabled and must trust that the retailer has done the job.

In addition to kill switches and metallic blockers, RFIDs may be silenced using a blocking tag. This special-purpose RFID tag responds to a reader's signal by broadcasting so much information that other tag responses are drowned out. While blocking tags exist,

---

[22] Michael Burns, "Retailers discover venerable radio technology", The Bottom Line, Vol. 20, No. 15, mid-November 2004.

[23] Information and Privacy Commissioner, Ontario, "Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology", February, 2004, at 12. Online: http://www.ipc.on.ca/docs/rfid.pdf.

[24] Harold E. Davis and Michael S. Luehlfing, "Radio Frequency Identification: The Wave of the Future", Journal of Accountancy, November 2004, 43-49, at 46.

they are of necessity more expensive, as they need a power source in order to generate sufficient “noise” that all other tags are drowned out. Further, deployment of blocking tags would put the onus on the consumer to be aware of RFID technology and actively to take steps to prevent the loss of their privacy. Use of blocking tags might also be banned through legislation, considering their potential to inhibit legitimate inventory control system uses of RFIDs.

Part II – Deployment of RFIDs

In Part II we present an overview of how both private and public sectors have implemented RFID technology, which is indicative of its overall development and deployment. In addition, we examine unique and interesting RFID uses that might not fit perfectly into the strict private or public division. Since RFID technology is still relatively new and the complete range of its potential is not yet fully known, it is important to examine proposed and speculative uses; the latter of which can be most troubling from a privacy perspective.

A recent study[25] 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. The purposes cited for this implementation included shipping, and tagging and tracking of pallets in the loading and unloading within distribution centres.

1. Commercial Uses

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,[26] could give companies constant awareness of where goods and shipments are, and immediate knowledge of delays.[27] The recent Federal Trade Commission Staff Report on RFIDs anticipated major cost savings from the use of RFIDs in the supply chain.[28] 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.[29] Gas stations have now made the purchase of gasoline so easy that customers simply wave an RFID-equipped key chain at a reader to obtain a receipt and drive away. Clearly the potential of RFIDs as tools for organizing and monitoring the supply of goods and services is extensive.

The next phase of private sector RFID deployment is widely 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,[30] although pilot

---

[25] Deloitte Canada. "Nearly half of Canadian retail and consumer corporations anticipate using RFID technology within two years – reveals Deloitte study", November 11, 2004. Online: http://www.Deloitte.com/dtt/press_release/0,1014,cid%3D65794%26pv%3DY,00.html.
[26] Jeffrey Silva, "ACLU says RFID in passport leaves Americans vulnerable", November 29, 2004. Online: http://rcrnews.com.
[27] Barnaby J. Feder, "RFID: Simple Concept Hobbled by Daunting Complexity", New York Times, November 21, 2004.
[28] *FTC Report*, *supra* note 12, at 9.
[29] Andy McCue, "Heathrow Airport to get taxi-tracking RFID system", Silicon.com, February 22, 2004.
[30] *FTC Report*, *supra* note 12, at 11.

projects are under way in various contexts. Gillette has, for example, experimented with "smart shelves"[31] which are equipped with a reader, while each individual item 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 hand-held 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.[32]

Retailers are also interested in how RFIDs could improve efficiency of operations, customer service, or 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.[33] 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.

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 heavily browsed, and so on. Privacy advocates have raised concerns about this kind of monitoring, even though it is not necessarily tied to personal information of particular consumers.

Customer loyalty cards are a different matter. Cards embedded with RFID tags may 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 without the cardholder's knowledge. Again, shoppers could be monitored to ascertain their habits or preferences, regardless of whether they actually make any purchases on any given visit to

---

[31] Carl Zetie, "RFID: The Good, the Bad and the Ugly", Information Week, December 15, 2003. Online: http://www.informationweek.com/story/showArticle.jhtml?articleID=16700081. See also: Mark Baard, "Lawmakers Alarmed by RFID Spying", Wired News, February 26, 2004. This experiment ended prematurely when it was discovered that Gillette was also photographing customers using hidden cameras as part of the experiment.

[32] 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. Online: U.C.L.A. Journal of Law and Technology http://www.lawtechjournal.com/articles/2004/05_041220_brito.php.

[33] 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.

the store.[34] RFIDs may be used to detect shoplifting, with significant advantages over current systems of in-store theft detection.[35]

RFIDs also offer significant health and safety benefits to consumers as well as industry. RFID tags attached to food items could allow for a much more specific recall of goods if it is found that a particular batch of food product is contaminated.[36] With perishable items, tags could inform on-shelf readers that the product has reached its expiry date, thus preventing consumers from unwittingly purchasing items past their prime that have been inadvertently left on the shelves.

On the more invasive side, one U.S. amusement park sought to use RFID chips in bracelets to offer parents a measure of security if their children should become lost while at the park[37] and subcutaneous RFIDs have already been used for the identification of lost pets.[38]

2. 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. So 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 U.S. 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."[39]

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 is 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

---

[34] *Working Document*, *supra* note 1, at 5-6.
[35] Potential anti-theft applications are numerous. In one pilot project, a U.K. supermarket used RFID tags on high priced items to trigger cameras when the items were removed from shelves. The images were destroyed if the tagged item was actually purchased. See: Scarlet Pruitt, "Privacy concerns surface at CeBIT RFID debate", Computer Weekly, March 22, 2004.
[36] See, for example, Laurie Sullivan, "PLM Software Has a Role in Food Safety", Information Week, January 12, 2004. Online: http://www.informationweek.com/story/showArticle.jhtml?articleID=17300286.
[37] Chet Brokaw, "House panel rejects measures to regulate implanted microchips", Associated Press, January 31, 2005.
[38] Alorie Gilbert, "Implanted ID chip finds way into ER, bars", CNETNews.com, January 21, 2005.
[39] *FTC Report*, *supra* note 12, at 12.

clothing that 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.[40] 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 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.[41] 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."[42] RFIDs can take this a step further: 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.[43]

3. Employee Surveillance

One potential use of RFIDs in enhancing business efficiency should not be ignored: employee monitoring and tracking systems. RFIDs in employee badges or uniforms, for example, could be used to track the location of the employee within the employer's premises, to measure how much time the employee spends in the washroom or on breaks, and even to record when an employee has left the premises.[44] This is hardly a science-fiction scenario; employee monitoring is a frequent practice and an established element of business efficiency programs, and technology is used to enhance the employer's employee monitoring abilities.[45] Chips on badges or in uniforms are only one manifestation of the potential use of RFIDs. Subcutaneous chips have already been contemplated for use in the U.S. military, and for police officers.[46]

4. Public Health and Safety

In some cases, industry concerns dovetail with government regulatory interests. This is particularly true in the context of heavily regulated aspects of the food supply system. RFIDs are being considered for use in tracking beef cattle in both Canada and the United States, particularly in the wake of recent incidents involving mad cow disease.

---

[40] *Ibid*., at 15.
[41] Katherine Albrecht, "Supermarket Cards: The Tip of the retail Surveillance Iceberg" (2002) 79 Denv. U.L. Rev. 534.
[42] *Ibid*., at 535.
[43] Jo Best, "Supermarket cans RFID trials in Germany", Silicon.com, March 1, 2004.
[44] In one instance it was reported that RFID tags were placed in 80,000 employee uniforms at the Star City Casino in Sydney Australia, as a means to control employee theft. See: Scott Granneman, "RFID Chips Are Here", June 27, 2003, The Register. Online: http://www.theregister.co.uk/2003/06/27/rfid_chips_are_here/print.html.
[45] E. Anne Uteck, *Electronic Surveillance and Workplace Privacy*, unpublished LL.M. thesis, 2004.
[46] Geoffrey James, "Can't hide your prying eyes", Computerworld, March 3, 2004.

Similarly, the U.S. Animal Health Association is working with other parties, including the U.S. Department of Agriculture and farming corporations, to employ a plan to track all cattle and identify all premises and herds potentially exposed to an animal disease within 48 hours of discovery. In this system, all cattle would have unique RFID numbers for intrastate commerce by July 2006.[47]

Concerns about the increasing problem of counterfeit drugs in the United States is driving the adoption of RFID technology in the pharmaceutical industry. A U.S. Food and Drug Administration Report on "Combating Counterfeit Drugs"[48] identified the need to create a comprehensive system of modern protections against counterfeit drugs, using new technologies such as RFIDs.[49] Current plans are to tag the large bottles of tablets used to stock pharmacies, but use of RFIDs in individual packages provided to consumers is being contemplated.[50]

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 home-owner 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.

The immediate applications in merchandise tracking systems are less obviously a privacy concern.[51] Many of the above applications for RFIDs are a long way from deployment, although all signs point to the eventual ubiquity of RFIDs in consumer items and in a variety of contexts. Companies are permitted, and indeed encouraged, to find more efficient ways of tracking their inventory and supplies, especially if these savings are passed along to the consumer. As long as the information on these tags is restricted to product information, and it appears that this is the current focus of the technology, there is no privacy concern. However, it is evident that the line between potential and current commercial uses of RFID technology is blurring and, indeed, anticipated deployment dates for more widespread RFID tagging are rapidly approaching.

---

[47] A major issue and obstacle to both the US and Canada's cattle RFID goals is the cost to ranchers of purchasing tags for every animal as well as readers and software. "Can RFID Protect the Beef Supply", RFID Journal, January 5, 2003. Online: http://www.rfidjournal.com/article/articleprint/722/-1/1/

[48] U.S. Food and Drug Administration, "Combating Counterfeit Drugs", February 2004. Online: http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html.

[49] Lester M. Crawford, "Remarks of the Acting FDA Commissioner: FDLI's 47th Annual Conference" (2004) 59 Food Drug L.J. 201, at 205.

[50] *FTC Report*, *supra* note 12, at 10.

[51] *Ibid*., at 13, noting "some consensus" from their workshop that RFIDs do not jeopardize consumer privacy.

5. Public Sector Use of RFIDs

The potential for government use of RFIDs is very broad, in part because of the many roles that governments play in society. Governments have their own supply chains and, in that context, RFID use may be comparable to pallet-level tracking in the private sector. Governments may seek to use RFIDs as part of regulatory schemes, in the delivery of service, or in relation to government employees, such as police officers or military personnel. However, as issuers of identity and other official documents, governments are contemplating deployment of larger and more powerful RFIDs.

In the U.S., it has been observed that "there are two big drivers of RFIDs, one of them is Wal-Mart, the other is [the Department of Defense] DOD."[52] RFID technology is being considered for use in inventory control, whether in the supply chain generally or in the tracking of equipment used on the front lines. [53] RFIDs are also being considered for use in the United States' border management system.[54]

RFIDs are being used on Canadian and American highways in a pre-paid system of highway or bridge tolls,[55] and, in Florida, an RFID system measurees the travel time of motorists.[56] In public transit systems, users pay by waving an RFID-equipped card before a reader at a subway turnstile,[57] a use that is particularly problematic from a privacy standpoint. Data gathered through such a system could provide detailed information about the travel patterns of individual customers.

Virginia is among the first states to explore the idea of creating a smart driver's license, which may eventually use combined RFID tags and biometric data, such as fingerprints or retinal scans[58] to make it easier for police and government officials to track fines and driving records. However, this is very preliminary.

The more complex RFID chips are capable of storing biometric information, and of having new information written to them. These types of chips are of significant interest to governments in an era of heightened security. The Transport Security Administration in the U.S. is considering the use of RFIDs on boarding passes to track airline passengers, and a number of jurisdictions are seriously discussing RFIDs as a mandatory part of travel documents such as passports.

---

[52] "The Next Big Thing For Government", Online: http://www.csa-dc.org/publications-press/ppc_update/10-1-04/4.htm

[53] Bob Brewin, "RFID Spreads With Feds", Federal Computer Week, September 29, 2004. Online: http://www.fcw.com/article84223-09-29-04-Web.

[54] Press Release, Department of Homeland Security, "Homeland Security Announces Plans to Test Radio Frequency Technology at Land Borders", January 25, 2005. Online: http://www.dhs.gov/dhspublic/display?content=4308.

[55] See http://www.macpass.com and http://www.407etr.com

[56] RFID Journal "RFID Drives Highway Traffic Report" Online: http://www.rfidjournal.com/article/articleprint/1243/-1/1/

[57] Washington Area Metropolitan Transit Authority online http://www.wmata.com/riding/smartrip.cfm.

[58] Mark Baard, "RFID Drivers Licenses Debated", Wired News, October 6, 2004. Online: http://www.wired.com/news/privacy/0,1848,65243,00.html

Governments are assessing the feasibility of RFID use in tracking currency and controlling money laundering and theft. The possible use of RFID tags in Euro notes has been the subject of some discussion as a means of addressing counterfeiting concerns.[59] Some public libraries have also begun to use RFIDs as an improved means for libraries to track books, but privacy advocates concerned about the capacity to link an individual's personal information to their reading choices. The Office of the Information and Privacy Commissioner of Ontario has issued a policy document aimed at library uses of RFIDs,[60] and a failed bill on RFIDs in California also attempted to address their use in the public library context.[61]

There are also reports that RFIDs are being considered for use in children either as a response to concerns about child abduction,[62] or as a means of ensuring safety through tracking their location. For example, it was reported that a school in Wales was considering tagging children to prevent them from leaving school without detection.[63] A similar use of RFIDs was reported to be contemplated in a California school.[64]

[59] "New rumours about spy chips in Euro notes", EDRI-gram, January 26, 2005. Online: http://www.edri.org/edrigram/number3.2/rfid.
[60] Information and Privacy Commissioner of Ontario, *Guidelines for Using RFID Tags in Ontario Public Libraries*, (June 2004). Online: Information and Privacy Commissioner/Ontario http://www.ipc.on.ca/docs/rfid-lib.pdf. (*Ontario Library Guidelines*)
[61] U.S., S.B. 1834, An Act to add Ch. 22.7 (commending with Section 22650) to Division 8 of the Business and Professions Code, relating to Business, 2003-04, Reg. Sess., Cal., 2004, s. 22650.
[62] Becky Blanton, "Big brother or the mark of the beast?", Sierra Times.com, January 27, 2005. Online: http://www.sierratimes.com/03/10/28/article_tn_blanton.htm.
[63] Andy McCue, "School children to be tagged in safety trial", Silicon.com, January 21, 2005.
[64] Dana Hull, "School first in state to track students with radio ID tags", February 9, 2005, San Jose Mercury News (California). Online: http://www.mercurynews.com/mld/mercurynews/living/education/10853541.htm.

6. RFIDs in Health Care

The potential use of RFIDs in the delivery of health services extends from hospital to home care. Subcutaneous RFID chips could well replace the hospital bracelet,[65] tracking patients in addition to inventory and equipment in medical facilities. RFIDs may also facilitate the care of elderly patients. Some suggest that seniors may be able to remain in their homes longer and with greater autonomy if RFIDs embedded in everyday objects were combined with readers placed strategically through the home to allow health care workers at a remote location to monitor whether elderly "patients" were preparing meals, using bathroom facilities, attending to personal hygiene and so on. It has been argued that the benefits of being able to live longer in one's own home outweigh the burdens of such close surveillance.[66]

7. 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.[67] 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.[68] RFIDs in the clothing or personal effects could be used to assist in 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.

8. Illegitimate Uses

Undoubtedly, RFIDs could be deployed in ways covert and illegitimate. It is technically possible, for example, for someone to surreptitiously plant an RFID chip on someone else's clothing or person through a casual slap on the back or a "bumping" incident in a crowded public space. The chip, with its unique identifier, could then be

---

[65] In October 2004, the U.S. Food and Drug Administration approved the "Verichip" for subcutaneous implantation in humans. The chip can be linked to a patient's medical records.
[66] *FTC Report*, *supra* note 12, at 11.
[67] See Jennifer Stoddart, Privacy Commissioner of Canada, "Privacy in a New Era: Challenges, Opportunities and Partnerships", Public Voice Symposium, September 13, 2004. Online: http://www.privcom.gc.ca/speech/2004/sp-d_040913_3.asp.
[68] See, e.g., Mark Baard, "Watchdogs Push for RFID Laws", Wired News, April 5, 2004. Online: http://www.wired.com/news/privacy/0,1848,62922,00.html.

used to track the specific individual. A more commonly cited concern is that potential criminals could scan one's home with a hand held reader to detect the nature and value of goods stored within. Other forms of surveillance may also be possible. For example, if RFID tags are used to store personally identifiable information, 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."[69]

[69] *Working Document*, *supra* note 1, at 6.

Part III – Overview of Developments Outside of Canada

Before conducting an assessment of data protection 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 the European Union.[70]

1. International

In November 2003, a Resolution on Radio-Frequency Identification[71] was adopted at the 25th International Conference of Data Protection and Privacy Commissioners. The Resolution noted that although "this technology can have positive and benign effects, there are also potential privacy implications."[72] 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."[73] The potential of this technology to be used to link product information with existing databases was emphasized.

The Resolution 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 are as follows:

> 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.[74]

---

[70] 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 office of the Information Commissioner of the United Kingdom has published reports on several topics that address RFIDs, although they do so in a relatively minor manner. (See, for example: "Public Attitudes to the Deployment of Surveillance Techniques in Public Places", March 2004: online: http://www.informationcommissioner.gov.uk/cms/DocumentUploads/cctv%20report.pdf; and "Technology Development and its Effect on Privacy and Law Enforcement", February 2004, online: http://www.informationcommissioner.gov.uk/cms/DocumentUploads/report%20parts%201&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", February 9, 2005, online: http://www.privacy.org.nz/top.html.)

[71] Online: http://www.privacyconference2003.org/resolutions/res5.DOC.

[72] *Ibid*.

[73] *Ibid*.

[74] *Ibid*.

The Resolution also noted that the "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."[75] 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 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.

[75] *Ibid*.

2. 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 RFIDs and privacy in the U.S. These concerns have led to the introduction of several bills at the state and federal level which 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 significant number remain under active consideration.[76]

At the federal level, Bill 4673, introduced in the House of Representatives in June 2004 required warning labels to be placed on any consumer products containing RFID devices. Furthermore, the label would inform consumers that the device could be used in tracking the product before and after purchase. The bill 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. The bill defined an RFID as a device "that acts as a transponder and enables data to be transmitted through a radio signal to a receiver and that is placed in a product to provide identification, tracking, or other information about the product or the consumer of the product."[77] Clearly this bill was focused on the deployment of RFIDs in the consumer context.

A bill introduced in the Missouri State Senate, entitled the RFID Right to Know Act of 2004,[78] defined RFIDs as "technologies that use radio waves to automatically identify individual items". It required mandatory labeling 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.

A bill introduced into the Virginia State House of Representatives[79] required public bodies to conduct privacy impact analyses prior to authorizing or prohibiting the use of invasive technologies. RFIDs were specifically mentioned, as were "tracking systems, facial recognition systems, hidden cameras, spyware, photo monitoring systems and Internet wiretaps."[80] This bill appears to have been aimed more at the adoption and use of RFIDs by public bodies rather than in the private sector. However, as discussed

---

[76] A Maryland bill that would have required the establishment of a Task Force to study the use of RFIDs was given an unfavourable report by the state's Committee on Economic Matters, and is expected to die as a result. U.S., H.B. 354, *An Act concerning Commercial Law-Task Force to Study the Use of Radio Frequency Identification Tags by Retailers and Manufacturers*, 2005, Reg. Sess., Md., 2005.
[77] H.R. No. 4673, 108th Congress, 2d Session, June 23, 2004, s. 2(c).
[78] U.S., S.B. 128, An Act to amend Ch. 407, RSMo, by adding thereto one new section relating to radio frequency identification tags (RFID), 93rd Gen. Assem., Reg. Sess., Miss., 2005. The bill has passed second reading and was referred to the Commerce, Energy and the Environment Committee in January of 2005.
[79] U.S., H.B. 1304, 2004, Reg. Sess., Va., 2004. This bill died in committee before the end of 2004.
[80] *Ibid*., s. 1

above, the widespread use and deployment of RFIDs in both public and private contexts makes public adoption a significant dimension of the problem.

In California, a bill[81] introduced by Senator Bowen set conditions on the use of RFIDs by certain entities. The bill specifically targeted libraries but had broader application as well. With respect to private entities, the bill set the following conditions to govern the use of the RFID where it "enables the user to collect information from RFID tags attached to consumer products to gather, store, use, or share information that could be used to identify an individual":

> a) The information is collected only to the extent permitted by law.
> b) The information has been provided by a customer for the purpose of completing a transaction to purchase or rent an item containing an RFID tag at a retail store.
> c) The information is not collected at any time before a customer actually initiates a transaction to purchase or rent an item or at any time after the customer completes the transaction.
> d) the information regards only a customer who actually presents the item for purchase or rent, and is in regard only to that item.[82]

Under the bill, libraries were prohibited from using RFIDs in relation to circulating materials in a manner that could be used to identify a borrower unless the following conditions were met: the information collected was no more than permitted by law; the information was provided voluntarily by the patron for the purpose of using the library facilities; the information was collected only at the point where the patron borrowed the item, and only in relation to that borrower and that item. This California bill did not mandate labeling or require that there be a mechanism to deactivate the tags at the point of purchase in consumer contexts.

A second California bill[83] introduced in February 2005 prohibited the use of RFIDs in identity documents created by public sector entities where the RFIDs would enable personal information to be remotely scanned. These documents include but are not limited to: driver's licences; identification cards issued for employees and contractors as well as ones issued by educational institutions; health insurance and benefit cards; benefit cards for any government supported aid program; and library cards.[84] Section 2 of the bill states: "Easy access to the information found on drivers' licenses and other similar identity documents facilitates the crime of identity theft." Similarly, a Texas bill prohibited school districts from requiring students "to use an identification device that uses radio frequency identification technology or similar technology to identify the student, transmit information regarding the student, or track the location of

[81] U.S., S.B. No. 1834, *supra* note 60.
[82] *Ibid*., Ch. 22.7, s. 22650.
[83] U.S., S.B. 682, *An Act to add Article 4 (commencing with s. 1798.9) to Ch. 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, relating to Privacy*, 2005-06, Reg. Sess., Cal., 2005.
[84] *Ibid*.

the student."[85] Also, a Rhode Island bill under consideration prohibits government use of RFIDs "for the purpose of tracking the movement or identity of any employee, student or client, or of any other individual as a condition of obtaining a benefit or services from such agency."[86]

A bill entitled *The Radio Frequency Identification – Right to Know Act* was introduced in Utah in 2004.[87] It recommended amending the state's *Consumer Sales Practices Act*[88] specifically to address RFID technology. It defined an RFID as: "a device a) made of a microchip; and b) that contains a unique number or identifier: i) related to an item or product; and ii) that can be read or transmitted to an external device using radio waves."[89] The bill stated that it should be an offense for retailers to sell a product containing an RFID to a consumer without providing notice on the product or packaging that the product contained an RFID. The label should 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. Further, it required any supplier to disable the RFID prior to the completion of the sale "unless the consumer chooses to leave it active."[90]

A second Utah bill proposed amendments to the *Utah Computer Crimes Act*. This bill, signed into law by the state Governor on March 11, 2005, amended the definition of "computer" to include an RFID tag and reader. The amendments make it an offence for unauthorized parties to access information stored on an RFID tag.[91]

A Massachusetts bill requires multi-level warnings. Retailers using RFIDs in their stores must "display a sign placed in a conspicuous location printed in a conspicuous type size"[92] 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 must be labeled specifically in a conspicuous location on the packaging. The labels should 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. Further, "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."[93] Finally, RFID systems deployed at the retail

---

[85] U.S. H.B. 2953, *An Act relating to the identification of public school students through the use of radio frequency identification technology*, 79th Legis., Reg. Sess., Tx, 2005, s. 1. Online: http://www.capitol.state.tx.us/79r/billtext/HB02953I.HTM.
[86] U.S., H.B. 5929, An Act Relating to State Affairs and Government – Restricting Radio Frequency Identification Devices, 2005, Reg. Sess., R.I., 2005, s. 42-140-1. Online: http://www.rilin.state.ri.us/BillText/BillText05/HouseText05/H5929.htm.
[87] U.S., H.B. 251, *Radio Frequency Identification – Right to Know Act*, 2004, Gen. Sess., Utah, 2004
[88] 13 Utah S.C. § 11(2004).
[89] U.S., H.B. 251, *supra* note 85.
[90] *Ibid*.
[91] U.S., H.B. 185, *Utah Computer Crimes Act Amendments*, 2005, Reg. Sess., Ut., 2005. Online: http://www.le.state.ut.us/~2005/bills/hbillamd/hb0185.htm.
[92] U.S., S.B. 181, *An Act Relative to Consumer Protection and Radio Frequency Identification Systems*, 2005, Reg. Sess., Mass., 2005. Online: http://www.mass.gov/legis/bills/senate/st00/st00181.htm.
[93] *Ibid*., s. 3(c).

level "shall only store, encode or track RFID tags attached to an item listed in the inventory of the commercial entity as un-purchased, except in cases of product returns, product recalls or for warranty purposes."[94] In other words, beyond these exceptional circumstances, the store shall not track items tagged with RFIDs after purchase.

New Mexico is considering a detailed bill that requires 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 also sanctions businesses against "coercing" consumers into keeping tags active, matching consumer personal information with tag information "beyond what is required to manage inventory" and sharing information gathered from RFID tags with third parties.[95] The bill faced fierce opposition from the retail and high tech sectors and was ultimately defeated. It is expected to be reintroduced in 2006. A similar bill was defeated in South Dakota. The South Dakota bill required retailers to obtain written consent from persons before any of their personal information was matched or stored with data collected from the products' RFID tags. Separate written consent would have been required for any sharing of this information with third parties. The bill also provided that tags be deactivated before consumers left a store in which they had purchased any tagged item.[96]

A Tennessee bill currently making its way simultaneously through the Senate[97] and the House,[98] addresses labeling issues related to RFIDs. It would amend 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."[99] Similar labeling requirements are also present in a recently introduced Nevada bill.[100] The onus to comply with the law is placed on any person who "produces, manufactures, packages, distributes or sells a retail product" and who has placed an RFID tag in the product or its packaging.[101] Any breach of the labeling requirements would constitute a deceptive trade practice.

---

[94] *Ibid*., s. 3(d).
[95] 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. Online: http://www.aeanet.org/governmentaffairs/gajl_HB0215newmexicorfid0205.asp.
[96] U.S., H.B. No. 1136, *An Act to regulate the use of radio frequency identification tags*, 80th Legis. Ass., Reg. Sess., S.Dak., 2005. Online: http://legis.state.sd.us/sessions/2005/bills/HB1136p.htm.
[97] 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.
[98] U.S., H.B. 300, *An Act to amend Tennesse Code Annotated, Title 47, Chapter 18, relative to consumer protection*, 2005, Reg. Sess., Tenn., 2005. .
[99] *Ibid*., s. 2, amending s. 47-18-104 of the *Tennessee Code Annotated*.
[100] U.S., S.B. 264, 2005, Reg. Sess., Nev., 2005.
[101] *Ibid*.

A New Hampshire bill requires retailers to notify consumers, orally or in writing, that an RFID tag is embedded in a product.[102] In contrast to other bills with labeling requirements, this one is much less specific about the location, visibility or contents of any label or notice given to consumers.

A few trends or points are worth noting with respect to these early legislative initiatives. First, they illustrate different threads in the response to privacy concerns raised by RFIDs. Some bills specifically address the use of RFID tags in government documents and in relation to government services. These bills seem to address risks associated with having personal documents "shouting out" personal information that could be read by non-authorized readers, and/or surreptitiously matched with other data or information about individuals without their knowledge.

Second, labeling requirements are the focus of a number of these legislative initiatives. 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. However, these labeling requirements do not flow automatically from the notice requirements in legislation such as *PIPEDA*. A general labeling requirement, where the chip only contains 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.

Labeling requirements in the bills discussed above typically stipulate that RFIDs be deactivated at the point of sale or that consumers be given the option of deactivating them. Such provisions, potentially protective of consumer privacy, will likely run into problems as technology advances and the continued activation of RFIDs becomes essential to the functioning of smart consumer products. Tags in clothing may be designed to communicate information to washing machines to more efficiently wash that article. Tags in grocery items may communicate with refrigerators to report their past expiry dates. Deactivation removes this utility and may increasingly be seen as an ineffective or sub-optimal option.[103]

The success or failure of these bills is tied to the demands they make on commercial interests. Bills addressing labeling requirements often specify the size, location and format of the label to ensure clear visibility. In some cases, additional notification is required in retail stores. 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. Retailers seem willing to consider these limitations as bearable ones.

The bills that have been defeated, such as the New Mexico and South Dakota bills, provided such strict limitations on the use of RFIDs, however, that the advantages

[102] U.S., H.B. 203-FN, *An Act relative to the use of tracking devices in consumer products*, 2005, Reg. Sess., N.H., 2005.
[103] *FTC Report*, *supra* note 112, at 21.

to retailers of using such tags were largely negated. This is an important lesson to be drawn from the U.S. experience: the protection of consumer privacy must be balanced against commercial interests in deploying useful technologies.

3. 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 issued guidelines for the use of RFIDs in the private sector. It followed with 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 accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concern. 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.[104]

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[105] 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."[106] The Working Party notes that whether or not the 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. 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. The Working Party notes that the Directive itself is instructive about whether or not it should apply: parties should take account "of all the means likely to be used either by the controller *or by any other person to identify the said person*."[107] Thus, it may be possible to consider the potential to link

---

[104] *Working Document*, *supra* note 1, at 2.
[105] 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, Official Journal L281, 23.11.1995, 31, online: http://europa.eu.int/comm/internal_market/privacy/law_en.htm.
[106] *Ibid*.
[107] *Ibid*., Recital 26.

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. 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 individual's rights."[108] This is quite distinct from the approach taken in the various U.S. 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.

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.[109] This latter requirement is an important one that has not commonly appeared in the U.S. bills. Since readers can be hidden, and can operate silently and invisibly, it is important to alert to their location. Second, consumers must understand the link between the presence of tags and readers and data collection; and 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

[108] *Working Document*, *supra* note 1, at 9.
[109] *Ibid*. at 10.

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.

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.[110] Beyond that, the Working Document contemplates 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 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.

[110] *Ibid*. at 14.

Part IV – Industry Standard Setting and Consumer Privacy Advocacy

1. Industry Standards

It is not surprising that in the United States, where self-regulation has generally been the preferred approach to protecting consumer privacy, industry standards are emerging to set norms and guidelines for the commercial deployment of RFIDs.

EPCglobal Inc. is a leader in setting international standards for electronic product code (EPC) technology – specifically RFIDs. Its privacy guidelines,[111] aimed at addressing consumer privacy concerns that might otherwise hinder the successful development and deployment of this technology, embrace four key themes: consumer notice; consumer education; consumer choice; and record use, retention and security.

The guidelines provide that consumers must be notified of the presence of an RFID tag in a product by the placing of an EPC logo on the product's packaging. Not only must consumers be educated about RFID technology and its benefits, but companies using RFID tags are expected to play a role in educating consumers about the meaning of the EPC logo. The guidelines also suggest that EPCglobal will be a forum for "both companies and consumers to learn of and address any uses of EPC technology in a manner inconsistent with these Guidelines."[112] Consumers will be informed of any choices they might have to discard, destroy or disable tags. The guidelines indicate that, for the most part, tags will be placed in disposable packaging surrounding the product and not in the product itself. Finally, the guidelines emphasize that the RFID tags themselves must not store customer personal information and that businesses must comply with relevant laws concerning the collection, control and custody of any personally identifiable information regarding their customers.

Beyond setting privacy guidelines, the actual standards developed for the technology by an organization such as EPCglobal can have an impact on privacy protection. This point was particularly emphasized by the EU Working Party on data protection issues in relation to RFIDs. However, as the Working Party noted, standardization of technology also raises its own privacy concerns. Standardization benefits industry by ensuring the interoperability of emerging technologies. However, the greater the interoperability of RFID technology, the greater the risk to personal privacy. For example, the ability of a single reader to read tags from a variety of different commercial sources will have the effect of increasing the potential impact on personal privacy.

[111] EPC Guidelines. Online: http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html.
[112] *Ibid*., guideline #3.

2. Consumer and Privacy Advocacy

The advocacy of consumer and privacy groups regarding the use of RFID technology has been significant. Advocates in the United States have noted that RFIDs raise novel privacy concerns,[113] that these concerns arise with respect to both public and private sector uses of RFIDs, that fair information practices provide a framework for addressing RFID privacy concerns, and that additional concerns can and must be addressed in the early stages of the development of the technology.

These novel privacy concerns arise from factors specific to the technology, particularly its unobtrusiveness. Because the chips are invisible to consumers, absent notification or labeling, consumers cannot know of their operation either at the point of sale or afterwards. Indeed, many cite the spectre of consumers walking around oblivious to the fact that their clothing, handbags and other personal items are shouting out information to anyone equipped with the technology to read it.[114] Another concern is the passive nature of RFID data collection. Normally, consumers make deliberate choices to provide personal information, as, for example, when they sign up for and use a loyalty card or make a payment using a debit or credit card. By contrast, RFIDs can be read at any number of points on any number of occasions without consumers being aware. Advocates are also concerned about the unique nature of the information being conveyed about consumer items by even the simplest RFID tag. They identify specific items, bought from specific stores at specific points in time. The potential for this information to be used to track consumers and to monitor their purchasing patterns is enormous. Equally alarming is the dramatic increase in the volume of information that could be collected, stored and linked to other personal data.[115] The American Civil Liberties Union (ACLU) has identified RFID use as another push forward in a "seemingly inexorable drift toward a surveillance society"[116] that is characterized by increased co-operation between the private sector and government.

The Electronic Privacy Information Centre (EPIC) has also developed guidelines for the use of RFID technology "in order to balance private enterprise interests against consumer privacy interests."[117] The starting point is compromise; there is no attempt to

---

[113] Paula J. Bruening , "Prepared Statement of Paula J. Breuning, Staff Counsel, The Center for Democracy and Technology, before the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, on Radio Frequency Idnetification (RFID) Technology", July 14, 2004. online: http://www.cdt.org/testimony/20040714breuning.pdf.

[114] For a general overview of privacy concerns, see *FTC Report*, *supra* note 12.

[115] See, Cedrick Laurant, "Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security and the Consumer" Before the Subcommittee on Commerce, Trade and Consumer Protection House Committee on Energy and Commerce", July 14, 2004. Online: http://www.epic.org/privacy/rfid/rfidtestimony.0704.html.

[116] Statement of Barry Steinhardt, Director, Technology and Liberty Project, American Civil Liberties Union on RFID Tags Before the Commerce, Trade and Consumer Protection Subcommittee of the House of Representatives Committee on Energy and Commerce, July 14, 2004. Online: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-60594.

[117] Electronic Privacy Information Centre (EPIC), "Proposed Guidelines for Use of RFID Technology: Enumerating the Rights and Duties of Consumers and Private Enterprises", June 21, 2004. Online: http://www.epic.org/privacy/rfid/rfid_gdlnes-062104.pdf. (*EPIC Guidelines*)

bar the deployment of the technology. Rather, the guidelines recognize two types of commercial deployment of RFIDs – first, as a substitute for product barcodes and, second, as a means of matching RFID data with pre-existing data about customers – and then set duties for retailers in both contexts.

With respect to RFID use as a replacement for barcodes, the guidelines require notice to consumers of the presence of tags, through labels, logos or equivalent means. Notice can be given where the item is located on the premises, such as on a shelf, or at the point of sale. The notice must be sufficient to inform the customer of "the nature of the RFID system and the data processing in place," and it must be "reasonably conspicuous." [118] Retailers must turn off the tags before the completion of any sale, unless the consumer consents to its continued activation for purposes related to warranty tracking, compliance with smart appliances, and so on. Items must be tagged in a manner that allows for the "easiest possible removal" of tags.

However, the EPIC guidelines do not address circumstances in which tags might be required to remain active for the purpose of product or merchandise return. This latter issue is a significant one, and would impact any policies, rules or guidelines relating to deactivation. If stores are required under consumer protection legislation to accept returns of items, and if RFIDs replace barcodes as a means of tracking and controlling inventory, it may well be reasonable, if not necessary, for the tag to remain active in order for the store effectively to permit a customer to refund or exchange merchandise.

Beyond their tagging and labeling requirements, the guidelines prohibit retailers who substitute RFIDs for barcodes to use the tags for tracking the movement of individuals, for example, throughout the store to discover shopping patterns. The guidelines specifically indicate that shops should not rely on RFID tags to prevent fraud or shoplifting. They should not record or store information from other tags on the person of the consumer, including ones from items previously purchased at that store. Finally, retailers must not "coerce individuals to keep tags turned on after purchase for such benefits as warrantee tracking, loss recovery, or compliance with smart appliances."[119] This latter provision seems to conflict with the need to balance business and consumer interests in the deployment of RFIDs. If RFIDs are implemented to streamline such features as customer returns and warranties, among other things, it seems odd not to permit companies to require the continued activation of RFIDs for these purposes. Further, it is hard to grasp what "coercion" means in this context. If a consumer has a smart appliance, and if the RFIDs embedded in the products are designed to communicate with the appliance, is it coercion to inform consumers that the smart appliance features will not work if the tag is deactivated?

The second type of RFID deployment identified in the EPIC guidelines is the matching of RFID data with other consumer information. The guidelines require written consent from individuals before any personally identifiable information is matched with data collected through the RFID system in place. Individuals must be informed of the

[118] *Ibid*., Guideline I(A)(1).
[119] *Ibid*., Guideline I(B)(3).

scope of the use of data gathered. Further, the guidelines limit data-matching to only those activities required to manage inventory, and they also bar disclosure of such data to non-affiliated third parties.[120] RFID tag information cannot be used to identify an individual. Data gathered through an RFID system must be securely stored, accurate, complete and current, and kept only for as long as is necessary for the purposes of collection. Organizations must provide information about their policies and practices with respect to the handling of personal information. The EPIC guidelines also contemplate the establishment of a parallel consumer option – that of allowing individuals to enroll anonymously in any RFID data gathering system.

A third part of the EPIC guidelines identifies certain rights of consumers: a right to access personal information collected through an RFID system, the right to have tags removed, and the right to challenge the compliance with the guidelines of parties employing RFID systems.

Overall, the EPIC guidelines follow generally accepted fair information practices, with some rules crafted specifically to address features of RFID technology. In this sense, they explicitly adapt existing principles to a new technology. This offers the benefits of consistency and familiarity with principles across technologies, while identifying ways in which the new technology challenges the application of the existing principles.

A 2004 report on RFIDs from the Office of the Information and Privacy Commissioner of Ontario[121] also emphasizes the importance of compliance with Fair Information Practices in the use of RFIDs. Requirements of notice and consent, consumer choice and control received particular attention and supported the conclusion that "[p]articipation in an RFID application should be strictly voluntary"[122] and should occur only with customer consent. The report stated that consumers should have the right to have a tag deactivated without cost and to have personal identity information kept separate from information identifying an object.[123] Beyond that, it recommends adherence to all of the Fair Information Practices and embraces the RFID-specific recommendations of EPIC.[124]

[120] This may be of limited comfort given the high degree of affiliation among major retailers.
[121] Tag, You're It, *supra* note 7.
[122] *Ibid*., at 20.
[123] *Ibid*.
[124] See *EPIC Guidelines*, *supra* note 112.

Part V – Canadian Privacy Law Applied to RFIDs

In this section of the report, we consider whether or not existing Canadian legislation to protect consumer privacy is sufficient to address the various issues raised by RFID technology. We focus primarily upon the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*. While we recognize that some provinces have relevant legislation governing their private sectors, much of this has been found to be "substantially similar" to *PIPEDA*, and so specific consideration of these statutes falls outside the scope of this project.

1. Application of the Personal Information Protection and Electronic Documents Act (PIPEDA) to the Commercial Use of RFID Technology

PIPEDA applies where an organization collects, uses or discloses personal information about its clients or customers in the course of its commercial activities".[125] It also applies to personal information about employees of an organization, which the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."[126] 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, partnership, person (which includes a corporation) or trade union.[127] 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.

The privacy concerns relating to the use of RFIDs by a private sector organization to collect, use or disclose personal information about its employees are disquieting. However, because *PIPEDA* does not govern the collection, use or disclosure of personal information of employees unless the organization operates a federal work, undertaking or business, these concerns will not be addressed in this section.

a. "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."[128] Any commercial organization that sells products containing RFID tags are carrying on a commercial activity and are subject to *PIPEDA*. However, when commercial organizations that employ RFID tags in

[125] *PIPEDA*, *supra* note 16, s.4(1)(*a*).
[126] *Ibid*., s. 4(1)(*b*).
[127] *Ibid*., s. 2.
[128] *Ibid*., s. 2.

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.*

b. "Personal Information"

PIPEDA applies where an organization collects, uses or discloses "personal information" in the course of commercial activities. "Personal information" is defined as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[129] These exceptions have been the subject of Findings made by the federal Privacy Commissioner,[130] whose office has recently signaled that it will take a strict interpretation of these exceptions.[131]

The definition implies that the personal 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.

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

---

[129] *Ibid*.

[130] 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." *PIPEDA* Case Summary #230, September 16, 2003. Online: http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030916_05_e.asp.

[131] 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, December 1, 2004. Online: http://www.mgblog.com/resc/GeistPCCSpamdecision.pdf.

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 plainly are 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, will be subject to *PIPEDA* and its privacy principles.

The potential for organization and monitoring of 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 Office of the federal Privacy Commissioner and 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.[132] The Privacy Commissioner applied a strict interpretation of what constituted "personal information" and did not discuss the particular context of the information collection. He 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."[133]

In the context of RFID technology and information collection, use and disclosure, these findings superficially may indicate that only highly specific information that identifies an individual meets the definition of "personal information" and that a purchase

[132] 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. *PIPED*A Case Summary #4 (23 July 2001), online: http://www.privcom.gc.ca/cf-dc/cf-dc_010723_04_e.asp.
[133] *PIPED*A Case Summary #14, (21 September 2001), online: http://www.privcom.gc.ca/cf-dc/cf-dc_010921_e.asp.

may not constitute personal information about the purchaser.[134] However, it would be risky to draw and rely on such conclusions. With respect to the latter finding, the Commissioner was careful to limit his 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 them. For example, the Assistant Privacy Commissioner recently indicated that if the circumstances render an individual identifiable, then the information at issue will be considered personal information under *PIPEDA*, notwithstanding the fact that the individual is not specifically named.[135]

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*.[136] The Commissioner found that although "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 individual." [137] The Commissioner found nothing in *PIPEDA* that would suggest business information and personal information must be mutually exclusive. 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.

Exactly how much precedential value these Findings should be accorded is questionable, as the Federal Court has indicated that they are not binding.[138] Potentially more problematic for privacy advocates concerned with the expansion of RFID technology is the 2004 decision of the Supreme Court of Canada in *R. v.Tessling*.[139] This case involved a warrantless use of a thermal imaging device that allegedly violated an accused's section 8 *Charter* rights. Although the Court's reasoning is not necessarily directly applicable to the use of RFID technology and the collection, use and disclosure of data in the private context, its consideration of the intersection of data obtained by the employment of a new technology with information from other sources may portend its view of what constitutes personal information generally. Justice Binnie held that thermal imaging of a home provided information that might or might not raise an inference about illegal activities taking place inside, depending upon other information with which it

---

[134] Consider the former Privacy Commissioner's statement that "It is certainly difficult to discern how an individual prescription can constitute personal information about the physician who wrote it." PIPEDA Case Summary #15 (2 October 2001), online: http://www.privcom.gc.ca/media/an/wn_011002_e.asp.
[135] *PIPEDA* Case Summary #270 (4 May 2004), online: http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040504_e.asp.
[136] *PIPEDA* Case Summary #220 (15 September 2003), online: http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030915_e.asp.
[137] *Ibid.*
[138] *Englander v. Telus Communications Inc.*, 2004 FCA 387, at para 48.
[139] 2004 S.C.R. 67, 244 D.L.R. (4th)541. For a more detailed discussion of this case, see *infra*.

could be combined. According to the Court, thermal imaging was but one straw on a fulcrum that tilts according to the amount of other evidence obtained by the Crown.[140]

Similarly, inventory information captured on an RFID tag would not likely constitute personal information, as it is not about an identifiable individual. The Act 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 jewelry worn by the consumer, and can draw inferences about the consumer 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 information 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, *Tessling* suggests that inventory information on an RFID tag 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.

However, the adoption of this *Tessling* reasoning to 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, consequently, decide whether or not to apply the principles under *PIPEDA*. This reasoning also seems to preclude *PIPEDA*'s application in situations where data from multiple RFID tags linked to an identifiable individual is matched and analysed for purchasing patterns or other information.

Although the consequences of *Tessling* may be more of a concern in the sphere of public law, where information on RFID tags may be another atomized piece of info that does not itself have a reasonable expectation of privacy, its reasoning may affect the application of *PIPEDA*. 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.

[140] *Ibid*., at para. 36.

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* interpretation will be relevant also 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.

c. Reasonableness in *PIPEDA*

Section 5(3) of *PIPEDA* contains a statement applicable generally 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.

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 section 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.

2. The Normative Provisions of PIPEDA

Subject to certain exceptions and requirements,[141] every organization that is subject to *PIPEDA* must comply with the obligations set out in Schedule 1 to the Act. [142] Schedule 1 incorporates the Principles and Commentary of the Model Code for the Protection of Personal Information adopted by the Canadian Standards Association. 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 presents 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.[143] 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.

a. 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 (for example, 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. Practically, this would entail in-store signage and/or product labeling to notify customers that products contain RFID tags that enable the collection of personal information and to explicate the purposes for which the information is collected.

---

[141] *PIPEDA*, *supra* note 16, ss. 6-9.
[142] *Ibid*., s. 5.
[143] 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.

b. Principle 3 – Consent

Generally, individuals must have knowledge of and consent to the collection, use or disclosure of their personal information. Signage and/or labeling could fulfill 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.[144] The form of consent may vary, depending on the sensitivity of the information.[145] Express consent will be required where the information is likely to be considered sensitive.[146] An individual may also withdraw consent at any time.[147]

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.[148] 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.

---

[144] *PIPEDA*, *supra* note 16, Principle 4.3.3.
[145] *Ibid*., Principle 4.3.4.
[146] *Ibid*., Principle 4.3.6.
[147] *Ibid*., Principle 4.3.8.
[148] *Ibid*., Principle 4.3.8.

c. Principle 4 – Limiting Collection

Information cannot be collected indiscriminately, but must be limited to that which is necessary for the purposes specified. 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), 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.

d. 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. 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.[149]

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 to the information pursuant to Principle 9.

3. 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.

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

[149] *Ibid*., Principle 4.3.1.

> 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.

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 drivers' 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. Section 7(3) of the Act provides:

> […] 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 […].

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, 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.[150] Similar concerns have been raised in the United States.[151] Section 7(3) 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

---

[150] See, for example, John Schwartz and Micheline Maynard, "Airlines Gave F.B.I. Millions of Records on Travelers After 9/11", The New York Times (1 May 2004), online: The New York Times http://travel2/nytimes.com/mem/travel/article_page.html?res=9B06E3D9153DF932A35756COA9629C8B63.

[151] These concerns have been raised with respect to broad powers of government in the U.S. under the *Patriot Act* (*Uniting and Strenthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, Pub.L.N. 107-56, 115 Stat. 272.) See: Wasseem 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.

> (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.

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."[152] However, as discussed earlier, the scope of these provisions in relation to data collected from RFIDs is more troubling.

Section 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….

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 very vulnerable situation.

4. 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 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 *R. v. Tessling*[153] discussed above, combined with the potential for secondary uses of personal information, raise unique concerns.

---

[152] S. Perrin et al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, (Toronto: Irwin Law, 2001) at 75.
[153] *Tessling*, *supra* note 133.

In *R. v. Tessling*, the Supreme Court of Canada heard the Crown's appeal of the decision of the Ontario Court of Appeal, which overturned the conviction of a man accused of a variety of drug and weapons offences. The case involved a claim under section 8 of the *Charter* that the warrantless use of a thermal imaging device violated the *Charter* rights of the accused. 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 his 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. Justice Binnie for the unanimous court noted that much of early privacy law was rooted in trespass law: "In an earlier era, privacy was associated with private property, whose possession protected against intruders."[154] He continued: "As technology developed, the protection offered by property rights diminished[…]. The courts were reluctant to accept the idea that, as technology developed, the sphere of protection for private life must shrink. Instead, it was recognized that the rights of private property were to some extent a proxy for the privacy that ownership of property originally conferred […]."[155] However, he acknowledged that privacy principles face competing demands from social and economic life, including a demand by society for security, safety and the suppression of crime.[156]

Justice Binnie identified three main privacy interests: personal privacy, territorial privacy and informational privacy. In the case of thermal imaging of one's home, he noted that "the privacy is essentially information (i.e., about the respondent's activities) but it also implicates his territorial privacy because although the police did not enter his house, that is where the activities of interest to them took place."[157] In Justice Binnie's view, 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 "a 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."[158] This shifts the focus from the individual's personal privacy to the privacy of his 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. Justice Abella (then of the Ontario Court of Appeal) had characterized the thermal imaging activity differently: in her view, it amounted to a search of the accused's home.[159]

Justice Binnie concluded that there was no reasonable expectation of privacy with respect to the thermal image created through this technology. Due to the nature of the

---

[154] *Ibid*., at para 16.
[155] *Ibid*.
[156] *Ibid*., at para 17.
[157] *Ibid*., at para 24.
[158] *Ibid*., at para 27.
[159] *R v. Tessling* 2003 CanLII 8861 (ON C.A.)

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. Justice Binnie's decision 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."[160]

Its disclosure scarcely affects the "dignity, integrity and autonomy" of the person whose house is subject of the FLIR image."[161]

The *Tessling* decision is disturbing in its implications for personal information privacy in general and 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 information about the object in which the tag is embedded. Although the collector can match this information can be matched with other gathered data so as to allow the collector to draw inferences about a particular individual, but 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*,[162] 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".[163]

While the *Tessling* case deals with the constitutional right of privacy in the form of the right to be freedom 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, sees 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."[164] This same author also identifies data mining as a major threat to privacy in the case of criminal investigations. Another author argues: "When state surveillance uses ubiquitous technologies, constitutional privacy protection may be diminished as social

---

[160] *Ibid*., at para 63.
[161] *Ibid*.
[162] [1993] 3 S.C.R. 281, 84 C.C.C. (3d) 203.
[163] *Ibid*., at 27.
[164] Renée 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.

conventions have already adapted to them."[165] 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, however; 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*, which are discussed below.

5. Implications of Analytical Approach Taken in Tessling

In developing a right of privacy under sections 7 and 8 of the *Charter*,[166] the Supreme Court of Canada has defined the main zones of privacy as territorial/spatial, personal and informational.[167] 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.[168] Adopting *Katz*, Canada's *Hunter v. Southam Inc*. "ruptured the shackles that confined claims to property."[169] 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 at protecting the dignity of the human person."[170] 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.[171] Therefore, a reasonable expectation of privacy may relate to a place or

---

[165] 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.
[166] *Canadian Charter of Rights and Freedoms*, Constitution Act, 1982, Part I, s. 7, 8.
[167] See for example, *R. v. Dyment* [1988] 2 SCR 417.
[168] *Katz v. U.S.*, 389 U.S. 347 (1967)
[169] *Dyment, supra* note 160, at 428; *Hunter v. Southam Inc.* [1984] 2 SCR 145.
[170] Canada, Department of Communications/Department of Justice, Privacy and Computers, The Report of the Task Force established by the Department of Communications/ Department of Justice (Ottawa: Information Canada, 1972) at 12-14. Quoted in *Dyment, ibid.* at para 21.
[171] *Ibid.* at para 22.

space, to the person or to information. Whether or not a particular technological device violates privacy may differ, depending on the Court's analytical approach to assessing the privacy interest.[172]

In *Tessling*, Justice Binnie characterizes the privacy interest as "essentially informational."[173] This approach reflects a trend that shifts the focus from an individual's spatial and personal privacy, which are both implicated by emerging technologies with surveillance capabilities, to his or her informational privacy. If no intimate information is collected or no information is gathered and linked with other information, on a *Tessling* analysis, no privacy interest has been violated. There is cause for concern when spatial and personal privacy interests do not form part of the analysis in the context of intrusive surveillance, particularly where it involves the person and/or the home. In effect, avoiding the broader analysis shrinks the zone of individual protection of privacy and, arguably, narrows privacy's general meaning.

Similarly, RFID technology raises privacy concerns in terms of the information gathered. If their full tracking and monitoring capabilities materialize, RFIDs will constitute a form of surveillance. In the retail context, for example, clothes, tires or shoes embedded with RFIDs that are allowed to remain active once a consumer leaves a store facilitate tracking, watching and unwarranted observation, albeit by an electronic eye. Consumers who purchase floor tiles, carpets or doors containing RFIDs can never know when they are being "scanned," monitored, or watched. It is as if we might be constantly shadowed by an increasingly comprehensive "data body" that does more than follow us. It can also precede us: before we arrive somewhere, we have already been measured and classified. Thus, upon arrival, we are treated according to whatever criteria has been connected to the profile that represents us.

RFID chips embedded in government-produced identification cards, passports, currency and highway and airline transportation systems are examples of the technology's potentially pervasive tracking and monitoring capabilities. Regardless of the nature and quality of the information obtained, this is surveillance: systems are used to monitor people's actions or communications; and their ability to define, determine and control the parameters of their space is diminished. In this way, the privacy interest individuals have in sustaining personal or physical space free from intrusion is potentially compromised.

---

[172] Justice Binnie's reasoning in *Tessling*, *supra* note 133, illustrates this point. In the Court of Appeal, by contrast, Justice Abella 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. By contrast, Justice Binnie takes 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.

[173] *Ibid*., at para. 24.

The Reasonable Expectation of Privacy

Protection is granted for privacy interests when courts and legislatures determine that an individual can reasonably expect privacy. This determination assesses both the subjective and objective aspects of the privacy expectation: the individual must have an actual expectation of privacy and that expectation must be one that society recognizes as reasonable.[174] While *Tessling* permitted the use of thermal imaging technology without a warrant even when associated in an area close to the home, and its American counterpart, *Kyllo,*[175] did not, both cases define important implications for assessing the reasonable expectation of privacy in the context of surveillance technology, including RFIDs.

Assuming that RFID technology will become ubiquitous, and that many RFIDs will remain activated, our ability to use this advancing technology will reduce our expectations of privacy. It will enable increasing, systematic and covert localization of individuals on a much wider scale. This substantially impacts people's traditional reasonable expectations of privacy in movement: they may have been visible at a certain time at a certain place, but much less traceable for a longer period of time. The overall result is that more of our lives, in more places, is exposed. The reasonableness of our privacy expectations in movement is diminished the more localization becomes a common side-effect of technology. It is not difficult to reduce reasonable privacy expectations by first eliminating the privacy, then the expectation of that privacy and, last, the reasonableness of our expectation of privacy. If society has no subjective expectation of privacy, because in fact, it has no privacy, then any claim to privacy would be objectively unreasonable to society as a whole. The eroding effect of technology on privacy is a slow, hardly perceptible process. There is no precise stage at which one can point to the use of technology as unreasonably tilting the balance of privacy. However, because of the fluid and flexible nature of privacy, society has been and will continue gradually to adapt to new technologies and to the privacy expectations that go with them.

6. RFIDs in the Employment Context

Employers increasingly are using surveillance devices, including video, electronic and biometric technology to monitor and obtain personal information about employees.[176] They justify such use in the name of increased productivity, improved workplace security and safety, reduced theft and minimized risks of liability associated with computer use.[177] RFID technology has not as yet been widely introduced into the Canadian private sector workplace but, from an employer's perspective, RFIDs offer new and improved ways to further the legitimate business rationales for using surveillance technology in the workplace. Arguably, as the cost of RFID technology drops, its attraction for employers grows, which is likely to raise employees' privacy concerns. From a legal perspective, the question arises as to whether the current trend, towards

[174] *Hunter, supra* note 162.
[175] *Kyllo v. United States*, 533 U.S. 27 (2001). In *Kyllo*, the use of technology not in general public use was not permissible.
[176] Uteck, *supra* note 44, at 1 (fn 3).
[177] *Ibid*., at 18-36.

balancing these competing interests by imposing a reasonableness standard, as reflected by *PIPEDA* Findings in the context of workplace surveillance, can be neatly applied to the use of RFIDs.[178] Or, will RFID technology disturb the balance of privacy in the employment context?

As mentioned, employers may want to use RFID technology in the workplace for a number of reasons. First, it could increase productivity and performance by measuring time, labour and human error costs and allow work to be adjusted accordingly. By connecting all phases of the supply chain, from purchasing and manufacturing to inventory and distribution, RFIDs create real-time information links that help expedite production and improve quality and delivery. In addition, the document-tracking capabilities of RFIDs could reduce loss by more quickly locating assets and documents and more easily tracking workflow. Moreover, performance and productivity could be enhanced by monitoring employee movement and conduct using RFIDs.

Internal theft, often cited by employers as a major and legitimate business concern, may be reduced if everything could be tracked by an RFID tag. In this way, employers are less vulnerable to financial loss due to theft by employees.

Security and safety could be further improved by replacing access cards with a more advanced RFID-based system that would allow only authorized employees to enter restricted, critical or sensitive work areas. RFID readers could be set up to trigger surveillance cameras or video recorders whenever an employee or vehicle enters or exits a controlled area. Employees could be monitored and located through RFID tags attached to equipment, tools or computers. And, finally, RFIDs could collect personally identifiable information about employees for investigations of misconduct or work rule violations.

Although undoubtedly useful in locating employees in emergency situations, the use of RFID technology in the workplace has a number of legitimate privacy implications: constant observation and tracking within the workplace and potentially off-site; the loss of anonymous movement; and the collection, use and disclosure of personal information without employees' knowledge and consent. Of particular concern for employees would be information collected by RFID-based systems being linked to other databases, such as personnel or medical records. Organizations need to address all of these concerns when considering this type of technology.

How might the law balance these competing, yet legitimate employment interests? Subject to the specific terms of an employment contract or the provisions of a

[178] See for example, *PIPEDA* Case Summary #114 (23 January 2003), online: http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp; PIPEDA Case Summary #264 (19 February 2004), online: http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_01_e.asp; PIPEDA Case Summary #265 (19 February 2004), online: http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040219_02_e.asp; PIPEDA Case Summary #273 (18 May 2004), online: http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040518_e.asp; PIPEDA Case Summary #279 (26 July 2004), online: http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040726_e.asp; PIPEDA Case Summary #290 (27 January 2005), online: http://www.privcom.gc.ca/cf-dc/2005/cf-dc_050127_e.asp.

collective agreement in a unionized workplace, informational privacy legislation has emerged as the principle means of addressing privacy concerns about the use of technology by employers.[179] *PIPEDA* applies to personal information about an employee that the employing "organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."[180] Although *it* does not apply to employment issues in provincially-regulated organizations, British Columbia[181] and Alberta[182] have enacted substantially similar legislation that applies to personal employee information.

PIPEDA seeks to balance the privacy interests of employees with the legitimate business interests of employers. Section 3 expressly refers to this balance:

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[183]

Under section5(3), an organization "may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances."[184] Thus, while *PIPEDA* clearly contemplates a balanced approach in assessing the competing interests in the workplace, the reasonableness clause creates an important limitation on the use of surveillance technology by employers.

Mirroring the general framework and established analysis taken in arbitral jurisprudence relating to surveillance and workplace privacy,[185] complaints involving technology-enhanced surveillance in the employment context have assessed the issue on the reasonableness standard.[186] The assessment of the reasonableness of employer action

---

[179] *PIPEDA, supra* note 16. British Columbia *Personal Information Protection Act, supra* note 16; and Alberta *Protection of Personal Information Act, supra* note 16..
The *Charter* does not apply to private parties, a common law right of privacy is uncertain and in those provinces where there is a statutory tort of invasion of privacy the legislation has serious limitations. See, Colin H.H. McNairn and Alexander K. Scott, *Privacy Law in Canada* (Toronto: Butterworths, 2001), c. 3. Arbitral jurisprudence has developed privacy principles in the context of surveillance, but most Canadian employees are not subject to a collective agreement.

[180] *PIPEDA, supra* note 16, s.4(1)(*b*).

[181] *PIPA* (B.C.), supra note 16, s.1 (personal information includes employee personal information).

[182] *PIPA* (Alberta), supra note 16, s.1(i), (d) and s.15(1).

[183] *PIPEDA, supra* note 16, s. 3 (referred to as the "purpose clause").

[184] *Ibid.* s.5(3) (referred to as the "reasonableness clause").

[185] Arbitrators attempt to balance the interests by adopting a reasonableness standard in assessing potentially invasive practices by employees. See for example, *Re Doman Forest Products Ltd. and IWA Loc. 1-357* (1990), 13 L.A.C. (4th) 275; *St. Mary's Hospital and HEU* (1997), 64 L.A.C. (4th) 383; *Re Labatt Ontario Breweries (Toronto Brewery) and Brewer, General and Professional Workers' Union* (1994), 42 L.A.C. 151; and *New Flyer Industries Ltd. And CAW-Canada, Loc. 3003* (2000) 85 L.A.C. (4th) 304.

[186] See for example, *PIPEDA* Case Summaries, *supra* note 171.

is weighed against the impact on the employee and not merely on the rationality of the employer action in furthering some valid objective. An employer's action will be reasonable only if its effect on an employee's expectation of privacy is proportional to the objective. Presumably, this analytical approach would be applied to complaints arising from the use of RFIDs by employers.

In addition, several of the core privacy principles in *PIPEDA* that employers must follow are particularly relevant to the use of RFIDs in the workplace.[187] Organizations (employers) must identify, document and inform an individual (employee) of its reasons for collecting personal information before or at the time of collection.[188] Employees have the right to know how RFIDs are being used and why certain information obtained via RFIDs is being collected and used. In this way, the principle ensures that employers address both the necessity or justifications for implementing RFIDs and the relevance of the information sought.

Central under *PIPEDA* is the requirement that organizations obtain consent of all individuals before handling any of their personal information.[189] The section 5(3) reasonableness clause places an objectively determined limit on consent so that, if the purpose of the collection, use or disclosure is inappropriate, section 5(3) can override even express consent. This provision is particularly significant where there is an imbalance of power and the consent given may not be truly voluntary, such as in the case of employees, who could be concerned about negative employment consequences if they withhold their consent, for example, to wear an RFID tag for access control purposes. As long as an employer proposes to collect, use or disclose employee personal information for purposes that a reasonable person would consider appropriate, however, an employee may have little choice but to consent.[190] Similarly, the consent exception provisions under section 7 potentially weaken the protection that is afforded.[191] For example, a theft investigation under section 7(1)(b) may justify the RFID tracking of company assets or humans to investigate misconduct.[192]

---

[187] *PIPEDA*, *supra* note 16, Schedule 1 .

[188] *Ibid.* Principle 2 reads: "The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected."

[189] *Ibid.* Principle 3 reads: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."

[190] See PIPEDA Case Summary #65 (14 August 2002), online: http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020814_e.asp. A number of employees alleged that their nuclear products employer had inappropriately required them to consent to the collection of their personal information for the purposes of a security clearance check or risk dismissal and that therefore their consent was not voluntary. Taking into account the nature of the business and the requirements as a licensed facility for access security clearance, the key consideration for the Privacy Commissioner was not whether there might be consequences if an employee refused to consent, but rather whether the collection itself was reasonable in the circumstances.

[191] *PIPEDA*, *supra* note 16, s.7 sets out the circumstances in which personal information may be collected, used or disclosed without the individual's consent.

[192] See PIPEDA Case Summary #73 (7 October 2002), online: http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021007_2_e.asp; PIPEDA Case Summary #84 (10 October 2002), online: http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021010_3_e.asp.

Nevertheless, organizations cannot collect information indiscriminately.[193] Compliance with this principle on the part of employers prevents employees from being subject to wholesale and arbitrary surveillance throughout the workplace. Personal information can be used only for those purposes to which the individual consents, and internal policies and procedures should ensure it is destroyed when no longer needed.[194] Limiting the use, disclosure and retention of personal information provides at least some measure of confidence to employees that employers are not unnecessarily using or retaining information. This limitation may be particularly welcomed by employees concerned that personal information collected by the RFID may be retrieved at a future time for disciplinary reasons or may be linked with personnel or medical records.

In sum, responding to the use of RFIDs in the employment context will require a balancing analysis that determinines the reasonableness of the surveillance. This assessment will evaluate of a number of factors, including the type of surveillance technology and whether or not there is a less intrusive method available for achieving the same objective; the nature and purpose of the RFID and the extent to which it is a form of invasive surveillance; the adequacy of notice to employees; and the way in which the RFID technology was implemented in the workplace. Arguably, RFID technology is less intrusive than other forms of surveillance technology currently being used in the workplace. The security and safety justifications for use of RFIDs in the workplace are particularly persuasive. Provided employers meet the reasonableness standard, RFIDs are likely to find their way lawfully into the private sector workplace.

7. RFIDs and Cookies – Analogous Technologies?

Although RFIDs are relatively new, the privacy issues they raise are not necessarily novel. In some ways, "cookies," a technology used in the online context, operate like RFID tags. 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 his or her web browser on behalf of a web site. 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 web site) and disappears after the session is complete. This sort of cookie may be useful in keeping track of the visitor's activity on the web site 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 web site to customize the view for returning visitors. In the simplest model, the web site's host server may maintain a log that matches the stored text along with the user's IP

[193] *PIPEDA*, *supra* note 16, Principle 4 reads: "The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means."
[194] *Ibid*. Principle 5 reads: "Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes."

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 web site.

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 web site 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 even that it exists.

In many ways cookies are analogous to RFIDs from a privacy point of view. A cookie is a unique identifier which is automatically reported to the originating web server when it is re-visited. 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 labeling, an RFID can be placed on a product and can communicate the information stored on them to readers all without the consumer's knowledge.

Cookies have been in use now for some time, 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, or 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 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 web sites depends on the ability of the site to identify and track user activity on their site. 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 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.[195]

[195] *Working Document, supra* note 1, at 7.

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.[196] Assuming that the information gathered through the use of cookies is "personally identifiable" information, a web site 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 web site 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 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 them to the purchase. Use of the technology, therefore, does not inherently give rise to the application of privacy legislation – it is only use in certain ways that brings it under the scope of the Act.

Under the EU *Directive on Data Protection in Electronic Communications*,[197] the European Union has directly addressed the privacy concerns raised by the use of cookies. The preamble to the Directive recognizes that while cookies raise serious privacy concerns, they may also serve useful functions:

> 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.[198]

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 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.[199] The Directive states explicitly that, used properly, cookies may offer increased web site 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.

---

[196] See, for example, Stepen Luciw, "Website data collection raises many privacy issues", June 15, 2001, Lawyers Weekly, Vol. 21, No. 7.
[197] Directive 2002/58/EC of 12 July 2002.
[198] *Ibid*., at para 25. Article 6 of the Directive sets specific requirements for the collection, use and disclosure of "traffic data" which would include data gathered through the use of cookies.
[199] *Ibid*., preamble.

While it is true that in Canada, these norms could be derived from the interpretation of the basic Fair Information Practices already in place, 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 their application 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' expense or initiative.

Conclusions & Recommendations

In this report we have sought to provide a detailed and comprehensive analysis of privacy concerns and policy options with respect to emerging RFID technology. The report began with an overview of current and contemplated uses of RFIDs across a broad range of contexts. We then looked at the emerging discussions around privacy concerns and canvassed attempts at regulation, policy development and privacy advocacy initiatives outside Canada. Our focus shifted next to Canada, with a detailed analysis of the ways in which PIPEDA can apply to the use of RFIDs in the commercial context, as well as some of the gaps or deficiencies in that legislation.

It is clear that although RFID technology is not currently 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 is likely that it will 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 be easily used in conjunction with other data bearing instruments (such as loyalty cards or credit cards) to match product data with personal information in a way that allows for the compilation of highly detailed personal profiles of consumers. Further, the technology can be used in a variety of other ways that raise separate privacy concerns. These may include tracking individuals, drawing inferences about individuals, and monitoring employees. 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 possibility for private sector data to migrate to government agencies renders the privacy implications of private sector use of these technologies more urgent. It is no longer appropriate to consider private sector privacy issues in isolation from broader citizen privacy concerns. Technologies such as RFIDs, which enhance the capacity for consumer profiling, data matching, and other forms of surveillance, must receive intense policy consideration.

While it is reasonable to state that existing privacy norms and rules should apply to RFID technology, most notably the applicable private sector privacy legislation such as PIPEDA, it may not be sufficient to simply 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 regulations 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 a product

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

RFIDs have attracted the attention of privacy commissioners and privacy advocates around the world, as well as of numerous legislative bodies. The growing body of initiatives to address RFID related privacy concerns provides a fertile ground for determining appropriate policy approaches. The table below summarizes some of the main policy options considered or proposed in relation to RFIDs and privacy:

Table 2. Proposals for the Regulation of RFID Use in the Consumer Context

Proposed Measure	**Where Recommended**	**Possible Features**	**Comments**
Right/ability of consumer to destroy, disable or remove tags	International Conference of Data Protection and Privacy Commissioners (1), New Mexico (2), Massachusetts(3), South Dakota(4), EPIC (5), Ontario Privacy Commissioner (6), U.S. federal bill (7), Utah (8)	-mandatory for retailers to give consumers the option to have tags deactivated at point of sale -give consumers a "right" to have tags removed or deactivated	-deactivation may interfere with ability to use smart appliances, or to return/exchange products, or access warranties -concern that it puts too much onus of awareness on consumers – i.e. if they don't deactivate tags, they consent to having them read, used, etc.

Proposed Measure	**Where Recommended**	**Possible Features**	**Comments**
Labeling Requirements	EPIC (5), U.S. federal bill (7), Missouri (9), Utah(8), Massachusetts (3), New Mexico(2), Tennessee (10), New Hampshire (11), EPCglobal (12), Ontario Privacy Commissioner (6), EU (14)	-mandatory labeling on each tagged product item -mandatory signs in any store using RFIDs; or signs on shelves containing tagged items -mandatory signage to indicate presence of a reader -signage to indicate who is collecting the data -specific provisions re content of label: -that product contains RFID tag -that the tag can be used to track product before and after purchase - that it is possible to have the tag deactivated or removed -specific requirements re size/lettering of the labels: -clear and readable -contrasting background -use of a logo to identify tagged products combined with education as to the meaning of the logo (EPCglobal)	-any labeling requirement should be specific as to the kind of labeling that would be considered sufficient -labeling requirements should apply not just to items containing RFID tags, but to the presence and location of RFID readers

Proposed Measure	Where Recommended	Possible Features	Comments
Limiting Data Collection	California (13), Ontario Privacy Commissioner (6), EPIC (5), EU (14)	-data collection limited to point of transaction (not before or after transaction) -right to have personal identity information kept separately from RFID data -no use of RFIDs to track consumers in store -no collection of data from tags on the customer's person -storage only for so long as is necessary to meet the purposes of collection	-if tags are primarily of benefit for inventory control, it may be reasonable to limit the use of tag data to inventory control purposes -limit on collecting or using data from tags from other sources on consumer's person may be helpful
Placement of RFID tags	Massachusetts (3), EPIC (5)	-if RFID is not central to the operation of the tagged item, it must be on a tag, label, or packaging so that it can be easily removed and discarded	-this would help reduce concerns about the tracking of individuals due to the presence of tagged items on their person or in their homes or cars
Limiting Uses	New Mexico (2), Massachusetts (3), South Dakota (4)	-use of tag data limited strictly to inventory management purposes -data matching only for inventory purposes -no sharing of information with unaffiliated third parties	-the bills containing these provisions were contentious, and were defeated

Proposed Measure	Where Recommended	Possible Features	Comments
Consent	South Dakota (4), EPIC (5), EU (14)	-written consent required for any data matching -separate written consent required for sharing of information with third parties -deactivation of tags at checkout unless individual consents to them remaining active -no coercion to keep RFIDs active after point of purchase	-written consent requirements may be cumbersome and therefore impractical in retail context -some attention may need to be paid to whether a consumer is considered to consent to presence of RFID tag when s/he purchases a tagged item with a clear label indicating presence of RFID -can consent forms for loyalty cards, credit cards, etc. include provisions whereby the consumer consents to the matching of RFID data with their personal data? -what amounts to coercion to keep RFID tags active? Would this include advantages offered to consumers such as ease of return of merchandise?

References:

(1) International Conference of Data Protection and Privacy Commissioners, RFID Resolution, online: http://www.privacyconference2003.org/resolutions/res5.DOC.

(2) 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. Online: http://www.aeanet.org/governmentaffairs/gajl_HB0215newmexicorfid0205.asp.

(3) U.S., S.B. 181, *An Act Relative to Consumer Protection and Radio Frequency Identification Systems*, 2005, Reg. Sess., Mass., 2005. Online: http://www.mass.gov/legis/bills/senate/st00/st00181.htm.

(4) U.S., H.B. No. 1136, *An Act to regulate the use of radio frequency identification tags*, 80th Legis. Ass., Reg. Sess., S.Dak., 2005. Online: http://legis.state.sd.us/sessions/2005/bills/HB1136p.htm.

(5) Electronic Privacy Information Centre (EPIC), "Proposed Guidelines for Use of RFID Technology: Enumerating the Rights and Duties of Consumers and Private Enterprises", June 21, 2004. Online: http://www.epic.org/privacy/rfid/rfid_gdlnes-062104.pdf.

(6) Information and Privacy Commissioner, Ontario, "Tag, You're It: Privacy Implications of Radio

Frequency Identification (RFID) Technology", February, 2004, at 12. Online: http:// www.ipc.on.ca/docs/rfid.pdf.
(7) H.R. No. 4673, 108th Congress, 2d Session, June 23, 2004.
(8) U.S., H.B. 251, *Radio Frequency Identification – Right to Know Act*, 2004, Gen. Sess., Utah, 2004.
(9) U.S., S.B. 128, An Act to amend Ch. 407, RSMo.
(10) 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.
(11) U.S., H.B. 203-FN, *An Act relative to the use of tracking devices in consumer products*, 2005, Reg. Sess., N.H., 2005.
(12) EPCglobal Inc., *Guidelines on EPC for Consumer Products*. Online: http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html.
(13) U.S., S.B. 1834, An Act to add Ch. 22.7 (commending with Section 22650) to Division 8 of the Business and Professions Code, relating to Business, 2003-04, Reg. Sess., Cal., 2004, s. 22650.
(14) Article 29 Data Protection Working Party, "Working document on data protection issues related to RFID technology", January 19, 2005, 10107/05/EN. Online: http://www.europa.eu.int/comm/privacy.

It is clear from this table that while the policy options considered largely map onto the fair information practices that form the normative core of PIPEDA, in most cases the proposed legislation has been specifically tailored to the RFID context. If RFID technology is to be widely deployed in the private sector in Canada, it is important to develop RFID-specific standards and guidelines for the application of the PIPEDA norms.

Recommendation 1:
The Office of the Privacy Commissioner of Canada should develop RFID specific standards and guidelines for the application of PIPEDA norms.

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.

Recommendation #2
Consumers must be made aware of the fact that data collected in the private sector may be sought by government departments and agencies, and may be obtained without their knowledge or consent.

This report identifies governments' interest in the potential benefits of RFID technology and their role in driving its development. Therefore, we recommend that all levels of government in Canada assume a corresponding burden to ensure that

developments address citizen privacy concerns through the adoption of mandatory privacy impact assessment policies for government that are similar to that adopted by the federal government.[200]

Recommendation #3
All levels of government in Canada should adopt mandatory privacy impact assessment policies that would apply to new programs or initiatives undertaken by government agencies or departments.

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.

Recommendation #4
The appropriate level of government should consider legislation or regulations that would require manufacturers and retailers to use RFID tags only on removable hang tags or product packaging.

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.

Recommendation #5
RFID-specific guidelines should be developed to address the ways in which PIPEDA will apply to the collection, use and disclosure of personal information through RFIDs. The guidelines should take into account the following issues:

- *Clearly visible notice should be provided in each organization that uses RFIDs. This notice should indicate the purposes for which RFIDs are used by the store. Information should be provided as to how individuals can identify, remove or deactivate tags located in items that the individual might purchase.*

- *Clearly visible notice of the presence of an RFID should be provided on each product or package containing an RFID tag. Notice of this kind may be given through use of a logo only if individuals have been made sufficiently aware of the meaning of the logo.*

- *Clearly visible notice should be given of the presence and location of any RFID*

[200] Government of Canada, Privacy Impact Assessment Policy, May 2, 2002. Online: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp. The Ontario government has also adopted Privacy Impact Assessment Guidelines. Online: http://www.gov.on.ca/mbs/english/fip/pia/pia.html.

reader.

- *Any organization that matches RFID data with personal information through the use of personal information on loyalty cards, credit cards or other documents or devices should provide clear notice that it does so. In the case of loyalty cards, this notice should be in the loyalty card agreement. It should also be provided through signs or notices at the point of checkout.*

- *Any loyalty card, credit card or other device or document that is itself embedded with an RFID that can be read from any distance should be clearly labeled so as to indicate the presence of the RFID and the fact that it can transmit data from a distance.*

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 U.S. 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 reader, 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.[201] Further, the blocking of tags may also ultimately be regulated because of its potential to interfere with legitimate uses of RFIDs.

As the use of RFIDs becomes more widespread in ever more diverse contexts, it is easily conceivable that individuals may carry on their person RFID-enabled documents or cards that identify them personally. These may include loyalty cards, student ID cards, driver's licences, or other such identity documents. They must know that such documents may be read from a distance and used to match their identity with other information communicated from RFID tags in their clothing, on their person or in their possession.

The marked lack of general public awareness of RFID technology and its implications must be overcome through public education. When RFIDs are deployed, they will be difficult for ordinary individuals to detect, and they can be read without the consumer's knowledge. Consumers must be made aware of the existence of RFIDs, their potential uses and misuses, and consumer rights in relation to this and other forms of

[201] See, for example, "Tag You're It", *supra* note 7, at 19.

electronic data gathering and matching. Notice and labeling are central to reducing the invisibility of this technology. Coupled with public education, this approach will help consumers understand the technology and its implications and place the technology within the context of other technologies and practices.

Recommendation #6
Federal and provincial information and privacy commissions should be proactive in educating consumers about RFID technology and in informing consumers of their rights with respect to this technology. RFID technology should be explained in context with other data collection practices, taking into account the range and variety of tags that may be in the possession or on the person of any given individual, and with an eye to possible secondary uses of private sector data.