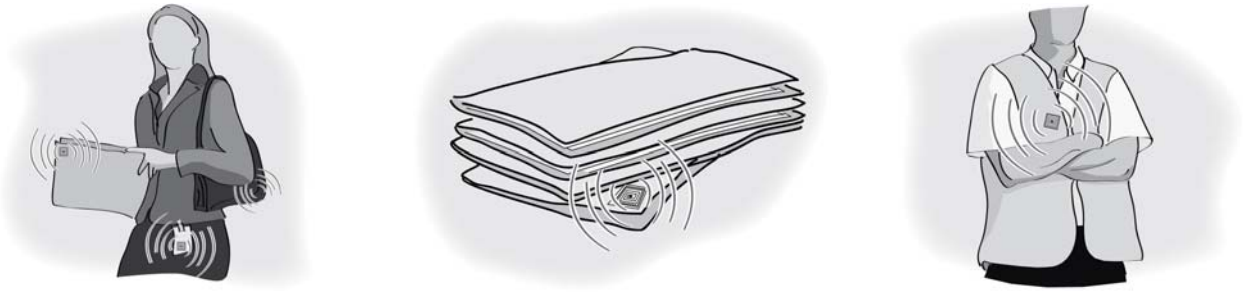
Office of the
Privacy Commissioner
of Canada

Commissariat à la
protection de la vie privée
du Canada



Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices

A Consultation Paper

March 2008

Radio Frequency Identification (RFID) in the Workplace: A Consultation Paper on Recommendations for Good Practices

Table of Contents

Executive Summary 1
Target Audience 2
Scope and Structure of the Consultation Paper 2
Introduction 4
PART I - RFID: Privacy Issues and Security Risks 5
1. What is RFID? 5
2. RFID in the Workplace 6
3. RFID Privacy Risks 8
3.1. Covert collection of personal information 8
3.2. "Function creep" and secondary uses 9
4. RFID Security Risks 10
PART II – Good Practices for RFID in the Workplace: Complying with Canada's Privacy Legislation 12
1. The Federal Public Sector – the *Privacy Act* 12
2. The Federal Private Sector – *PIPEDA* 12
3. RFID and personal information 13
3.1. Personal information written to a tag 13
3.2. A tag can become a "proxy" for the individual 14
3.3. Information about possessions can be manipulated to form a profile 14
3.4. Falling through the cracks? 14
4. Reasonable expectation of privacy in the workplace 16
4.1. Reasonableness and RFID Implants? 17
5. Good Practices for Using RFID in the Workplace 17
5.1. Accountability (Principle 4.1) 18
5.2. Identifying Purposes (Principle 4.2) 18
5.3. Consent (Principle 4.3) 19
5.4. Limiting Collection (Principle 4.4) 20
5.4.1. Technological Limitations on Collection 20
5.5. Limiting Use, Disclosure and Retention (Principle 4.5) 22
5.6. Accuracy (Principle 4.6) 22
5.7. Safeguards (Principle 4.7) 22
5.8. Openness (Principle 4.8) 23
5.9. Individual Access (Principle 4.9) 23
5.10. Challenging Compliance (Principle 4.10) 24
6. RFID in the Workplace – Conclusion 24
PART III – Consultation Questions 26
Appendix I – RFID Technology 28
Appendix II – Selected sources on RFID 29
Appendix III – Scope of Application of *PIPEDA and Privacy Act* 31
Endnotes 32

Executive Summary

The Privacy Commissioner of Canada prepared this consultation paper to set out good practice rules for organizations that seek to harness the benefits of RFID technologies. While RFID has potential applications across a wide range of sectors and activities, this document is focused on the use of RFID in the workplace. The Commissioner is concerned that Radio Frequency Identification (RFID) systems have the potential to be used as tools for surveillance, which could very much undermine the dignity and autonomy of employees. The central message of this paper is that where these technologies are deployed in a workplace, the deployment must be respectful of privacy and in conformity with Fair Information Principles.

The paper recognizes that there are already a variety of actual and contemplated uses of RFID in the workplace. RFID technology can be used to track tools, equipment or inventory, to monitor access to facilities or secure areas, or to monitor patterns of activity. RFID systems can also be designed to enhance security and safety. While some uses of RFID may offer benefits to employees, RFID in the workplace also raises important privacy concerns for employees. For example, it is most often people who are using the tools and equipment and moving the inventory, so by extension, their movements and productivity may be under greater scrutiny.

Part I of the paper provides a brief overview of RFID technology and the privacy and security risks involved in the use of RFID systems generally. Individuals who are already familiar with RFID technology would still benefit from reading the summary of privacy and security risks in this section as it provides background to the positions taken in Parts II and III of the paper.

Part II introduces the *Personal Information Protection and Electronic Documents Act* (*PIPEDA)*[1] and the *Privacy Act*[2] and talks about several ways in which the data contained on an RFID tag can become personal information. It discusses reasonable expectations of privacy in the workplace and refers to various findings as well as relevant court cases.

The paper then outlines the steps organizations should take, and the questions that should be asked, before proceeding with RFID applications in the workplace. In some circumstances, employers may rightly conclude that costs of some applications outweigh the benefits. Where they choose to proceed, the Commissioner offers good practices for organizations to follow based on Fair Information Principles.

Part III contains a series of questions to which we invite responses, but we welcome feedback on anything in this document. We welcome in particular the comments of those who are potentially directly affected by RFID in the workplace, namely employers, employees and trade unions as well as developers of RFID technology.

Target Audience

This consultation paper was written with several audiences in mind: employers who are contemplating, or already using, RFID technology to track employees or assets, but also employees and unions to raise their awareness of the issues. For these audiences, the paper avoids technical language where this does not sacrifice accuracy. However, the consultation paper was also written to encourage RFID vendors to be more accountable for the products they are developing. We are seeking feedback from all of these groups, as well as other interested parties, to clarify the recommendations for best practices made here.

Scope and Structure of the Consultation Paper

While RFID has potential applications across a wide range of sectors and activities, this document is focused on the use of RFID in the workplace. By issuing this consultation paper at this time, the Privacy Commissioner in no way wants to convey the message that she condones, or condemns, the use of RFID technology for tracking employees. Her objective is to set out good practice rules for organizations that seek to harness the benefits of RFID technologies so that these technologies may be deployed in a manner that is respectful of privacy and in conformity with Fair Information Principles. Creating a working environment that is respectful of employees' dignity and autonomy is a shared responsibility among employers, employees and trade unions.

This document is divided in three parts. Part I provides an overview of RFID technology and the privacy and security risks involved in the use of RFID systems generally. It deals with the state of technology as it currently exists and anticipates how it may develop to affect the right to privacy in the specific context of the workplace.

Part II provides an introduction to the *Personal Information Protection and Electronic Documents Act* (*PIPEDA)* [3] and the *Privacy Act*.[4] It sets out the views of the Office of the Privacy Commissioner on good practices for the use of RFID systems in the workplace in a manner that conforms with *PIPEDA* and the *Privacy Act*.

Part III contains a series of questions to which we invite responses.

In 2005 the Office of the Privacy Commissioner wrote to several large corporations in Canada whose business activities made them likely to use RFID. We asked them to help us understand the emerging use of RFID in Canada.[5] Only one organization stated that it was using RFIDs to track employees, but its use of RFID was revealing and something we felt needed to be addressed.

The organization told us that all employees carry access devices containing active or passive RFIDs. The use of some equipment, such as forklifts, is controlled through these devices. Records are kept of these readings, including attempts to access unauthorized areas or equipment. The activities of some employees are tracked for the purpose of determining the time spent in each activity as well as attendance. In addition, the organization stated that, in its view, it was not collecting personal information.

Nothing in this consultation document should be considered to interfere with or fetter the discretion of the Office of the Privacy Commissioner of Canada to carry out its responsibilities, especially with respect to any complaint filed by an individual under *PIPEDA* or the *Privacy Act*.

The good practices for use of RFID in the workplace set out in this document may need to be revised as more is learned about the impact of RFID technology on privacy. As the technology evolves and, as new RFID applications are developed, these good practices will be updated.

Introduction

> *"...privacy is an essential democratic value, because if we cannot maintain a sense of self and personal domain, we will be much less likely to exercise our other fundamental human rights."*[6] Professor Valerie Steeves, Presentation to The Standing Senate Committee on Social Affairs, Science and Technology on Bill S-21, to guarantee the human right to privacy, September 20, 2001.

The Privacy Commissioner of Canada is an advocate for privacy rights. In addition to investigating complaints and conducting audits, she has the authority to publish information about personal information-handling practices in the public and private sector, conduct research into privacy issues, and promote awareness and understanding of privacy issues by the Canadian public.

The Commissioner has been tracking the progress of Radio Frequency Identification (RFID) applications for some time and has expressed concern about this technology, particularly for human identification, in her Annual Reports to Parliament. She believes that RFID may have dramatic implications for privacy protection and that it is now necessary to identify good practices for organizations subject to the *PIPEDA* and the *Privacy Act*. While RFID has potential applications across a wide range of sectors and activities, this document has as its particular focus the use of RFID in the workplace.

There are already a variety of actual and contemplated uses of RFID in the workplace. RFID technology can be used to track tools, equipment or inventory, to monitor access to facilities or secure areas, or to monitor patterns of activity. RFID systems can also be designed to enhance security and safety. While some uses of RFID may offer benefits to employees, RFID in the workplace also raises important privacy concerns for employees. Such concerns have yet to be formally addressed in other studies and guidelines. Although the full nature and scale of likely use of RFID in the workplace is as yet unknown, the timing is nevertheless appropriate for the articulation of good practices.

The Commissioner recognizes that with RFID, as with other emerging technologies, capacities and applications can develop with extra-ordinary speed, making accurate predictions about the impact of the technology difficult. As a result, while this document identifies a series of good practices for the use of RFID in the workplace, it also solicits feedback on the application of Fair Information Principles to RFID technology in the employment context with a series of questions at the end of Part III.

As with all technologies, it is essential to address privacy issues inherent in RFID technology in advance of deployment. To do so allows employers to determine whether it is appropriate or necessary to use RFID technology. It pushes system developers to incorporate privacy features in the emerging technology in order to meet client demands. It empowers employees and the unions which represent them to take an active role in decision-making around the introduction of new workplace surveillance systems. It fosters the development of good practices before privacy invasive ones become entrenched. It helps identify systems that should not be deployed.

The protection of privacy is intimately related to human dignity and autonomy. Many Canadians spend a great deal of their time at work. The potential for increased workplace surveillance through the use of RFID technology must be addressed. The use of such technologies in a manner that is respectful of privacy is crucial to maintaining human dignity in the employment context.

PART I - RFID: Privacy Issues and Security Risks

1. What is RFID?

> *"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."*[7] Mark Weiser, "*The Computer for the 21st Century*".

The following description provides a very basic overview of RFID technology. More detail on the functioning of RFIDs is provided in Appendix I to this document. References for further reading are provided in Appendix II.

RFID is a generic term used to describe technologies that involve the use of data stored on small chips or tags which can be communicated to a reader from a distance by means of radio transmission. There are three basic components to the technology: the RFID tags themselves (which consist of an antenna attached to a microchip), the RFID readers, and the supporting database infrastructure (hardware and software). It is important to define the term RFID broadly, because the technical capabilities and distinctions among RF technologies will evolve over time.[8]

A significant feature of RFID technology is that tags do not require a direct line of sight for reading and may be read through hard material such as book covers or other packaging material. Further, more than one tag can be read at a time. Each tag can identify the specific object to which it is attached, even if that object is one of a multitude of identical items. When using bar codes, for example, one bottle of water has the same barcode as all other bottles of water of that particular brand. RFID technology enables each individual bottle to have its own unique ID.

RFID is a family of technologies that varies greatly in its level of sophistication and capacity. For example, supply chain tags, known as EPC (Electronic Product Code) tags, are designed to be simple, cheap and disposable. To keep the cost of the tag as low as possible, EPC tags carry very little data in on-board memory. By contrast, some tags have the capacity to store significant amounts of data, including biometric data.[9]

Other technologies in the RF family, such as contactless cards or "smart cards" are RF devices that may have additional layers of security.[10] Proponents of contactless card technology argue that it is a much more complex technology. For example, in secure card access applications, the contactless smart card-based device can verify that the reader is authentic and can provide its own authentication to the reader before starting a secure transaction.[11] As well, communication between the contactless smart card-based device and the reader can be encrypted to prevent eavesdropping. Yet from the perspective of employee and workplace privacy, smart cards and RFID tags raise essentially the same privacy issues. While smart cards may offer enhanced security and authenticity features, the good practices set out in this document are applicable equally to the collection of personal data through RFID and through the use of smart cards because both pose risks to privacy.

Not all devices that use radio frequencies are RFID technology. For example, anti-theft devices attached to consumer items in stores operate using radio frequencies, but they do not contain the unique identifiers that are a feature of RFID technology.

Sensors (or "motes") also form part of the wireless device RF family. Sensors are small hardware devices that respond to physical stimulus and produce an electronic signal, similar to RFID tags, which emit information about their environments, such as movement, light, temperature or humidity. Sensors generally contain batteries and can have similar applications to the more complex RFID tags, such as sensing whether or not a secure port container has been opened.[12]

There are also "chipless" RFID systems, where tiny chemical particles with varying degrees of magnetism respond when they are queried by a reader. A contemplated application for this RF technology would be embedding the particles in, or printing them on, paper and having readers placed inside copy machines to prevent unauthorized copying.[13]

To the extent that any of these technologies are used in the workplace to monitor the activities or whereabouts of employees, or to gather data on identifiable employees, the good practices set out in this document will apply.

2. RFID in the Workplace

> *"Workplace privacy is an important part of the basic autonomy rights of individuals in our society. People spend a big part of their lives in the workplace. What happens in the workplace – including whether privacy is respected – can have a profound effect on employees' sense of dignity, their sense of freedom, and their sense of autonomy. Continual surveillance is dehumanizing. It does not help create an enthusiastic workforce*."[14] Jennifer Stoddart, Privacy Commissioner of Canada, November 30, 2006.

People expect to have some privacy at work, even if they are on their employer's premises and using the employer's equipment. At the same time, it is normal that working for someone will mean giving up some privacy. Employers need basic information about their employees for things like pay and benefits, and they have to be able to ensure that work is being done efficiently and safely.[15]

But the monitoring of employees and their activities can be taken to a point where the employee suffers an unacceptable loss of privacy. Such a loss of privacy will have an impact on employee dignity and autonomy. Today, the possibilities for infringing on privacy in the workplace are greater than ever before. In addition to psychological tests, web-browsing records, video surveillance, keystroke monitoring, genetic testing and global positioning systems, employers now have RFID as an additional tool at their disposal to monitor employee activity. As the cost of implementing RFID systems drops over the coming years, organizations may choose to use RFID systems to track productivity, improve security and reduce theft.[16] There is the additional risk that employees with RFID devices and identity documents may be tracked outside the workplace.

Although RFID systems may bring benefits to employers and even, in some circumstances, to employees, a recognition of the advantages of the technology should not require a surrender of employee privacy. In developing this document, the OPC is firmly of the view that taking a proactive

stance in the development and deployment of new technologies can enhance privacy by ensuring careful and appropriate design and deployment of the technologies in a manner that anticipates and respects privacy concerns.

The Commissioner was concerned about the findings of a 2005 report about RFID use in the workplace produced by the RAND Corporation.[17] The report focused on six, large, private sector organizations in the United States. It found that some employers already use RFID technology to track employees and that the organizations did not have policies in place to govern these activities. Among the findings:

- Every organization indicated that the records collected by the RFID-enabled access control system were linked (via an employee's name or similar identifier) to other databases. In all cases, they were linked to personnel records and, in one case, to allergy-related medical records.

- None of the organizations in the study had developed a data retention policy and all of them were retaining the access control data indefinitely. Only one company had an enterprise-wide policy statement explaining the retention and uses of the records collected by the access control system, but it was only provided to select employees.[18]

Had a proactive approach to privacy been taken in the adoption and implementation of RFID technology in these cases, the deployment of the technology would likely have been carried out in a very different manner.

RFID is already being used in some workplaces. For example:

- IBM is marketing a system to use an RFID tag embedded in customized identification badges. A network of receivers throughout the site picks up the unique signal transmitted by each tag and the system calculates the exact location of the tag at that moment.[19]

- A casino in Sydney, Australia uses RFID to manage its inventory of over 80,000 uniforms, which have a value of almost two million US dollars. The casino addressed its laundry-tracking problems by placing RFID tags in each uniform. Uniforms are tracked throughout the system by strategically placed readers.[20]

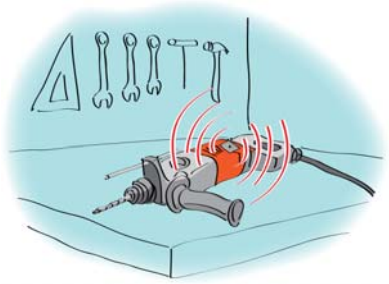
- In July 2005, one of the UK's largest trade unions, the GMB, demanded an end to RFID for staff tracking in European grocery stores, claiming an invasion of workers' privacy. Workers were asked to wear small computers on their wrists, arms and fingers which instructed them as to where to go and what to do.[21]

If an RFID tag on a tool or object in the workplace is read in context with other chipped devices, such as the employee's identification card, the potential for employee surveillance becomes very real. Stephanie Perrin notes:

> *. . . tool inventory control is a major cost for many service industries, so tools that remember where they have been and what they did there may become hot sellers. The value of tool tracking may be considered to be higher than the dignity of the workmen who use the tools.*[22]

In the employment context, the tracking of the movement of workers may be an explicit goal in the adoption of an RFID system. Already some companies are engaged in fairly elaborate experiments with tracking assets and employees through RFID. For example, IBM is engaged in a pilot project with a leading global petrochemical company which is piloting a comprehensive location awareness and asset tracking system. They have approved plans to move forward with additional locations. The system includes:

- Active RFID tags worn by personnel in critical work environments.
- Receivers to detect RFID tags within each physical area entrance and continuously update location in virtual real-time.
- Automatic updates from human resource systems verifying worker certifications and authorizations to restricted zones.
- Alerts generated if safety or security zones are breached.[23]



Sophisticated and expensive devices, which combine RFID and Global Positioning System (GPS) technology, are capable of providing continuous and fairly precise geographical data. If the tags can then be associated with an individual, then by that association the individual's movements can be tracked. To illustrate, a GPS tag system, proposed as a means to track city public works equipment in Montreal, was seen by some as an indirect means to monitor the work habits of city employees.[24]

RFID tags have also been contemplated for use with employees engaged in high risk activities, such as firefighters or soldiers. The tags may allow rapid access to identification and medical information of individuals who are badly injured and unconscious.[25]

These examples provide some insight into how the privacy rights of workers may be affected by the adoption and implementation of workplace RFID systems. The potential impact on privacy is discussed in greater detail below.

3. RFID Privacy Risks

RFID systems raise new privacy risks in addition to other forms of surveillance of employee activity, such as video and keystroke monitoring. RFID tracking in the workplace, because it includes both locational information and date and time information, makes it possible to automate the tracking of employees and also to become more precisely aware of their interactions with other employees. The greater the degree of surveillance of employees, the lesser the degree of privacy and, ultimately, of dignity and autonomy in the workplace.

There are certain risks that, while also present with some other surveillance technologies, must be highlighted when discussing RFID. These are outlined below.

3.1. Covert collection of personal information

RFID technology has the potential to be located anywhere and everywhere. RFID tags are small and can be embedded onto objects and documents without the knowledge of the individual who obtains those items. Research to reduce the size of tags is progressing rapidly. For example, Hitachi

announced a few years ago its very small (less than 0.4mm) mu-chip passive tag could be embedded in paper to track documents.[26] More recently, it has developed much smaller RFID "powder" that could be used for similar purposes.[27] Eastman Kodak is even developing an ingestible RFID tag that could be incorporated into medication.[28]

As radio waves travel easily and silently through fabric, plastic, and other materials and are not restricted to line of sight, it is possible to read RFID tags sewn into clothing such as uniforms, or affixed to objects contained in pockets, purses, backpacks, and more. Tags can be read from a distance, by readers that can be incorporated invisibly into nearly any environment where human beings or items are present. A tag may be read from longer distances than expected if the range of a reader is increased. It may not, therefore, be readily apparent that RFID technology is in use, making it virtually impossible for a person to know if he or she, or any items in his or her possession, are being "scanned". Thus, depending on how RFID is being used in the workplace, the employees may be completely unaware that they are being monitored, or they may be unaware of the full extent of the monitoring.

It is possible that RFID tags deployed by an organization may be "read" by unauthorized readers. Thus, the presence of RFID tags may expose employees to the risk that their movements and activities may be tracked by someone other than their employer, and possibly for illicit or harmful purposes.[29]

Developments in technology, and in particular nanotechnology, may increase the capacity to conduct covert surveillance. While we are reaching the physical limits of the storage and processing capacity of today's computers, nanotechnology will allow for the creation of infinitely smaller, much more powerful computing and sensing devices. These devices could be placed throughout our natural environment and not be visible to the human eye.[30]

3.2. "Function creep" and secondary uses

The original purposes for which an RFID system is introduced into the workplace may evolve over time and may result in increased surveillance of individuals by tracking more and more of their activities. For example, Helsinki International Airport had been using RFID technology to log ground staff working hours. In 2006 it announced that it will now also use RFID to track all ground staff tasks.[31]

In addition, data gathered using RFID may be sought by others for purposes unrelated to employment. For instance, users of toll payment systems that require the use of RFID transponders in vehicles have had their records subpoenaed in divorce cases for the purpose of proving claims of marital infidelity. The records may assist in determining where an individual's car was at a particular time.[32]

It is possible that information gathered in the workplace for the purpose of tracking inventory or equipment and linked to identifiable individuals might be used for purposes of employee discipline, or even for the purposes of criminal investigation or prosecution.

Further, government agencies and departments may seek access to data held by organizations for a variety of purposes, including the investigation of crimes, threats to national security and the enforcement of other laws. It is also conceivable that RFID-based data could be obtained to monitor and track individuals who are associated with unpopular political causes.

4. RFID Security Risks

Several different RFID security risks have been identified.[33]

- Forging tag contents: While read-only RFID tags cannot be overwritten, and should be more difficult to exploit, the contents of writable, un-protected tags can be easily altered. For example, data on a tag associated with one item could be captured by an attacker and pasted onto the tag of another item.

- Physical manipulation: A tag could be removed from one item and attached to another. For example, an RFID tag attached to a laptop containing sensitive information could be left on a desk or attached to another asset. Where RFID tags are embedded in employee uniforms or name tags, persons other than the employee may use the tag or uniform, leaving a false record of the movements or activities of the employee.

- Cloning: Wireless pickpockets can use cloning devices to capture tag information. For example, an RFID-enabled employee access badge can be cloned in a parking lot, granting an attacker access to the workplace without authorization. More complex tags that use encryption have been successfully hacked in brute force attacks. Even the implantable RFID tag has been cloned, so the attacker could use the information to gain access to anything the tag points to, such as medical records.[34]

- Eavesdropping: By tapping into the RFID transmissions a third party can gain access to the same information sought to be recorded by the employer.

- Replaying: An attacker may intercept a valid transmission and then repeat it.

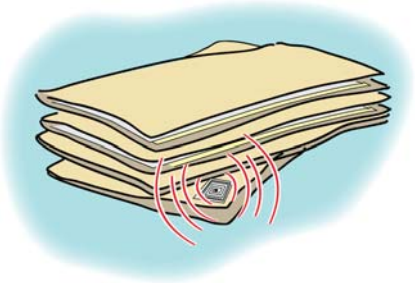
- Infecting the tags: Researchers have discovered a way to infect RFID tags with a computer worm, so that products and ID cards could be used to spread malicious code.[35]

While many of these security risks have their most direct impact on the business operations of organizations, they may also have ramifications for employees. Employees may be called to account for their actions where records created through a third party's illegal use or appropriation of their tags or of a smart card show that the employee improperly accessed a restricted area, was the last person to use a missing piece of equipment, and so on.

RFID security issues may be addressed through a variety of means including policy, process and technology. There are clear advantages to addressing security and privacy issues prior to the adoption and deployment of this technology, whether it be through policy, process or technology design. In some instances, these risks may be avoided by the simple decision not to use an RFID-enabled device.

Privacy and security are terms that are often confused or conflated. Proper data security is certainly required by privacy laws, as insecure data or systems can pose a severe risk to privacy. Yet an organization cannot meet its legal privacy obligations merely by ensuring that data is collected, used and disclosed in a secure manner. The collection, use and disclosure of personal information must be carried out in a manner that is consistent with the Fair Information Principles embodied in privacy legislation.

PART II – Good Practices for RFID in the Workplace: Complying with Canada's Privacy Legislation



There are no specific requirements in Canada for organizations using RFID to inform individuals about the presence of the technology, its purpose or how the information gathered will be used. However, if an organization is gathering personal information, then privacy laws apply. And when the data collected, used or disclosed through an RFID system are linked to an individual, privacy issues are raised. Depending on the nature of the workplace, the norms contained in *PIPEDA* or the federal *Privacy Act* may apply. These statutes and their application are addressed in greater detail in this Part.

1. The Federal Public Sector – the *Privacy Act*

The federal *Privacy Act*, which applies to the federal public sector,[36] provides some safeguards with respect to the public sector use of RFID. For example, sections 4 to 8 of the *Privacy Act* set out a collection, use and disclosure framework for the personal information-handling practices of the federal government. There are Treasury Board policies governing the management of personal information holdings,[37] the Government Security Policy,[38] an Employee Privacy Code[39] as well as the Treasury Board Privacy Impact Assessment Policy.[40] A Privacy Impact Assessment is a process that helps an organization determine whether a new technology, information systems or initiative meet basic privacy requirements.

The *Privacy Act* would better protect privacy rights if the legislation were updated to reflect the growing use of such technologies. The *Privacy Act* has not been substantially amended since it came into effect in 1983, long before personal computers, the Internet, wireless communications and other communications and information technologies revolutionized Canadian society. In June 2006, the Commissioner tabled a report with the Standing Committee on Access to Information, Privacy and Ethics outlining proposed reforms to the Act.

While federal government institutions are subject to the *Privacy Act*, Treasury Board has introduced a more comprehensive criteria based on *PIPEDA* through the Privacy Impact Assessment Process. These *PIPEDA*-based criteria should be considered by federal government institutions to improve their personal information handling practices.

Given the focus on the *PIPEDA*-based criteria in Treasury Board's own materials, this Office is of the view that the discussion of the application of *PIPEDA* to RFID applications is relevant to organizations governed by the *Privacy Act*.

2. The Federal Private Sector – *PIPEDA*

PIPEDA applies to personal information that is collected, used or disclosed in the course of commercial activities by federal works, undertakings and businesses and organizations that collect, use or disclose personal information in the course of commercial activities. *PIPEDA* is a general law that applies to the

collection of personal information regardless of the technology that is used. *PIPEDA* applies throughout Canada except in those provinces—British Columbia, Alberta and Quebec—that have substantially similar legislation governing the private sector, and in Ontario with respect to certain matters governed by the *Personal Health Information Protection Act*.[41]

PIPEDA 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*.[42] This can involve diverse types of organizations. Explicitly included in the definition of "federal work, undertaking or business" in *PIPEDA* are employees of banks, airlines, inter-provincial railways, ferries and shipping lines, and radio stations. Other organizations will also fall under the definition. For example, the Commissioner has already issued findings concerning an Internet service provider and a nuclear power plant.

There is a patchwork of laws protecting employee information in Canada. The personal information of employees in organizations within the broader private sector is not generally governed by *PIPEDA*, although the provinces of Alberta, British Columbia and Quebec have privacy legislation which protects personal employee information. In addition, provincial government employees may be covered by the relevant provincial public sector privacy statute, and these statutes may also cover employees in public institutions such as universities and hospitals.

Where *PIPEDA*, or the *Privacy Act*, is the legislation that appears to apply, there is another question to answer. To trigger the protections under these laws, the information that is collected, used or disclosed by means of RFID technology must meet the definition of "personal information" in these laws.

3. RFID and personal information

Under *PIPEDA*, "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."[43] Where it has been determined that employee information is subject to *PIPEDA*, then application of the Act will depend on whether the information that is collected, used or disclosed by means of RFID technology is personal information.

Under the *Privacy Act*, "personal information" means "information about an identifiable individual that is recorded in any form."[44] The Act contains a detailed list of examples of the kind of information that can be considered personal information, as well as some exceptions. The courts have interpreted the term "personal information" quite broadly.[45]

There are several ways that the data contained on an RFID tag can become personal information.

3.1. Personal information written to a tag

If the microchip in the RFID tag has personal information of an individual written to it, then it is a repository of personal information. This could include, for example, the person's name and address, an identifier uniquely linked to a person, or biometric information, such as a fingerprint, in digital form.

3.2. A tag can become a "proxy" for the individual

An RFID tag containing a unique identifier has the potential to become a "proxy" for an individual when it becomes associated with that individual. In such circumstances, it will become personal information. This would be the case with an RFID-enabled identification badge or uniform. Location data gathered by scanning tags associated with individuals is also personal information. Several cases illustrate circumstances where information can become personal information through its association with a particular individual.

In *PIPEDA* Finding #319, the Assistant Privacy Commissioner found that an IP address can be considered personal information if it can be associated with an identifiable individual, but a port address is not personal information as it is not linked to an identifiable individual.[46] Following this logic, the Assistant Commissioner would consider the data on an RFID tag that can be associated with a particular individual to be personal information.

In *PIPEDA* Finding #270, the Assistant Privacy Commissioner found that an individual does not have to be named for something to constitute his or her personal information. If the situation renders the individual identifiable, then the information at issue will be considered personal information under *PIPEDA*.[47]

Similarly, in a decision under Alberta's *Personal Information Protection Act*, the investigator stated, in the case of information captured by video surveillance: "When a surveillance camera is switched on it is capturing information. If an individual in the frame can be identified, then the captured image is "information about an identifiable individual."[48] In another Investigation Report, the Alberta OIPC investigator addressed an issue similar to the one raised here. In that case, information recorded about events leading up to a car accident by the car's event data recorder (EDR) was held to be the personal information of the driver, as the information sought constituted information about a driver whose identity was known. The investigator noted: "Precision was seeking to obtain detailed information about the manner in which E.P. was operating the vehicle prior to the crash. I am therefore satisfied that the EDR data is in fact "information about an identifiable individual" as contemplated by PIPA."[49]

3.3. Information about possessions can be manipulated to form a profile

Information about possessions that can be manipulated or processed to form a profile is personal information. This is the case whether the information was gathered through multiple visits to a facility or organization, or through access to a database recording activities of certain tags that were manipulated by an individual. For example, PricewaterhouseCoopers announced in 2006 that it will be using an RFID-enabled "Real Time Location System" in their Mexico City office to track when laptops and other portable items move outside of a particular zone. The database will record the item's location, who moved it, and whether the movement is authorized. It will trigger an alarm if the movement is not permitted.[50] All of this information would contribute to building a profile of an individual's activities.

3.4. Falling through the cracks?

A difficult area emerges in the workplace context. In some cases, information is about both the individual employee and the work they perform. If the predominant characteristic of the information is that of the employment and not the employee, then the information is information produced at

work and it is not considered to be personal information. For example, in *PIPEDA* Finding #14, the Privacy Commissioner found that the prescribing habits of physicians did not meet the definition of personal information. The OPC would discourage organizations from applying this reasoning more broadly.

It is worth noting that the Assistant Privacy Commissioner has found nothing in *PIPEDA* to indicate that business information and personal information must be mutually exclusive. In *PIPEDA* Finding #220, the Assistant Privacy Commissioner argued that the sales records attributed to the complainant to show her performance relative to others were personal information for the purposes of the Act.[51] As Scassa *et al*. have suggested: "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."[52]

The approach of the OPC, as set out in its submission to the Standing Committee on Access to Information, Privacy and Ethics, is to "look at *how information is used*, and not *where it is produced*."[53]

The difficulty of characterizing some information is also illustrated in *Dagg v. Canada*,[54] where an access to information application requested employee sign-in sheets for weekend access to a building. The Department provided part, but not all, of the information on the basis that the information about the comings and goings of identifiable individuals was personal information. The Court decided that the information related to the individual's position, and not to the individual. While the Court noted that there was a privacy interest at stake, it found that this information related to the functions of public officials. This connection to public duties was enough for the Court to decide that the right of access takes precedence over the right to privacy.

These cases show the difficulties of dealing with "hybrid" information – information that is both personal information and a record of some other sort. In *Dagg*, the tension was between personal information and information about the activities of public officials. In Case Summary #14, it was between personal information and information produced at work. The problem of hybrid information is raised in the context of workplace surveillance, as video, audio, or keystroke surveillance of employees workplace activities might not fall under *PIPEDA* if the records of the surveillance were considered to be information produced at work.

Even where personal information protection legislation contains a definition of "work product information", as is the case in British Columbia,[55] it can be difficult to determine what amounts to work product information.

However, it seems clear, through our findings and a number of labour arbitration cases,[56] that information gathered about an employee using workplace surveillance techniques is considered personal information, and that privacy norms apply.

We would caution employers to be extremely wary of relying on a loosely defined concept of "work product" to avoid addressing Fair Information Principles in workplace surveillance systems, such as those involving RFID technology.

4. Reasonable expectation of privacy in the workplace

Section 3 of *PIPEDA* states that the purpose of the legislation is to establish the 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. Subsection 5(3) confirms that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

The concept of the "reasonable person" and his or her expectations thus plays a key role in setting the boundaries between legitimate and intrusive practices in the workplace. If an employer's collection, use or disclosure of personal information about employees is not one that a reasonable person would consider appropriate in the circumstances, it will violate the norms set out in the legislation. Thus, the first step is to enquire into the reasonableness of any collection, use or disclosure of personal information.

Employers have legitimate requirements for collecting personal information about their employees. They need to know who they are hiring. They need to address performance issues and to ensure the physical security of their workplace. They may see electronic monitoring and other surveillance practices as necessary to ensure productivity, stop leaks of confidential information, and prevent workplace harassment.[57]

However, the existence of a legitimate objective does not mean that the measure chosen to achieve it is also reasonable in the circumstances. The possibility that an individual employee might do something harmful does not justify treating all employees as suspects. The questionable benefit of knowing what every employee is doing on company time and equipment, at all times, needs to be weighed against the cost. This includes the impact on staff morale and trust.[58] There is a body of labour arbitration case law that rejects the sweeping use of surveillance in the workplace as unreasonable.[59]

The loss of privacy must always be weighed against the benefits of data collection, and the purposes for the measure must be grounded in a defensible need. To assess the appropriateness of using RFID for employee monitoring purposes, it is useful to consider the following four part test applied by the Federal Court in *Eastmond v. Canadian Pacific Railway*:[60]

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?

In *PIPEDA* Finding #279, the Assistant Commissioner found that using video surveillance to monitor employee productivity contravened Section 5(3) of the Act. The Case Summary includes some general observations about using video surveillance to monitor employee productivity and these provide some insight on how the Assistant Commissioner might view productivity monitoring using RFID technology:

> *The Act... demands that the cost to human dignity form part of the equation. Continuous, indiscriminate surveillance of employees... was based on a lack of trust and treats all individuals with suspicion when the underlying problems may rest with a few individuals or with a management plan that may not be entirely sound. The effect... of such omnipresent observation was stifling. While it may prevent undesirable behaviour, it also forces the employee to call into question every potential action, every potential comment no matter how benign. The goal of ensuring adherence to the company's vision comes at too high a price to our individual autonomy and freedom.*[61]

In Finding #281,[62] the Assistant Commissioner reflected on whether the loss of privacy, from the collection and use of a biometric voice print, was proportionate to the benefits the company would likely gain. She found that the voice print, used solely for one-to-one authentication purposes in a voice password system, was not unduly invasive. It had been explained to employees, and the Assistant Commissioner felt that an alternative concurrent system would not ensure the desired level of security and thus would not meet those purposes. The complainant pursued the matter but did not persuade the Federal Court.[63] The Federal Court of Appeal recently upheld the Federal Court's decision, agreeing that a reasonable person would find the collection and use of a biometric voiceprint in a voice password system reasonable in the circumstances.[64]

4.1. Reasonableness and RFID Implants?

Some may argue that there are certain occupations for which implants might be a reasonable option for limited purposes, such as trying to locate a soldier or firefighter who needs to be rescued in an emergency. The need for a high level of security may also be cited. For example, one Cincinnati based company recently implanted tags in the forearms of two employees as a means of providing secure restricted access to vaults containing highly sensitive data.[65] But is it necessarily more beneficial to have the RFID tags implanted rather than present in a uniform or badge or worn on an anklet or bracelet? If hiding the RFID for security purposes is the rationale for the implant, it must be recognized that an attacker, as well as a rescuer, may have a reader that will pick up the implant to locate the sought after individual. As well, there would be no employee escape, in off-hours, from an implant.

Implanting employees with RFID tags against their will is unacceptable under any circumstances. Such activity raises fundamental human rights concerns, including bodily integrity. Employment should never be made contingent on a willingness to be implanted with an RFID tag. Indeed, it may be appropriate to consider legislation that would flatly ban the use of subdermal RFID implants except in extraordinary circumstances.

5. Good Practices for Using RFID in the Workplace

This section outlines the steps organizations should take and the questions they should ask before proceeding with RFID applications in the workplace. In some circumstances, employers may rightly conclude that costs of some applications outweigh the benefits.

Schedule 1 of *PIPEDA* contains the Fair Information Principles. As mentioned earlier, the Treasury Board makes use of *PIPEDA*-based Fair Information Principles in its Privacy Impact Assessment

Process[66] for federal government institutions that are governed by the *Privacy Act* and we have taken a similar approach by using the *PIPEDA*-based criteria.

It would be important for organizations to consult the precise wording of these Principles[67] as a starting point for ensuring compliance with the *PIPEDA*. The next step would be to apply the more focused guidance outlined below to the RFID application under consideration. This section is followed by a series of consultation questions.

5.1. Accountability (Principle 4.1)[68]

Someone within the organization must be accountable for the use of RFID systems. It must be easy for employees to find out who this person is so that they can ask questions.

The individual accountable for privacy compliance should be involved in the design of any RFID system and should complete a Privacy Impact Assessment[69] (PIA) on its application in advance of deployment. By addressing privacy at the design stage, organizations can help ensure that their RFID-related activities comply with Canada's privacy laws and meet their employees' reasonable privacy expectations.

The responsible individual must be aware of all collections of personal information by the RFID system and all subsequent uses, disclosures and the retention period. This may include procedures for approving new and unanticipated uses of information gathered by RFID systems and ongoing PIAs. This might also extend to preparing procedures for dealing with unauthorized uses of access control records.

Any data from the RFID system that is transferred to a third party for processing must be protected by a contract that provides comparable protection while it is being processed.

The components of an RFID system must be labeled or coded with the identity of the organization that is responsible for them. Without knowledge about the device that is collecting data, it would be difficult to satisfy the principles of Openness and Accountability."[70]

5.2. Identifying Purposes (Principle 4.2)

Organizations can balance their "need to know" with their employees' right to privacy, if they ensure that they collect, use, and disclose personal information about their employees for appropriate purposes only.

The "identifying purposes" principle requires organizations to identify the purposes for which personal information is collected at or before the time the information is collected. In the employment context, this can be done through personnel manuals, policy statements or other such documents, providing they are made easily available to employees. More importantly, however, the components of all RFID systems should be identified and marked to make their use clearly evident and transparent.

Employees must be notified of the purposes for which personal information is collected using RFID technology. It is a good practice to break down and identify as specifically as possible the purposes for the use, collection and disclosure of information gathered through the use of RFID tags.

RFID technology could be designed to address the identification of purposes. Indeed, building Fair Information Principles into technology is not a new idea. Some work is being done to build Fair Information Practices into the communication between RFID readers and tags. For example, Floerkemeier *et al* have showed how separate purpose "declarations" could be used for different reader queries to identify the specific purposes for which a tag is being read. They identify fourteen such purposes, which include, for example: "Access control" ("Tag IDs are scanned for the purpose of access control, e.g., by identifying a pass holder or by authorizing the validity of an access key."), "Anti-theft", "Asset management" (where "tags are read to provide a picture of the whereabouts of assets."), and "Emergency services" ("The system is monitoring tags to provide rescue workers with occupancy information.")[71]

However it is accomplished, all purposes for which personal information is collected must be identified. Collecting information about the location of an item for the purpose of monitoring its movements potentially enables the tracking of people through association with the unique identifier in the RFID tag. For example, the tracking of a piece of equipment within the workplace may indirectly provide the employer with information about the activities or whereabouts of the employee who is authorized to use that equipment. If the tracking can be justified as reasonable, then this purpose for the collection of personal information must be separately identified (see "Limiting Collection").[72]

5.3. Consent (Principle 4.3)

Consent is a cornerstone of the Fair Information Principles. If an organization wishes to collect personal information using RFID technology, the organization, having notified employees of the purpose for which the information is being collected, must also obtain their consent.

Principle 4.3.2 requires both the *knowledge and* consent of the employee for the collection, use or disclosure of personal information. In *PIPEDA* Finding #273[73], the Assistant Commissioner found that the organization had not made reasonable efforts to inform its employees of the limited video surveillance it was undertaking (which the Assistant Commissioner found to be reasonable in this situation). The employer had posted a memorandum to notify the employees about how the information being collected by the cameras would be used, but the employees were not aware of the memorandum in question. To resolve this complaint, the Assistant Commissioner recommended that the organization develop and make available a policy document on the use of the surveillance cameras, following the components set out in Principle 4.1.4.

Because RFID systems in the workplace are a relatively new (or perhaps just unnoticed) phenomenon, many employees will be unfamiliar with the technology, how it operates and how data is collected, used and stored. Organizations implementing an RFID system should do more than make available documentation about it, they should educate employees.

Organizations should note that in *Englander v. Telus Communications Inc.*,[74] the Federal Court of Appeal confirmed that an organization needs to make an effort to help individuals understand their privacy rights. It ruled that organizations have primary responsibility to inform individuals about the primary and any secondary purposes motivating a collection, use or disclosure of any personal information, as well as their options in a particular information bargain, including any ability to opt out of a particular collection, use or disclosure of personal information. At issue in *Englander* was a cell phone customer's decision to allow his name, address, and phone number to appear in the telephone

directory. The court found that Telus violated *PIPEDA* by failing to make a reasonable effort to ensure its customers were advised of the purposes for which personal information would be used, and by failing to adequately advise customers of their ability to opt out of the publication of their information in the public telephone directory.

Under *PIPEDA*, consent must be free and informed. A question that often arises in the context of *PIPEDA* is whether an employee's consent to the collection and use of their personal information in the workplace, required by their employer as a condition for continuing employment, can be considered to be truly voluntary consent. Decisions by the employer to introduce video-surveillance cameras, GPS systems, and biometric security systems, are some of the examples we see of a growing trend towards increased workplace surveillance for multiple purposes, including security, product safety, performance management and/or business efficiency.[75] RFID technology adds yet another dimension to this surveillance. It should be remembered that any collection, use or disclosure of personal information *must* meet the test of what the reasonable person would consider appropriate in the circumstances. An employee certainly cannot be required, as a condition of employment, to consent to an information gathering practice that would not meet this test of reasonableness.

Under Section 7 of *PIPEDA*, there are several situations where personal information can be collected, used or disclosed without the individual's consent. These include the collection of information "for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province" where seeking consent would "compromise the availability or the accuracy of the information".[76] In *Eastmond v. Canadian Pacific Railway*, the Federal Court was of the view that this exception applied to video surveillance in the workplace aimed at detecting theft.[77] Exceptions to the requirement of consent also apply to the collection of information by an organization for disclosure on its own initiative to government of matters related to national security, the defence of Canada or the conduct of international affairs. These exceptions may prove to be important in the context of RFID technology, as RFID creates the potential for organizations to collect unprecedented amounts of personal information. Employers, employees and trade unions should be aware of the issues raised by the presence of these provisions in the Act.

5.4. Limiting Collection (Principle 4.4)

The limiting collection principle mandates that information cannot be collected indiscriminately, but must be limited to that which is necessary for the identified purposes. In the employment context, it is often difficult for an employee to determine whether an organization is adhering to this practice as, in most cases, the employee cannot be certain whether data collection is taking place in a non-compliant manner or for purposes beyond the scope of those which have been identified.

Organizations need to ensure that any data collection is directly related to the reasonable and legitimate purpose(s) to which the employee has consented.

5.4.1 Technological Limitations on Collection

Mechanisms to limit collection could include screening out transmissions from non-targeted tags. Specifically, rather than issuing indiscriminate read commands and then filtering to retain the tags of interest, reader queries could target only relevant tags.[78] It is a second best option to dump data immediately that it was not necessary to collect in the first place.

Organizations could configure the technology to recognize distinct collection practices. For example, Floerkemeier *et al* identify four of these:

- Anonymous Monitoring: This allows for the collection of information without the need to know the unique ID of any given tag. Floerkemeier uses the examples of sensor applications such as automatic door openers or the counting of the number of items in a given area.[79]

- Local Identification: This is used to identify the presence of a certain item in a particular area, but does not show where it has come from. Revealing the past locations of an item would not be permitted without an appropriately strong justification, such as a criminal investigation. A declaration of use only for local identification would provide the employee with some assurance that his or her movements would not be tracked across different locations.

- Item Tracking: This practice goes beyond local identification and involves the tracking of items as they move from one location to another. This has the potential to enable the tracking of employees through association of the employee with the unique identifier in the RFID tag.

- Person Tracking: A workplace system might be designed to collect information about an employee's location or movements. This might be done, for example, through RFID tags in ID cards or uniforms. It is also possible that such information can be gleaned from item-tracking, if the item in question can be associated with an identifiable individual. If item-tracking is also used to track persons, this additional purpose for collection must be identified.[80] Person tracking will almost certainly raise more substantial privacy issues than item tracking.

These collection declarations can be used to selectively allow tags to remain anonymous, whenever possible.[81] With this in mind, organizations should consider the 4-point test that the OPC has used when assessing the reasonableness of the data collection (see Section 4).

Whenever possible, anonymous monitoring should be used instead of monitoring that could identify the employee. Anonymous replies are already part of some RFID protocols.

Floerkemeier *et al* also suggest that a sophisticated version of an ordinary RFID tag, a so-called "watchdog tag," could be used to provide transparency to the otherwise invisible tag detection process. It could be used in conjunction with the other built in privacy features discussed above. The tag would decode the commands sent by the reader and make them available on a screen for inspection. This type of watchdog tag could log all data transfers so that they could be provided to employees upon request. The watchdog tag could be a discrete device or its functions could be integrated into a mobile phone.[82] The watchdog tag could be an enhancement to transparency, in that it could set out the operator's identification, the purpose and type of data collection and the target range of tags.

5.5. Limiting Use, Disclosure and Retention (Principle 4.5)

Organizations must not use or disclose personal information for purposes other than those for which it was collected, unless the individual consents or the law requires it. In cases where information has already been collected and the organization wants to use or disclose the information for a new purpose, employee consent is required. For example, if an employer has collected information using RFIDs for the purpose of tracking equipment, then linking this information to employee personal information and using it for disciplinary purposes would be beyond the scope of the original collection.

Organizations should avoid using RFID systems to collect information for disciplinary purposes prior to assessing the situation through the lens of the 4-part reasonable person test.

Information that is inadvertently collected should be immediately disposed of in a secure manner. Organizations must retain personal information only for as long as necessary to achieve the purposes for which it was collected. When the information is no longer required, it must be disposed of immediately, in a secure fashion, taking into consideration requirements for employees' right of access.

5.6. Accuracy (Principle 4.6)

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

Organizations may encounter a scenario where employees contest the accuracy of the information gathered using an RFID system. For example, an employee may challenge their registration on a reader that they claim not to have experienced.[83] It is possible that other individuals might use uniforms, badges or other items embedded with RFID tags containing information pertaining to an employee, with or without the employee's consent. As well, whether a tag can be hacked and the data altered will be of major concern for organizations, unions and employees. For example, an RFID-enabled badge of an employee in an airport or nuclear facility might be an attractive target for an unauthorized person seeking access to a secured area.

Vendors should provide organizations and employees with a risk analysis of the accuracy of information their RFID system will provide, based on the particular applications. With this information, organizations and employees will know the perceived limits of a particular RFID system and be in a better position to know when to challenge conclusions derived from it.

5.7. Safeguards (Principle 4.7)

Personal information must be protected in a manner commensurate with its sensitivity. The sensitivity of information may vary according to context. Security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification (see "RFID security risks"). Personal information that is no longer required for the identified purposes must be disposed of in a secure manner.

5.8. Openness (Principle 4.8)

It is essential for organizations that make use of RFID systems to devote adequate time and resources to educating employees about how the technology functions, where the RFID tags and readers are located, what information will be collected and how that information will be used. Employees must be told about the presence of all RFID tags on items in their environment (such as products and packaging, tools and other assets) and the presence of all readers.

They should also be given a demonstration of how the information is gathered in the workplace. For example, employees should know that RFID tags broadcast information without the employee taking any action.

Employees must be told whether the RFID-related information will be linked with other personal information and whether the information will be made available to third parties.

There must be no hidden RFID tags or readers. Notice that an RFID tag is being read can be achieved by placing a sign close to the reader, or by having the reader emit a tone or flash a light when a reading takes place. In addition, a tag equipped with memory could count the number of times that it has been read.[84]

The location of all tags and readers is also important as it may be possible that RFID systems could interfere with active implantable medical devices. The International Commission on Non-Ionizing Radiation Protection looked at this question in 2002, but more research is needed to determine whether this is the case.[85]

5.9. Individual Access (Principle 4.9)

Employees are entitled to have access to their personal information that is collected by their employer. For employees to fully exercise this right of access, they must know the scope of the collection that is taking place. There must be no hidden RFID tags or readers – it is difficult if not impossible for an employee to request information relating to a tag of which she is unaware, or to inquire about data gathered by a reader that is hidden. Thus, all RFID readers must be identifiable so that employees can request access to the personal information that has been collected and question whether the data that has been gathered has been used for a purpose for which they have not granted consent.

For example, if an employee wanted to request all the data that is associated with her RFID-enabled employee card, she could:[86]

- request a printout, explained in plain language, of what is on her card;
- request all records of her entry and exit of building and site facilities, including parking, cafeteria access and billing, if it were on the same card;
- request all records of the sharing of her data with third parties, and
- request all records and technical documentation that would allow her to understand which readers in the wider population might be capable of reading all or parts of her card.

She might also want to request all the uses that had been made of information collected through this card, including any decisions that had been made about her. For example, if information collected through the RFID-enabled card was being used by the organization to inform judgments about the employee's productivity, she would have the opportunity to challenge the reasonableness of this purpose and the accuracy of the information collected.

5.10. Challenging Compliance (Principle 4.10)

The employee must be able to challenge the organization's compliance with the other principles by making inquiries or lodging a complaint. The organization must investigate all of the complaints it receives in a timely manner and must give a comprehensive response to the employee.

An individual can complain to our Office, or to the appropriate provincial commissioner, if, for example, he or she believes that an organization used RFID technology to collect personal information surreptitiously or was collecting information beyond what was required to meet the identified purposes. Other than employees of FWUBS, employees of private sector organizations within provinces that do not have private sector privacy legislation do not have these rights.

6. RFID in the Workplace – Conclusion

> "Our first task is to balance the rights and needs and convenience and security of society against the less convenient nature of human rights, which are always awkward, always difficult, but just simply fundamental."[87] John Godfrey, quoted in *Privacy Where Do We Draw the Line?* Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, 1997, at 15.

In the workplace, good privacy practice is not just about avoiding complaints, grievances, or lawsuits. Whether or not privacy is protected by law or contract, fostering a workplace culture where privacy is valued and respected contributes to morale and mutual trust, and makes good sense.[88]

The privacy issues raised by workplace surveillance are not new, yet technology continues to enhance the capacity of employers to monitor a very wide range of activity within the workplace. RFID technology is yet one more tool that can be used in workplace surveillance. Nevertheless, RFID poses particular concerns: the technology is new and thus poorly understood by many, its range of capacities and shortcomings are not fully known by those who use it, and it can be used ubiquitously and invisibly. These features mean that the introduction of RFID technology into the workplace requires careful attention in order to ensure that the privacy rights of employees are not trampled upon.

When employers are considering adopting new technologies in the workplace, a privacy impact assessment should be conducted. Further, privacy considerations should inform the choice of a particular system, or should influence the customization of a technology for the workplace. While new technologies may have the capacity to infringe on privacy, they may also be capable of being configured so as to address privacy concerns, or to limit privacy and security risks. This document

anticipates, to a large extent, the deployment of RFID in the workplace, and in this respect, one of its goals is to direct employers to take privacy law into account in choosing and implementing an RFID system.

Although the choice to adopt an RFID system largely rests with the employer, employees and the trade unions who may represent them also have a role to play in protecting their privacy. Where possible, employees should be involved in the choice and implementation of RFID systems in the workplace. This ability to play a role at the outset can enhance the autonomy and dignity of individual workers, and also contributes to ensuring consent to the contemplated uses of the technology. There is also much to be said for avoiding human identification where possible. RFID tagging of products and assets may provide benefits to the organization with relatively few privacy risks. But RFID tagging of employees through identity documents, uniforms, anklets and bracelets necessarily implicates privacy interests that might be avoided through other approaches.

The values of autonomy and dignity are also enhanced by an implementation of technology that is respectful of employees. Employers who seek to introduce new technologies such as RFID into the workplace should take the time to educate and inform their employees about the technology, the particular system implemented, how it functions, and what information it is being used to collect. In some circumstances, employers may rightly conclude that costs of some applications outweigh the benefits.

PART III – Consultation Questions

We welcome your feedback on anything in this document to enrich the debate on the use of RFID systems in the workplace. We welcome in particular the comments of those who are potentially directly affected by RFID in the workplace, namely employers, employees and trade unions as well as developers of RFID technology.

To encourage this debate to take place, we have set out several broad questions that we would like answered.

1. Where RFID systems are used in a workplace, human dignity needs to be considered and the 4-part reasonable person test should guide their use.
   - What should the parameters be?
   - What uses of RFID systems should be forbidden in the workplace?

2. RFID systems should be designed and customized to incorporate Fair Information Principles before they are deployed.
   - How can vendors be encouraged to complete and present their clients with a Privacy Impact Assessment (PIA) of an RFID system?
   - How can organizations that are contemplating an RFID solution independently verify claims of privacy compliance made by the vendor?
   - How can employers be encouraged to ask for a completed PIA in advance of deployment to ensure the RFID system has been configured to be compliant with privacy legislation?

3. RFID systems should be configured so that they collect the minimal amount necessary to accomplish the purpose.
   - How can employers be encouraged to configure RFID systems for anonymous monitoring where possible, so that information can be collected without having to know the unique ID of a given tag?
   - How can employers be encouraged to identify the presence of a certain item in a particular area without correlating it with information about that item's movement from one place to another?

4. There should be no hidden RFID tags or readers.
   - Given the industry trend to decrease the size of RFID tags (and the ability to conceal readers), what are some strategies to ensure that RFID systems are more transparent in the workplace?

5. Employers should consult employees (and unions) before the introduction of workplace surveillance systems or technologies with surveillance capabilities, such as RFID.
   - Do you believe any particular group or type of workers may be particularly disadvantaged as a result of surveillance by RFID systems?

6. Employees must be told whether RFID-related information will be linked with other personal information and whether the information will be made available to third parties.
   - What linkages should be forbidden?

- What personal information from elsewhere in the organization might it be reasonable to link to an RFID and under what circumstances?

7. Implanting employees with RFID tags against their will is unacceptable under any circumstances. Employment should never be made contingent on a willingness to be implanted with an RFID tag.
   - What other considerations need to be brought to bear on the discussion of RFID implants in the workplace?

8. What strategies would you recommend for the community of privacy commissioners to best deal with this issue in the years ahead?

9. What are the alternatives to RFID that might avoid some of the privacy risks described in this paper?

We will issue our recommendations for good practices, including a report on the comments we received, after the close of the comment period.

Comments on this RFID consultation paper may be sent by postal mail to the Office of the Privacy Commissioner of Canada by April 30, 2008:

RFID Consultation
Office of the Privacy Commissioner of Canada
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3

We would prefer to receive your comments by email at: consultation@privcom.gc.ca

For all general inquiries, please contact:

Toll-free: 1-800-282-1376
Phone: (613) 995-8210
Fax: (613) 947-6850
TTY: (613) 992-9190

Appendix I – RFID Technology

Tags can generally be divided into three main categories: passive, semi-passive and active. The categorization depends upon the presence or absence of a battery, and has an impact on the range from which a tag can be read. Passive tags have the simplest design and have no power source or on-tag transmitter. They rely upon the signal transmitted by the reader for activation. The absence of the battery means that they can be much smaller and cheaper than active tags. A passive tag can be read at a distance of 5 metres or less.

Semi-passive tags have a battery, but, lacking an integrated transmitter, they must still rely upon the reader for their ability to communicate. They can nevertheless be read at a much greater range than a passive tag – up to a maximum of 100 metres.[89]

Active RFID tags have a battery and an active transmitter. Active tags tend to be larger than passive tags and can be read from much greater distances. Their range is also greater than semi-passive tags, as they contain their own transmitter.[90]

Tags can be either read-only or read-write tags. These terms refer to whether or not the information stored on the tag can be changed or erased. A read-only tag is a form of RFID tag that will accept only a single numerical identifier, while a read-write tag will allow the stored data to be altered.[91] More complex RFID tags can contain read-write memory that can be programmed by a reader and they may also contain biometric information or even sensors to detect changes in moisture or pressure around the tag.

RFID tags can be designed to communicate with any reader (such tags are referred to as "promiscuous"). Alternatively, they may be designed to communicate only with a reader that provides an authentication credential before the tags respond (such tags are called "secure.")

An RFID reader, or interrogator, is a device to communicate with the RFID tag. It broadcasts a radio signal, which is received by the tag. The tag then transmits its information back to the reader. Readers can either be portable handheld terminals or fixed devices that can be positioned in strategic places such as in loading bays in shipping and receiving facilities, under carpets, or in doorways.

For further information on RFID technology see the resources listed in Appendix II.

Appendix II – Selected sources on RFID

Katherine Albrecht and Liz Mcintyre. *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*. Nashville: Nelson Current, 2005. http://www.spychips.com/

Edward Balkovich, et al., "9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace." RAND Corporation, 2005. http://www.rand.org/pubs/technical_reports/TR197/.

Ann Cavoukian, Information and Privacy Commissioner of Ontario. "Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology," February 2004. http://www.ipc.on.ca/images/Resources/up-rfid.pdf.

Ann Cavoukian, Information and Privacy Commissioner of Ontario. "Privacy Guidelines for RFID Information Systems", June 2006. http://www.ipc.on.ca/images/Resources/up-1rfidgdlines.pdf.

Center for Democracy and Technology, "CDT Working Group on RFID: Best Practices for Deployment of RFID Technology", May 1, 2006. Online: CDT: http://www.cdt.org/privacy/20060501rfid-best-practices.php.

Dutch Data Protection Authority, RFID: Promising or Irresponsible? Contribution to the social debate about RFID. The Hague, October 2006. Online: http://www.dutchdpa.nl/documenten/en_rap_2006_rfid.shtml?refer=true

Electronic Frontier Foundation, "Radio Frequency Identification (RFID)". Online: EFF: http://www.eff.org/Privacy/RFID/.

Electronic Privacy Information Center, "Radio Frequency Identification (RFID) Systems". Online: EPIC: http://www.epic.org/privacy/rfid/.

European Commission, Information Society, "Towards an RFID Policy for Europe". Online: Europa: http://ec.europa.eu/information_society/policy/rfid/index_en.htm.

European Parliament, Scientific Technology Options Assessment, *RFID and Identity Management in Everyday Life*, IPOL/A/STOA/2006-22. Online: http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf.

Federal Trade Commission, RFID Radio Frequency Identification: Applications and Implications for Consumers, March 2005. Online: FTC: http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf.

Christian Floerkemeier, et al., "Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols," Institute for Pervasive Computing, Switzerland, 2004. Online: http://www.vs.inf.ethz.ch/res/papers/floerkem2004-rfidprivacy.pdf (also available in Hitomi Murakami, Hideyuki Nakashima, Hideyuki Tokuda, Michiaki Yasumura (Eds.): Ubiquitous Computing Systems : Second International Symposium, UCS, Tokyo, Japan, November 8-9, 2004, Revised Selected Papers. Berlin: Springer-Verlag, 2005, at 214-231.

Simson Garfinkel and Beth Rosenberg, eds. *RFID: Applications, Security, and Privacy*. New Jersey: Pearson Education, 2005.

International Conference of Data Protection & Privacy Commissioners, "Resolution on Radio Frequency Identification", 20 November, 2003. Online: http://www.privacyconference2003.org/resolutions/res5.DOC.

International Telecommunications Union, *The Internet of Things*. November 2005. Online: International Telecommunications Union: http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf.

Ari Juels, "RFID Security and Privacy: A Research Survey." RSA Laboratories, 28 September 2005. Online: RSA: http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf#search=%22rfid%20contactless%20card%20distinctions%22.

Gaétan Laberge, Commission d'accès à l'information du Québec, "Radiofrequency identification technology (RFID): is there reason to mistrust it?" May 2006. Online: Commission d'accès à l'information du Québec: http://www.cai.gouv.qc.ca/06_documentation/01_pdf/RFID_en.pdf.

Office of the Privacy Commissioner of Canada, "Fact Sheet: RFID Technology". Online: OPC: http://www.privcom.gc.ca/fs-fi/02_05_d_28_e.asp.

Organisation for Economic Co-operation and Development, "Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations", 27 February, 2006, at 7. Online: OECD: http://www.oecd.org/dataoecd/57/43/36323191.pdf.

Teresa Scassa, Dr. Theodore Chiasson, Professor Michael Deturbide and Anne Uteck, "An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies" (April 2005) Online: Dalhousie University: http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf.

Appendix III – Scope of Application of *PIPEDA and Privacy Act*

***Personal Information Protection and Electronic Documents Act* (*PIPEDA*), S.C. 2000, c.-5.**

PIPEDA applies to the personal information of employees who are employed in "federal work, undertaking or business".

"Federal work, undertaking or business" means any work, undertaking or business that is within the legislative authority of Parliament. It includes

(a) a work, undertaking or business that is operated or carried on for or in connection with navigation and shipping, whether inland or maritime, including the operation of ships and transportation by ship anywhere in Canada;

(b) a railway, canal, telegraph or other work or undertaking that connects a province with another province, or that extends beyond the limits of a province;

(c) a line of ships that connects a province with another province, or that extends beyond the limits of a province;

(d) a ferry between a province and another province or between a province and a country other than Canada;

(e) aerodromes, aircraft or a line of air transportation;

(f) a radio broadcasting station;

(g) a bank;

(h) a work that, although wholly situated within a province, is before or after its execution declared by Parliament to be for the general advantage of Canada or for the advantage of two or more provinces;

(i) a work, undertaking or business outside the exclusive legislative authority of the legislatures of the provinces; and

(j) a work, undertaking or business to which federal laws, within the meaning of section 2 of the *Oceans Act*, apply under section 20 of that Act and any regulations made under paragraph 26(1)(k) of that Act."

***Privacy Act*, R.S.C. 1985, c. P-21.**

The *Privacy Act* applies to government institutions. These are defined in the Act as:

"(*a*) any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule, and

(*b*) any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the *Financial Administration Act*"

Endnotes

[1] S.C. 2000, c. 5. Online: Department of Justice Canada: http://laws.justice.gc.ca/en/P-8.6/258031.html.

[2] R.S.C. 1985, c. P-21. Online: Department of Justice Canada: http://laws.justice.gc.ca/en/P-21/255104.html#rid-255111.

[3] S.C. 2000, c. 5. Online: Department of Justice Canada: http://laws.justice.gc.ca/en/P-8.6/258031.html.

[4] R.S.C. 1985, c. P-21. Online: Department of Justice Canada: http://laws.justice.gc.ca/en/P-21/255104.html#rid-255111.

[5] Privacy Commissioner of Canada, *Annual Report to Parliament 2005, Report on the Personal Information Protection and Electronic Documents Act*. Online: Office of the Privacy Commissioner: http://www.privcom.gc.ca/information/ar/200506/2005_pipeda_e.asp#020.

[6] Professor Valerie Steeves, Presentation to The Standing Senate Committee on Social Affairs, Science and Technology on Bill S-21, to guarantee the human right to privacy, September 20, 2001. Online: Government of Canada: http://www.parl.gc.ca/37/1/parlbus/commbus/senate/Com-e/soci-e/25ev-e.htm?Language=E&Parl=37&Ses=1&comm_id=47.

[7] M. Weiser. "The Computer for the 21st Century", *Scientific American*, Vol. 265, No. 3 (1991), pp. 94–104.

[8] Ari Juels. "RFID Security and Privacy: A Research Survey." RSA Laboratories, 28 September 2005, p. 3. Online: RSA: http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf.

[9] *Ibid*., p. 2.

[10] According to the Smart Card Alliance: "A contactless smart chip-based device includes an embedded secure microcontroller or equivalent intelligence, internal memory, and a small antenna, and communicates with a reader through a contactless radio frequency (RF) interface. The contactless interface provides users with the convenience of allowing the contactless device to be read at short distances with fast transfer of data. Contactless smart chip technology is available in a variety of forms – plastic cards, watches, key fobs, documents, and other handheld devices such as mobile phones." From: Smart Card Alliance, "Contactless Chip Technology: The Business Benefits". Online: Smart Card Alliance: http://www.smartcardalliance.org/alliance_activities/contactless_business_benefits.cfm.

[11] Smart Card Alliance, "RFID Tags and Contactless Smart Card Technology: Comparing and Contrasting Applications and Capabilities," Online: HID Global: http://www.hidcorp.com/documents/tagsVsSmartcards_wp_en.pdf

[12] Juels, *supra* note 8, p. 16.

[13] "Firewall Protection for Paper Documents," *RFID Journal*, February 11, 2004. Online: *RFID Journal*: http://www.rfidjournal.com/article/articleview/790/1/1.

[14] Address by Jennifer Stoddart, Privacy Commissioner of Canada, "Finding the right workplace privacy balance," The Ryerson University Workshop on Workplace Privacy, November 30, 2006. Online: http://www.privcom.gc.ca/speech/2006/sp-d_061130_e.asp.

[15] Office of the Privacy Commissioner of Canada, *Fact Sheet: Workplace Privacy*. Online: OPC: http://www.privcom.gc.ca/fs-fi/02_05_d_17_e.asp.

[16] Teresa Scassa et al., *An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies*, April 2005, p. 48. Online: Dalhousie University: http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf.

[17] Edward Balkovich et al., *9 to 5: Do You Know If Your Boss Knows Where You Are? Case Studies of Radio Frequency Identification Usage in the Workplace*. RAND Corporation, 2005, p. 14. Online: Rand Corp.: http://www.rand.org/pubs/technical_reports/TR197/.

[18] *Ibid*., pp. 13–14.

[19] IBM, *IBM RFID Solution for Asset Tracking – location awareness and safety*. Online: IBM: http://www-03.ibm.com/industries/chemicalspetroleum/doc/content/solution/1518038320.html.

[20] "Silent Commerce has Arrived," *RFID Journal* Online: RFID Journal: http://www.rfidjournal.com/magazine/article/767/1/95/. The Sydney Casino project is highlighted by Accenture, the company which implemented it, in its promotional brochure. Online: Accenture: http://www.accenture.com/NR/rdonlyres/39F0E23D-7ABF-46EB-90C0-63FDB59FDA7A/0/Star_City_Casino_Final.pdf.

[21] This story was reported by several sources including Michael Milllar, "Union calls for halt to RFID tracking of workers," July 18, 2005. Online: PersonnelToday.com: http://www.personneltoday.com/articles/2005/07/18/30851/union-calls-for-halt-to-rfid-tracking-of-workers.html and on the GMB union site Online: http://www.gmb.org.uk/Templates/Internal.asp?NodeID=92057.

[22] Stephanie Perrin, "RFID and Global Privacy Policy," in Garfinkel, Simson and Rosenberg, eds., *RFID: Applications, Security, and Privacy*. New Jersey: Pearson Education, 2005, at 64. Also available online: ID Trail Project: http://idtrail.org/files/Perrin%20-%20RFID%20and%20Global%20Privacy%20Policy.pdf.

[23] IBM, *IBM RFID Solution for Asset Tracking – location awareness and safety*. Online: IBM: http://www-03.ibm.com/industries/chemicalspetroleum/doc/content/solution/1518038120.html.

[24] "Montreal to use GPS to keep tabs on workers", *Toronto Star*, April 26, 2006 pp. A1, A8.

[25] K.C. Jones, "VeriChip wants to test human implantable RFID on military," *TechWeb,* August 23, 2006. Online: TechWeb: http://www.techweb.com/wire/ebiz/192203522.

[26] Hitachi, Mu Solutions. Online: Hitachi : http://www.hitachi-eu.com/mu/Products/Mu%20Chip.htm.

[27] CBC News, "Hitachi develops powder-sized RFID chips," February 23, 2007. Online: http://www.cbc.ca/technology/story/2007/02/23/tech-rfid.html.

[28] "Kodak's RFID Moment," *RFID Journal*. Online: http://www.rfidjournal.com/article/articleview/3100/.

[29] Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, January 19, 2005, 10107/05/EN, pp. 6–7. Online: Europa: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

[30] Lisa Madelon Campbell, "Nanotechnology and the United States National Plan for Research and Development In Support of Critical Infrastructure Protection", *Canadian Journal of Law and Technology*, Vol. 5, No. 3, November 2006, Online: http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_workbook2_E.html#section003.

[31] "Finnair, IBM and Nokia Improve Passenger Service at Helsinki Airport: Radio Frequency Identification Technology Streamlines Airport Ground Handling," IBM Press Release, June 12, 2006. Online: IBM: http://www-03.ibm.com/press/us/en/pressrelease/19805.wss.

[32] Bob Barr, "The Real Toll is Your Privacy", *The Atlanta Journal Constitution*, August 15, 2007. Online: Bob Barr: http://www.bobbarr.org/default_print.asp?pt=newsdescr&RI=873.

[33] Adapted from DN-Systems *RFID: Security Concerns*. Online: DN-Systems: http://www.dn-systems.de/technology/RFID/.

[34] Annalee Newitz, "The RFID Hacking Underground", *Wired*, Vol. 14, No. 05, May 2006. Online: Wired: http://www.wired.com/wired/archive/14.05/rfid.html.

[35] Melanie R. Rieback, Bruno Crispo and Andrew S. Tanenbaum, *Is Your Cat Infected With a Computer Virus?*, Computer Systems Group, Vrije Universiteit Amsterdam, 2006. Online: Vrije Universiteit: http://www.rfidvirus.org/papers/percom.06.pdf. See also: Will Knight, "RFID Worm Created in the

Lab," *New Scientist*, March 15, 2006. Online: New Scientist: http://www.newscientisttech.com/channel/tech/dn8854.html.

[36] *Privacy Act*, s. 2 and Schedule. See Appendix III to this document.

[37] Treasury Board of Canada Secretariat, *Strategic Direction for Government: Information Management*. Online: Treasury Board of Canada Secretariat: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/im-gi/sdg-osg1_e.asp.

[38] Treasury Board of Canada Secretariat, *Government Security Policy*. Online: Treasury Board: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp.

[39] Treasury Board of Canada Secretariat, *Employee Privacy Code*. Online: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP3_3-2_e.asp.

[40] Treasury Board of Canada Secretariat, Privacy Impact Assessment Policy and Guidelines. Online: Treasury Board of Canada Secretariat: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp.

[41] S.O. 2004, c. 3.

[42] This term is defined in *PIPEDA*. The definition is reproduced in Appendix III.

[43] *Ibid*. s.2,

[44] For example, in *Dagg v. Canada (Minister of Finance),* Justice La Forest stated: "As noted by Jerome A.C.J. in *Canada (Information Commissioner) v. Canada (Solicitor General)*, supra, at p. 557, the language of this section is 'deliberately broad' and 'entirely consistent with the great pains that have been taken to safeguard individual identity'. Its intent *seems to be to capture <u>any</u> information about a specific person, subject only to specific exceptions [citation omitted]. Such an interpretation accords with the plain language of the statute, its legislative history and the privileged, foundational position of privacy interests in our social and legal culture*." *Privacy Act*, s.3.

[45] *Dagg v. Canada*, [1997] 2 S.C.R. 403. Online: LEXUM: http://scc.lexum.umontreal.ca/en/1997/1997rcs2-403/1997rcs2-403.html.

[46] *PIPEDA* Case Summary #319, "ISP's anti-spam measures questioned", February 13, 2006. Online: OPC: http://www.privcom.gc.ca/cf-dc/2005/319_20051103_e.asp.

[47] *PIPEDA* Case Summary #270, "Bank agrees to modify automated message", June 21, 2004. Online: OPC: http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040504_e.asp.

[48] Investigation Report P2005-IR-04, R.J. Hoffman Holdings Ltd., May 13, 2005. Online: Alberta Information and Privacy Commissioner: http://www.oipc.ab.ca/ims/client/upload/P2005_IR_004May13.pdf.

[49] Investigation Report P2005-IR-009, Precision Drilling Corporation, November 4, 2005. Online: Alberta Information and Privacy Commissioner: http://www.oipc.ab.ca/ims/client/upload/Investigation%20Report%20P2005-IR-009.pdf.

[50] "Mexican university selects AXCESS asset management RFID solution," *More RFID*, May 10, 2006. Online: *More RFID*: http://www.morerfid.com/details.php?subdetail=Report&action=details&report_id=2192&display=RFID.

[51] *PIPEDA* Case Summary #220, "Telemarketer objects to her employer sharing her sales results with other employees", January 19, 2004. Online: OPC: http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030915_e.asp.

[52] Scassa et al.

[53] Submission Presented to the Standing Committee on Access to Information, Privacy and Ethics, February 22, 2007. Online: OPC: http://www.privcom.gc.ca/parl/2007/sub_070222_e.asp.

[54] *Dagg v. Canada*, [1997] 2 S.C.R. 403. Online: LEXUM: http://scc.lexum.umontreal.ca/en/1997/1997rcs2-403/1997rcs2-403.html.

[55] *Personal Information Protection Act*, [SBC 2003] Chapter 63, s. 1.

[56] See, for example: *Re Puretex Knitting Co. Ltd. and Canadian Textile and Chemical Union* (1979), 23 L.A.C. (2d) 14; *Ross v. Rosedale Transport Ltd.,* [2003] C.L.A.D. No. 237; Re Canadian Pacific Ltd. and Brotherhood of Maintenance of Way Employees (1996), 59 L.A.C. (4th) 111.

[57] OPC, *supra* note 15.

[58] *Ibid*.

[59] See, for example: *Re Puretex Knitting Co. Ltd. and Canadian Textile and Chemical Union* (1979), 23 L.A.C. (2d) 14; *Ross v. Rosedale Transport Ltd.,* [2003] C.L.A.D. No. 237; Re Canadian Pacific Ltd. and Brotherhood of Maintenance of Way Employees (1996), 59 L.A.C. (4th) 111.

[60] (2004), 16 Admin. L.R. (4th) 275 • (2004), 33 C.P.R. (4th) 1, at para 127.

[61] *PIPEDA* Case Summary #279, "Surveillance of employees at work", September 27, 2004. Online: OPC: http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040726_e.asp.

[62] *PIPEDA* Case Summary #281, "Organization uses biometrics for authentication purposes", October 26, 2004. Online: OPC: http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp.

[63] *Turner v. Telus Communications Inc*., [2005] F.C. 1601.

[64] *Wansink v. Telus Communications Inc.,* [2007] FCA 21.

[65] Todd Lewan, "Microchip implants park privacy worry; security measures may lead to tracking", AP via Chicago Tribune, July 30, 2007. .

[66] Privacy Impact Assessment Policy and Guidelines, *supra* note 40.

[67] Schedule 1, *PIPEDA*.

[68] *PIPEDA*, Schedule 1, Principle 4.1.

[69] Office of the Privacy Commissioner of Canada, PIA Resources. Online: http://www.privcom.gc.ca/pia-efvp/index_e.asp.

[70] Christian Floerkemeier, et al., *Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols*, Institute for Pervasive Computing, Switzerland, 2004, p. 4. Online: http://www.vs.inf.ethz.ch/res/papers/floerkem2004-rfidprivacy.pdf (also available in Hitomi Murakami, Hideyuki Nakashima, Hideyuki Tokuda, Michiaki Yasumura [eds.], *Ubiquitous Computing Systems : Second International Symposium*, UCS, Tokyo, Japan, November 8-9, 2004, Revised Selected Papers. Berlin: Springer-Verlag, 2005, pp. 214–231).

[71] *Ibid*.

[72] *Ibid*.

[73] *PIPEDA* Case Summary # 273, "After installing surveillance cameras in the workplace, a broadcasting company has agreed to inform its employees about the purpose and to adopt a policy regarding its use," June 21, 2004. Online: OPC: http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040518_e.asp.

[74] 2004 FCA 387. Online: Federal Court of Appeal: http://decisions.fca-caf.gc.ca/en/2004/2004fca387/2004fca387.html.

[75] Presentation by Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada, to the Canadian Life and Health Insurance Association 2006 Joint Annual Conference of the Compliance Section and Consumer Complaints Officers Section, May 11, 2006. Online: OPC: http://www.privcom.gc.ca/speech/2006/sp-d_060511_pk_e.asp.

[76] *PIPEDA*, s. 7(1)(*b*).

[77] *Eastmond v. Canadian Pacific Railway,* 2004 FC 852, at para 187. Online: Federal Court of Canada: http://decisions.fct-cf.gc.ca/en/2004/2004fc852/2004fc852.html. It is worth noting, however, that the particular design of the system, with certain safeguards and limitations, played a role in the Court's decision.

[78] Floerkemeier et al., p. 7.

[79] *Ibid*.

[80] *Ibid*. p. 5.

[81] *Ibid*.
[82] *Ibid*.
[83] Perrin, *supra* note 21, p. 76.
[84] Simson Garfinkel, "Adapting Fair Information Practices to Low-Cost RFID System," in Simson Garfinkel and Beth Rosenberg (eds.), *RFID: Applications, Security, and Privacy*, New Jersey: Pearson Education, 2005, p. 522.
[85] *Possible Health Risks to the General Public from the Use of Security and Similar Devices,* International Commission on Non-Ionizing Radiation Protection, 2002. Online: ICNIRP: http://www.icnirp.de/documents/ExSummary.pdf.
[86] Adapted from Perrin, *supra* note 21, p. 79.
[87] John Godfrey, quoted in *Privacy: Where Do We Draw the Line?* Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, 1997, p. 15. Online: OPC: http://www.privcom.gc.ca/information/02_06_03d_e.pdf.
[88] Fact Sheet, *supra* note 15.
[89] Teresa Scassa et al., "Consumer Privacy and Radio Frequency Identification Technology" *Ottawa Law Review*, Vol. 37, 2005-2006, p. 218.
[90] Simson Garfinkel and Henry Holtzman, "Understanding RFID Technology," in Simson Garfinkel and Beth Rosenberg (eds.), *RFID: Applications, Security, and Privacy*, New Jersey: Pearson Education, 2005, p. 17.
[91] *Ibid*., p. 18.