Radio Frequency Identification and the Need to Protect Personal Information

by Mavis Taillieu, MLA

Radio frequency identification (RFID) is an emerging use of technology that could permit unprecedented collection of personal information. This, in turn, linked with other information data bases, many without the knowledge or consent of affected individuals are problematic for those who feel there is a need to protect personal information and privacy. In this brave new world, technology is advancing at light speed while our understanding of what it can do is moving at the speed of a tortoise. This article argues that it is time for legislators to take a serious look at RFID technology and its implications for Canadian society.

In 2004, the Ontario Privacy Commissioner, Anne Cavoukian, issued a report outlining the dangers to our privacy from Radio Frequency Identification (RFID) – a highly specific identification method relying on data storing devices called chips or tags, and remote retrieving devices called transceivers or readers. The tag is a small object ranging from a couple of centimeters square to the size of a grain of pepper that can be attached to, or incorporated into a product, animal or person. RFID tags contain silicone chips and antennae to enable them to receive and respond to radio frequency queries from an RFID transceiver or reader. In June 2006, the commissioner issued guidelines for companies employing this technology which focused on three overarching principles. There should be focus on RFID information systems rather than just the technology, there should be built-in privacy and security from the outset, and a maximization of individual participation and consent.

It is not the RFID technology that has raised privacy concerns but the associated possibilities. RFID tags are unique and specific and therefore highly identifiable with the product, animal or person. They have been referred to as "barcodes on steroids" because unlike barcodes that identify (for example) all cans of Cola as Cola, these tags identify every single can of Cola in the world as unique and different. Unlike bar codes that are read with light beams RFID uses radio waves which can read RFID tags through purses, pockets and even vehicles. This technology is presently used in supply management to track movement of goods worldwide and for inventory control. At this level it poses little threat but item level use of RFID tags in the retail sector, when linked to personally identifiable information, could facilitate the tracking and surveillance of individuals. If each item purchased could be linked with other information like credit card information or cell phone information which in turn could be linked to banking information that could result in complete profiles about shopping habits, personal preferences, personal movement and personal spending habits.

RFID is currently used in several applications around the world. It is used in library book and bookstore tracking, building access control, airline baggage tracking, ap-

Mavis Taillieu is the Member for Morris at the Legislative Assembly of Manitoba. This is a revised version of a paper presented at the 44th Canadian Regional Conference of the Commonwealth Parliamentary Association held in Gatineau in July 2006.

parel and pharmaceutical tracking, and employee badges. Cattle are tagged with RFID. A number of countries have begun using it in passports. At present Canadian passports do not contain RFID. Inmates in correction institutes in several States in America wear RFID embedded wrist bands to track their whereabouts. The toll booths on the 407 north of Toronto use RFID to automatically bill people's accounts as they pass through and their RFID embedded cards are read by the remote reader. Nexus cards proposed for secure trans-border crossing between Canada and the USA contain RFID chips. RFID technology is being studied at the University of Manitoba.

In October of 2004 the Food and Drug Administration in the USA approved the first RFID chips that can be implanted in humans. These chips from VeriChip Corporation, a subsidiary of Applied Digital Solutions Incorporated can hold personal health information, personal credit card and banking information, special codes or passwords, or indeed any information about the individual. A beach club in Spain has patrons implant a chip in their hand which contains there credit card numbers so they don't have to carry money. As of February of this year a surveillance company in Cincinnati became the first American company to use VeriChip implanted in employees for access to its data centre. Canada's Therapeutic Directorate has not yet approved the implantable RFID technology for use in Canada but VeriChip has opened offices in Vancouver and Ottawa. Dr. Ian Kerr, Canada Research Chair in Ethics, Law and Technology, University of Ottawa, Faculty of Law has said these chips are easy to clone and has asked the question of whether to regulate these in Canada and just who should be in charge of that regulation.

The Privacy Commissioner for Canada, Jennifer Stoddard undertook a study of RFID use in Canada in 2005 and concluded that "greater public and political awareness of the potentially intrusive nature of RFID is essential now". She concluded that RFID use in Canada has already expanded beyond simply tracking materials but is being linked to personal information and sometimes used to track people.

We live in an age of excessive collection and sharing of personal information. The past few decades have witnessed a dramatic transformation in the way we shop, bank and go about our daily business – changes that have resulted in an unprecedented proliferation of records and data. "Small details that were once captured in dim memories or fading scraps of paper are now preserved forever in the digital minds of computers, in vast data bases with fertile fields of personal data" said author Daniel Solove.

There are three main data collectors; governments, non-profit organizations and commercial entities. The collection, trade, rent and sale of personal information is big business. The Canadian Marketing Association estimates there are 480,000 jobs generating $51 billion in sales annually, involving the collection of consumer information, analyzing of customer data bases and brokering of personal information.

> ***Creation of mega data bases of personal information are the new banks and personal information is the new currency.***

Individuals give up their personal information wittingly or unwittingly as purchasers, subscribers, registrants, members, card holders, donors, contest entrants, survey respondents and even to mere enquirers.

The increasing accumulation of personal data and consolidation of data bases leaves individuals vulnerable to abuses by those with access to the data. Potential uses of this data are limited only by law and ethics.

In Canada, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) governs the collection, use and disclosure of personal data by organizations in the course of commercial activities. However, there is not great compliance with the law. Philippa Lawson, executive director and general council of the Canadian Internet Policy and Public Interest Clinic released a study that found that retailers, on-line in particular, were not compliant with PIPEDA. "Our study shows quite clearly there is a very high level of non-compliance out there when it comes to the kinds of things that consumers aren't aware of. That is the sharing and use of their personal data behind the scenes. Companies are not being as forthright about that and are not giving consumers meaningful choice."

Furthermore, we should not be lulled into believing security is infallible. Between February 15, 2005 and June 30, 2006 there were 222 breaches of security involving more than 88 million records containing sensitive personal information in the USA. The majority of these were due to hackers, stolen laptops or dishonest inside employees. Over 10 million people in the United States last year fell victim to identity theft. Two major Canadian credit bureaus Equifax and Trans Union indicate they receive 1400-1800 identity theft complaints per month - the majority from Ontario. Equifax itself has had data breaches were information was stolen.

Mary Kirwan, lawyer, writer and IT security expert said "it's no joke to stay one step ahead of the virtual bad

guys. Keyloggers are devices used by parents to monitor children's Internet surfing habits and by employers to monitor employees on-line. In the wrong hands Keyloggers are the ultimate spyware tool, enabling criminals to take screen shots, and record keystrokes to capture sensitive data such as banking passwords and PIN numbers...". There are potentially massive amounts of personal information to be stolen but the public is largely unaware of the lack of on-line security."

Lack of compliance and lack of security enhances the prospect of identity theft – the fastest growing crime in Canada today

Identity theft in broad terms refers to all types of crime in which someone wrongfully obtains and uses another person's identifying information for the purposes of fraud or other criminal activity, typically for economic gain. Such data can include name, date of birth, mother's maiden name, social insurance numbers, personal health numbers, birth certificates, passports, driver's license and credit card numbers. Once stolen this information can be used to create financial accounts, transfer bank balances, apply for loans or credit, purchase goods and services or in fact steal your identity.

Information is stolen from a variety of sources – the mail, family members or relatives, from your residence or garbage. But it has become much more sophisticated. It is now obtained from data miners, hackers, from computers or laptops in the workplace with access to huge data bases. New uses of technology like RFID could potentially increase collection of data, misuse of data and increase the risk of having identity theft occur, occur more often and occur more easily.

Legislators should be proactive in discussion, education and possible legislation regarding protection of personal information in light of advancing technologies of which the public is generally unaware. If people give informed consent to share their personal information based on the recognition it will be used for the purposes identified, that it will not be shared and will be safeguarded there is more chance there will be acceptance. Privacy assessments should be a part of all emerging technologies and public participation and consent are necessary.

Jennifer Stoddard, Privacy Commissioner for Canada, in her 2005 Annual Report to Parliament in May had this to say: "I would like to report much good news about privacy in Canada. But it's not all good news. Concern among Canadians about their loss of privacy and the misuse of their personal information has never been greater. The concern stems from the growing threats to personal information in an electronic environment of massive and continuous data circulation."

In a research poll undertaken by the Privacy Commissioner Canadians identified privacy as among the most important issues facing the country. Canadians support strong and responsive public and private sector privacy laws. Seventy percent (70%)expressed a strong sense that their privacy and protection of their personal information was being eroded. A substantial majority of those surveyed said there was no real privacy because technology has made it too easy for governments to keep track of people.

Following the rash of security breaches and losses of personal information in the United States 23 States have enacted "duty to notify" legislation where the company who collected personal information must notify individuals about any potential compromise of that information. Up until only two years ago California was the only State with such a law. There are 12 states where there is some form of legislation regarding the use of RFID technology. They range from creating a task force to study RFIDs in Maryland to prohibiting government from requiring people to have a RFID chip embedded in them in Wisconsin, South Dakota and New Hampshire.

In Canada, and according to the Privacy Commissioner, PIPEDA applies to RFID use and data linking. This legislation is under review and one of the things being recommended is stronger enforcement of the law.

British Columbia, Alberta, Quebec and Ontario (for health information only) have enacted substantially similar legislation to PIPEDA and therefore are governed by their provincial laws. Brian Bowman, a renowned privacy lawyer from Winnipeg believes that provincial legislation would precipitate better compliance with the laws because businesses would recognize and identify with local legislation.

> ***To my knowledge there are no acts of legislation specific to RFIDs in Canada.***

I have proposed a Private Members Bill entitled The *Protection of Personal Information and Identity Theft Prevention Act* which is intended to enact substantially similar legislation in Manitoba. There is a "duty to notify" clause which I believe is the first broadly-based obligation of its kind in Canada. This Bill was rejected by the current NDP government as almost all private member's Bills are. I do believe that "duty to notify" clauses will appear in future legislation regarding the protection of personal information and may be considered in the current review of PIPEDA.

Your personal information defines you. It's not just name, address, phone number, e-mail address, social insurance number, bank account numbers, PINs, date of birth, driver's license, but declaration of ethnicity, religion, sexual orientation, political affiliation and personal associations and personal preferences, and to where you travel. It also includes biometrics like photographs, finger and palm prints, facial and iris scans, and DNA.

Individuals need to protect their personal information, and need to know why they should, before it is given away for the sake of convenience and security. When we give up all our personal information we become vulnerable to advancing technologies and those who know how to misuse them. When we give up our personal information we give up all our right to privacy.

Canadians view privacy rights in several ways: the right to be left alone, the right to control what others know about us, the right to expect that information about us should be gathered only when it serves a specific purpose, and should be used only for that purpose and it is a social value that is shared by the rest of the community.

Privacy is something we may not think about until we don't have it. And once we don't have it we will never get it back.

Sources

Annual Report to Parliament 2005 on the Personal Information Protection and Electronic Documents Act, RFID Technology, www.privcom.gc.ca/information/ar/200506/2005_pipeda_e.asp

RPP 2005-06\Offices of the Information and privacy Commissioners, www.tbs-sct.gc.ca/est-pre/20052006/IPC-CIP/IPC-CIPr5602_e.asp

Industry Canada – RFID Beyond Customer mandate, www.strategis.ic.gc.ca

Compliance with Canadian data Protection Laws, Are retailers measuring up? – April 2006, On the Data Trail: How detailed information about you gets into the hands of organizations with whom you have no relationship – April 2006, Canadian Internet Policy and Public Interest Clinic, Faculty of Law/University of Ontario

Tag, You're it: Privacy Implications of Radio frequency Identification (RFID) Technology, RFIDs: Homing in on Privacy Information and Privacy Commissioner Ontario, Commissioner Cavoukian Issues RFID Guidelines aimed at protecting privacy, Guidelines for using RFID tags in Ontario Public Libraries www.ipc.on.ca

RFID Journal: RFID vendors need a privacy strategy, www.rfidjournal.com/article/articleview/2428/1/128/, and other related articles

RFID: The Big Brother Bar Code, www.spychips.com/alec-big-brother-barcode-article.html

RFID Nineteen Eight-Four, www.spychips.com/press-releases/us-employees-verichipped.html, and other related articles

Radio Frequency Identification, http://en.wikipedia.org/wiki/RFID

RFID Gazette Privacy, www.rfidgazette.org/privacy

VeriChip, http://en.wikipedia.org/wiki/VeriChip

EPC Global, www.epcglobalcanada.org

The horns of a security dilemma – Mary Kirwan, www.theglobeandmail.com/servlet/story/RTGAM.20050512.gtkirwanmay12/BNStory/Tech

Identity Theft, http://en.wikipedia.org/wiki/Identity_theft

Mapleleafweb – National Identity cards – the next step?, Mapleleafweb – What about the right to privacy? www.mapleleafweb.com/features/privacy/id_cards

Junkbusters – RFID and Privacy, www.junkbusters.com/rfid.html

The year of RFID legislation, www.cephas-libary.com/mwo/nwo_the_year_of_rfid_legislation.html

Health –care chips could get under your skin, www.expressnews.ualberta.ca/article.cfm?id=7633

Publica: Legal implications of using RFID highlighted, www.heydary.com/publications/rfid-laws.html

it business.ca: Federal Privacy Commissioner to tackle RFID, www.itbusiness.ca/it/client/en/ComputerCanada/News.asp?id=39586&cid=3

Bruce Schneier on RFID passports, www.schneier.com/blog/archives/2004/10/rfid_passports.html

Choicepoint, www.epic.org/privacy/choicepoint/

Privacy Rights Clearing House: A chronology of data breaches reported since the Choicepoint incident, www.privacyrights.org