Information
and Privacy
Commissioner/
Ontario

Tag, You're It:

Privacy Implications of Radio Frequency Identification (RFID) Technology

Ann Cavoukian, Ph.D.
Commissioner
February 2004

Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, gratefully acknowledges the work of Lawrence Surtees and Laura Boyd in preparing this report.

Information and Privacy
Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

This publication is also available on the IPC website.

Table of Contents

Introduction

Every day, in dozens of ways and places, each Ontarian leaves a tell-tale electronic trail of his or her daily activities through a stream of computer bits and images that is collected, analyzed, merged and even sold to others – often without our knowledge or consent.[1] Our lives are increasingly being opened to a greater level of scrutiny in minute detail, aided by the convergence of digital technologies and an ever-growing appetite by corporate marketers and government agencies to obtain yet more detailed information about each of us.

Video cameras can be found almost anywhere to record our movements in apartments, stores, office buildings and at public locations such as parking lots, street corners and at instant tellers. Security "wipe" card systems track our comings and goings at the office. Our telephone calls are logged, our phone number displayed to those we call, and e-mails are monitored by employers. Every transaction with a credit or bank debit card adds more information to the burgeoning computer files tracking our most intimate transactions. Surf the Internet and both government agencies and business marketers may monitor your visit to a Web site, resulting in an assembled profile and marketing data secretly sent to other – or your own – personal computer.[2] All that information is leading those who know how to collect and analyze it to follow you directly to your front door, telephone or computer screen.[3]

Anonymity has become a thing of the past. The day is close at hand when a permanent digital archive of our every move and activity could be created, such as the so-called "Lifelog" created by Microsoft Corp. researcher Gordon Bell.[4]

Now imagine if tiny and ubiquitous radio emitting tags that cost just pennies apiece were placed in every product or article we consume. In our jeans and sweaters. Inside all consumer good packages, including groceries and shaving foam. In the tires of our cars. In our pets and livestock. Even embedded in our currency. Unique tags that are able to communicate with scanning "reader" devices herald the prospect of information being compiled about individuals in unprecedented detail as well as give rise to the prospect of being tracked by our personal possessions.

Futuristic? Perhaps, but this brave new world is closer than we think, thanks to the emerging technology of Radio Frequency Identification – dubbed RFID.

U.S. retail giant Wal-Mart recently announced that it wants its top 100 suppliers, by 2005,[5] to begin fitting their cases and pallets with RFID tags – tiny microchips that can automatically transmit to a special scanner all of the information about a container's contents or about individual products. Wal-Mart's other 12,000 suppliers would be expected to follow suit by 2006. A number of those suppliers are tempted to do more than just affix chips to the goods they ship to Wal-Mart; they are also looking to implement RFID technology more broadly within their own organizations in hopes of cutting their own supply chain costs. Retailers and consumer products manufacturers, aware of

Wal-Mart's interest in RFID, have also begun eyeing it as the next supply chain technology to invest in.[6]

When Wal-Mart talks, suppliers listen, as when the retail giant declared in 1984 that it wanted to use bar codes as a better way to manage inventory: soon after, bar codes became *de rigeur*. If a supplier refused to use bar codes, it lost Wal-Mart's business – a death knell for most. The same thing is happening today with radio tags. Only radio frequency identification has been likened to bar codes on steroids.[7]

Through RFID, "In the near future, every single object will be connected to the Internet through a wireless address and unique identifier," said Dirk Heyman, global head of life science and consumer product industries at Sun Microsystems Inc.[8]

RFID technology has a number of privacy implications. This paper was produced:

- as an educational tool to help the public understand what an RFID is;
- to help focus attention on the privacy issues; and
- to advance the privacy principles that need to be considered by businesses during the design and use of this technology.

What is RFID?

RFID is a more recent term referring to a family of sensing technologies that has been in use for more than 50 years. The technology of radio identification was devised for military applications during the Second World War. Radio frequency transponders were first installed on Allied aircraft to identify whether they were friendly. Hence the name for that early technology, dubbed Identify Friend or Foe (IFF), which is an essential feature on every military and civilian aircraft in the world today.[9]

Following the war, new applications were developed for RFID to track military equipment and personnel. Two companies were spun off from the U.S. nuclear weapons laboratory at Los Alamos in the late 1970s to commercialize RFID tracking technology and, by the early 1980s, initial applications were used to identify cattle and to track railway cars.[10]

RFID is now a generic term for a variety of technologies that use radio waves to automatically identify individual items.

How RFID Systems Work

All RFID systems have two integral parts: a tag, and a reader. Readers capture the information stored or gathered by the tag. The tag is composed of three parts (shown in the picture below):

- An antenna;
- A wireless "transducer" which may also be linked to a single silicon microchip unit containing memory storage; and
- An encapsulating material.

Types of RFID Systems

Chipless versus Chip RFID

One broad classification of RFID tags is whether they contain a microchip. “Chip” tags contain an integrated circuit chip, whereas “chipless” tags do not. Chipless tags are less expensive to make and may store up to 24 bits of information – which provides enough memory for a company’s internal use, such as on a shop floor or within a warehouse. However, that is not enough for mass-market applications.

In order for a reader to identify all manufactured items, an RFID tag must have enough memory storage to hold a very large ID number designed to identify a massive number of objects. And the reader must be able to read multiple tags within its range and in close proximity. Chip tag RFID systems enable data, such as a serial number or product code, to be stored and transmitted by portable tags to readers that process the data according to the needs of a particular application.[11] Small chips currently able to store 96-bits of data – enough to include a manufacturer’s name, a product name and one of trillions of unique numbers that can be assigned to products.

At the heart of that technology are tiny computer chips smaller than a grain of sand to track items at a short distance. Hitachi, the Japanese semiconductor company, has unveiled a prototype for the next generation of its -Chip (pronounced mu-chip). The chip is only 0.3 millimeters square, roughly half the size of the smallest RFID chip on the market.[12] It can also hold 128-bits of data.

Hitachi currently sells its RFID chips (with an antenna embedded on the substrate) for 43 cents (US) each on orders of 70,000 or more.

Active and Passive RFID Tags

The working of RFID systems and their features depend on the type of tag system used. There are two main types of RFID tag: active or passive, which differ depending on whether they have their own power system.[13]

Active RFID tags, which have both an on-tag power source and an active transmitter, offer superior performance. Because they are connected to their own battery, they can be read at a much higher range – from several kilometers away. But they are larger and more expensive. Active RFID tags are suitable for manufacturing, such as tracking components on an assembly line, or for logistics – primarily where the tag device will be reused.

Passive tags have no power source and no on-tag transmitter, which gives them a range of less than 10-metres and makes them sensitive to regulatory and environmental constraints. However, they have the most potential for lowest cost, making them suited for mass single-use applications.

Inductively Coupled RFID Tags

Passive RFID tags are powered by the magnetic field generated by the reader. The tag's antenna receives the electromagnetic energy generated by the reader then modulates that energy through its transducer to retrieve or transmit data back to the reader. The antenna in an inductive RFID tag is made from a metal coil of copper or aluminum wire.

Capacitively Coupled RFID Tags

Capacitively coupled tags eliminate the metal coil antenna by using conductive ink. These tags, such as the BiStatix tag made by Motorola, can be bent, torn or crumpled and still relay data to a reader. Although the price of a capacitively coupled tag is as low as 50 cents (US), it has a very limited range.[14]

Read-Only and Read-Write

Chip tags may be read-only or read-write. A read-only memory chip has an identification code recorded at the time of manufacture or when allocated to an object. Read-only tags are much cheaper and are typically used in passive tags.

Read-write tags can have their memory changed, or written to, many times. Because they enable their ID codes to be changed, they offer greater functions but at a greater cost – as much as $200 (US) each.[15]

Readers

RFID tags are interrogated by readers, which in turn are connected to a host computer. In a passive system, the RFID reader transmits an energy field that “wakes up” the tag and powers its chip, enabling it to transmit or store data. Active tags may periodically transmit a signal, much like a lighthouse beacon, so that data may be captured by multiple readers distributed throughout a facility.[16] RFID systems typically work at higher frequencies in the UHF (or ultrahigh) frequency band (between 900 Megahertz to 1.9 Gigahertz).

Readers may be portable handheld terminals, or fixed devices positioned at strategic points such as a store entrance, assembly line or toll booth. The reader is equipped with antennas for sending and receiving signals, a transceiver and a processor to decode data.

RFID readers typically cost $1,000 (US) or more. Companies may need many readers to cover all their factories, warehouses and stores. Readers typically operate at one radio frequency. If tags from three different manufacturers used three different frequencies, a retailer might have to have multiple readers in some locations, increasing the cost further.[17] With no standards in place regarding tags and readers, it is prohibitive for any organization to read multiple tags.

From Bar Code to Smart Label

Smart labelling is the latest technology, combining features of barcodes, Electronic Article Surveillance (EAS) and traditional RFID in ultra-thin tags. New RFID products, such as Philips Semiconductors' I·CODE chip and Zebra Technologies' smart label printer, now enable businesses to serve mass markets that require many millions of smart labels each year.

While barcodes have historically been the primary means of tracking products, RFID systems are being viewed by many businesses as the preferred technology for keeping tab on products and vehicles. One reason for this is because the read/write capability of an active RFID system enables the use of interactive applications.

RFID technology differs from bar codes in several important ways:

- Information is specific to that individual item. With bar code technology, every can of Coke has *the same UPC* or bar code number (a bottle of Coke in Toronto has the same number as a bottle of Coke in Tokyo). With RFID, *every individual Coke bottle* could have a unique ID number that could be linked to the person buying it when he or she scans a credit card or a frequent shopper card (i.e., a "registration system").

- RFID tags can be read from a distance instead of the line-of-sight required by a bar code system.

- RFID works in harsh environments and may also be read through a variety of substances or conditions such as snow, fog, ice, or paint, where barcodes have proved useless.[18]

- RFID systems enable tagged objects to 'speak' to electronic readers potentially over the entire course of a product's lifecycle – from production to disposal – providing retailers or manufacturers with an unblinking, voyeuristic view of consumer attitudes and purchase behaviour. The data transmitted by a tag may provide identification or location information, or specifics about the product tagged, such as price, colour, or place and date of purchase; and

- RFID systems enable stored data to be altered during product manufacturing stages or lifecycle.

To Smart Dust

RFID chips are also easy to hide. For example, they can be sewn into the seams of clothes, sandwiched between layers of cardboard, molded into plastic or rubber, and integrated into consumer package design. Companies are even experimenting with making the product packages themselves serve as antennas. New RFID technology heralds even smaller tags. Researchers at Corning have developed tiny coded beads invisible to the human eye that can be embedded in inks to tag currency and other documents, or added to substances like automobile paint, explosives, or other products that law enforcement officers or retailers have a strong interest in tracking. Researchers say that technology may be ready for commercial use in three to six years.[19]

Alien Technology of Morgan Hill, Calif. has developed new chip-making technology to make dust-size RFID microchips. Its new production facility will be able to make 80 billion chips a year.[20]

The potential scale of RFID systems could be shrunk even more dramatically based on work by a team of researchers at the University of California in Berkeley, Ca. They have developed a complete sensor system, which they call "smart dust," with its own power supply, programmable microprocessor and optical communication link – all within a cubic millimeter. A second research group has developed a new software operating system, called TinyOS, for networks of tiny sensors constrained by minimal hardware.[21]

Price Still Barrier to Adoption

RFID supporters envision a world where RFID reader devices are everywhere – in stores, cars, clothes and factories – even in our home refrigerators. But RFID tags will not become ubiquitous in consumer products as long as the price of the tags is viewed as prohibitively expensive by many businesses. RFID tags currently cost from 20 cents to $1 (US) each, which still makes them impractical for identifying millions of items that cost only a few dollars, according to estimates from the Auto-ID Center at the Massachusetts Institute of Technology.

MIT Auto-ID Center

The Auto-ID Center, spearheaded by the Massachusetts Institute of Technology and financed by sponsors including Proctor & Gamble, was formed to develop a low cost RFID tag suitable for mass retail applications. Founded in 1999, the Auto-ID Center is a partnership that now boasts over 100 global companies – including retailers, consumer product manufacturers, automakers and software companies – and six leading research universities.[22]

The MIT Center is also shepherding the creation of standards, like the Electronic Product Code (EPC) standard unveiled in September 2003, that it touts as the building blocks to create an "Internet of things."[23] The EPC code goes far beyond the widely used Universal Product Code – or UPC bar codes. The EPC can identify many more unique objects, as well as link an object to people and information through use of Internet addresses.[24]

The Auto-ID Center has also developed a multi-frequency reader that will be manufactured by MIT spinoff ThingMagic.[25] RFID systems use unlicensed frequencies bands, which gives rise to a lack of co-ordination because there is no universal frequency standard. That would mean a global company would require multiple systems for use in different countries.

MIT's experts predict that in quantities of one billion, RFID tags would approach 10 cents each. The holy grail of five-cent tags – the stated primary goal of the Auto-ID Center – would be attained in lots of 10 billion.[26] More recent technological developments may put a one-cent tag within reach, according to Sanjay Sarma, research director of the MIT Auto-ID Center. He believes a one-cent tag would fuel demand for RFID equal to that for bar codes.[27]

Estimates of the RFID market vary. But there is a consensus that big growth is not expected until after 2005 when the tag price is expected to fall significantly.[28] Market research firm International Data Corp. predicts shipments of handheld RFID readers alone will increase ten-fold by 2007.[29] The market for tags alone is expected to be worth more than $120-million (US) a year in 2006 equating to 2.4 billion tags at five cents a piece. As many as 40-billion objects could be tagged each year by the end of the decade when the market for RFID systems, software and tags could be worth $10 billion (US) a year, according to a report prepared for the MIT Auto-ID Center.[30]

Applications & Uses

Despite the current cost of RFID tags and readers, many organizations have begun implementing smart label technology.

In Canada, current uses of RFID include:

- ESSO Imperial Oil has been using RFID tags in its *SpeedPass* system since 1997 and Shell Oil in its *EasyPay* tags. Speedpass allows users to pay for their gas without using cash or a credit card through a transponder located in the pump that recognizes a user's ID code contained in a key tag.[31]

- Frequent users of the Highway 407 toll road north of Toronto are billed with RFID transponders;[32] and

- The Western Beef Development Centre in Saskatoon placed RFID tags on 292 calves in a trial at the University of Saskatchewan's Termuende research farm near Lanigan, Sask. in June 2002.[33] Meat packing plants are indicating that in the future they'll only provide carcass information if electronic tags are used, which will drive adoption of the electronic tags in livestock herds, says Gordon Stephenson, executive director of the Western Beef Development Centre. He adds electronic tags won't be valuable to the producer unless they also have a reader. He also said there needs to be a tie-in between the electronic tag and the Canadian Cattle Identification Agency number so there aren't separate trace-back, management and electronic tags. "Hopefully, sometime in the future, producers can have a management tag and this electronic tag will also be their CFIA animal ID tag."[34]

While RFID technology has not yet become widespread in Canada or the United States, corporations in Europe and Asia have moved forward with more aggressive plans to tag consumer products, spurred by improved performance, and decreased size and cost of RFID systems. Applications for RFID tags that have emerged include:

- Ford Motor Co. specified in 2001 that all tires provided in future vehicles are to contain a UHF transponder to allow speedy identification.

- Tire manufacturer Michelin recently began fleet testing of a radio frequency tire identification system for passenger and light truck tires.[35]

- Gillette announced in November 2002 that it would not wait for the development of an RFID standard and would order 500 million UHF transponder tags to replace barcodes in March 2003.[36] Gillette also teamed up with two major retailers, Wal-Mart in the United States and Tesco PLC in Great Britain, to test specially designed shelves that would allow for real-time tracking of inventory levels. The “smart shelves” would read radio frequency waves emitted by microchips embedded in millions of shavers and other products.[37]

- Microsoft announced that it would develop software that will enable retailers, manufacturers, and distributors to use RFID tags to track goods within stores and factories, as well as programs specifically designed to use the new retail tagging technology.[38]

- New Hanover County Public Library in North Carolina recently installed an RFID self-checkout workstation and a self-return book drop powered by VTLS, Inc. Three more libraries have made commitments to VTLS to install its RFID technology.

- German retail conglomerate Metro AG is developing “stores of the future,” in which groceries and household items sold in its Extra stores will be equipped with RFID tags.[39]

- Marks & Spencer, one of the largest retailers in the United Kingdom, is developing a massive project to tag clothing. The project is a follow-up to the company’s implementation of a program in 2002 to place RFID tags in 3.5 million produce delivery trays.[40]

- The Tokyo International Book Fair unveiled an RFID system in 2003 that would allow booksellers to track consumers’ in-store reading preferences.[41]

- Italian fashion retailer Prada deployed an RFID system in its trendy flagship store in New York City in late 2001 to label shoes, garments and accessories as part of a broad “smart retailer” technology trial.[42]

- Euro cash could be embedded with RFID tags if a reported deal between the European Central Bank and Hitachi becomes reality.[43] The European Central Bank is moving forward with plans to embed RFID tags as thin as a human hair into the fibers of Euro bank notes by 2005, despite consumer protests. A spokesman for the ECB in Frankfurt confirmed on July 4, 2003 that the bank intends to add further protection to the Euro.[44] (The 12 nations that currently use the Euro are Italy, Luxembourg, the Netherlands, Spain, Portugal, Ireland, Greece, Germany, France, Finland, Belgium and Austria.) The currency tags would enable information to be recorded about each transaction in which the currency is passed. Governments and law enforcement agencies hail the technology as a means of preventing money-laundering, black-market transactions, and even bribery demands for unmarked bills.[45]

Privacy Issues Loom

The Euro currency RFID deal would be a major boon to the nascent RFID industry, which has been seeking a major mass-market application. The volumes associated with such use would cause RFID tag prices to fall – and further stimulate adoption, according to researchers at MIT's Auto-ID Center. However, consumer advocates fear that use of RFID technology would eliminate the anonymity that cash affords.

RFID is also being deployed to track and identify individuals, which further underscores some of the profound privacy implications of the technology.

Alexandra Hospital in Singapore began using a new RFID tracking system in its accident and emergency department in the wake of the Severe Acute Respiratory Syndrome (SARS) outbreak in spring 2003. All patients, visitors, and staff entering the hospital are issued a card embedded with an RFID chip, so that if they are later diagnosed with SARS, a record of all other individuals with whom that person has been in contact can be immediately determined. Other hospitals in Singapore are expected to adopt similar technology.[46]

Opposition Mounts

It is the fear of ubiquitous tracking by anybody with a proper reader – without knowledge or consent – that has prompted many individuals and privacy advocacy organizations to voice strong opposition to widespread implementation of RFID tags. Consumer boycotts were organized in 2003 year against two companies that planned to adopt RFID tags.[47]

Italian clothier Benetton Group sparked a furor when it announced that it would implant RFID tags in the apparel products it retails.[48] Public opposition forced the company to cancel its plans.[49] (Benetton had planned to put *I Code* semiconductor tags made by Philips Semiconductor into clothing labels made by Lab ID of Bologna, Italy, and scanned by handheld devices made by Psion Teklogix Inc. of Mississauga, Ont.)

Gillette also stirred privacy concerns when it announced plans in January 2003 to buy 500 million RFID tags.[50] But its subsequent trial of a so-called "smart shelf" with Wal-Mart at a store in Massachusetts and in Great Britain with Tesco's retail outlet in Cambridge led to calls for consumer boycotts of its products when it was revealed that Gillette was taking photographs of unsuspecting consumers.[51] In a nod to public opposition, Wal-Mart announced that it would limit the use of RFID tags to warehouses and distribution centers, canceling its smart shelf test with Gillette.[52]

The debate over RFID technology touches upon many controversial privacy policy issues. At its most fundamental, widespread use of RFID tags could enable corporations to track every move consumers make. But RFID is only useful if it is linked to a source of market or business intelligence such as inventory databases, demographic or psychographic markers.[53] And the ability of RFID systems to enable the linking of product information with the identity of a specific consumer is problematic without proper safeguards, as the Gillette trial demonstrated.

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

The development of powerful customer relation management (or CRM) databases underscores the argument of one leading Canadian privacy expert that "surveillance has become a creeping and potential function of all personal databases."[55] Yet, the unfettered use of those customer-specific databases can also be highly problematic for a business. A well-publicized incident involving U.S.-based online bookseller Amazon.com in early 2001 illustrated that more than privacy is at stake with the proper use of new digital locating and marketing technologies. The strategy of dynamic pricing, which gauges a shopper's desire and financial means in order to set prices accordingly, also raises the prospect of price-fixing. Amazon.com was caught selling the same DVD movies to different customers at different prices.[56] Injudicious use of technologies including RFID and CRM stands to further imperil consumer trust in digital networks.

Informational Privacy and Loss of Control

The overriding concern shared by many opponents of RFID is comparable to the fears associated with other potentially intrusive technologies, such as biometrics and cellphone location finding, that impact an individual's informational privacy.[57] This is the idea that information about an individual belongs to that person, and is to be communicated or not, as the individual determines. That concept is also known as informational self-determination.[58] The loss of control over an individual's personal information has a significant impact on the individual's ability to be autonomous. As one scholar has noted:

> … Loss of autonomy means loss of one's capacity to control one's life… A right to control information about one's self is fundamental to being a self-determining and responsible being.[59]

Consumers generally accept that any transaction beyond the use of cash requires the disclosure of some personal information. And most people acknowledge that companies need to collect, use and disclose customer information to conduct business. However, informational privacy issues arise when companies use or collect data with RFID systems that go beyond customer expectations. These issues were identified in the Electronic Privacy Information Centre's (EPIC) recent policy paper on RFIDs[60] EPIC recognized that, while there are beneficial uses of RFID, the technology could be deployed in ways that threaten privacy and civil liberties. For example:

- **Hidden placement of tags.** RFID tags can be embedded into/onto objects and documents without the knowledge of the individual who obtains those items. As radio waves travel easily and silently through fabric, plastic, and other materials, it is possible to read RFID tags sewn into clothing or affixed to objects contained in purses, shopping bags, suitcases, and more.

- **Unique identifiers for all objects worldwide.** The Electronic Product Code potentially enables every object on earth to have its own unique ID. The use of unique ID numbers could lead to the creation of a global item registration system in which every physical object is identified and linked to its purchaser or owner at the point of sale or transfer.

- **Massive data aggregation.** RFID deployment requires the creation of massive databases containing unique tag data. These records could be linked with personal identifying data, especially as computer memory and processing capacities expand.

- **Hidden readers.** Tags can be read from a distance, not restricted to line of sight, by readers that can be incorporated invisibly into nearly any environment where human beings or items congregate. RFID readers have already been experimentally embedded into floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into retail shelving and counters, making it virtually impossible for a consumer to know when or if he or she was being "scanned."

- **Individual tracking and profiling.** If personal identity were linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent. For example, a tag embedded in a shoe could serve as a de facto identifier for the person wearing it. Even if item-level information remains generic, identifying items people wear or carry could associate them with, for example, particular events like political rallies.

Although the ability of RFID readers to collect data from tags once a consumer has left a store or moved beyond the readers' range is currently limited, consumer groups and privacy advocates note that RFID technology is quickly advancing, while measures to protect individual privacy by limiting the amount and type of information corporations can collect about their customers is perceived as lacking.[61]

Safeguards Needed

As RFID technology becomes more advanced, consumers fear the loss of all ability to evade products implanted with chips. It could soon be impossible for consumers to know whether a product or package contains an RFID tracking chip. "There is a worry in our field as to how these things will be used, given the lack of coherent privacy regulations," said Dan Moniz, staff technologist at the Electronic Frontier Foundation, a San Francisco-based digital watchdog organization.[62]

Big Brother Fears

Calls by government law enforcement and national security agencies in the wake of the September 11, 2001 terrorist attacks to link public and private databases together have heightened concerns about the "Big Brother" implications of any data collection technology such as RFID. Such fears can no longer be dismissed as unreasonable when considered against the controversial "Total Information Awareness" (TIA) proposal of the U.S. Defence Advanced Research Projects Agency. Its stated aim was to gather data from all available sources and compile it into a mammoth database whose scope would include transaction data contained in current databases, such as financial histories, medical records, communications, travel records and commercial and other private transactions.[63]

Public fears have not been eased by MIT's Auto-ID Center presentation of its vision of RFID technology to U.S. Homeland Security Secretary Tom Ridge last year. Many sponsors of the MIT Center believe Ridge's blessing is key to widespread acceptance of the technology. The leaked minutes of a meeting on RFID attended by an official from the U.S. Department of Defence state that RFID technology will catch on "when the government mandates it for homeland security reasons."[64]

Law-enforcement agencies in Canada have also thought about gaining access to RFID systems. The Ontario Provincial Police has reportedly investigated the efficacy of developing a reader that could enable them to interrogate "any and all tags that might be attached to virtually anything," according to Clifford Horowitz, chairman and chief executive officer of SAMSys Technologies of Richmond Hill, Ont.[65]

Those concerns have led numerous organizations, including the EFF, to call for widespread debates about the social implications of RFID. One major U.S. newspaper also recently declared that it is time for legislators to call for a timeout on adopting further intrusive technologies and security laws.[66]

Blocker Tags

Pending those broader discussions, opponents of RFID tags have proposed various measures to side-step the chips' information-gathering, ranging from boycotting the products of companies which use or plan to implement RFID technology to disabling the tags by crushing or puncturing them, or carrying blocker tags that impair readers by simulating the signals of many different RFID tags.

Researchers at a leading security technology firm have developed an RFID blocker tag. Similar in size and cost to a conventional RFID tag, the prototype blocker tag made by RSA Security disrupts the transmission of information to scanning devices and thwarts data collection.[67] While an ordinary RFID tag is a simple, cheap (e.g., five-cent) passive device intended as an “electronic bar-code’‘ for use in supply-chain management, a blocker tag is a cheap passive RFID device that can simulate many ordinary RFID tags simultaneously. When carried by a consumer, a blocker tag thus “blocks’‘ RFID readers. It can do so universally by simulating all possible RFID tags. Or a blocker tag can block selectively by simulating only selected subsets of ID codes, such as those by a particular manufacturer, or those in a designated “privacy zone.’‘[68]

However, such a solution may not be ideal, either for consumers or businesses alike. Blocker tags are expensive and place the onus of privacy protection solely on consumers.

Kill Switches

The MIT Auto-ID Center has endorsed incorporating a “kill switch” into specifications for RFID tags, helping assuage some privacy concerns over the use of the tags. Several RFID manufacturers, including Philips Semiconductor, Alien Technology, and Matrics, plan to use the kill switch in their tags.[69]

The kill switch would allow a company to deactivate the RFID tag. Once disabled by the kill switch, the tag cannot be reactivated. Under the current configuration of the kill switch, customers would be asked by clerks if they would like the RFID tag to be disabled. That scenario seems unwieldy in a retail setting, however, where clerks could not be reasonably expected to convey the nuances of the impact of RFID tags to consumers who may not be familiar with them.

A draft proposal by the MIT Auto-ID Center recommends retailers disable the tags at checkout, but only when shoppers ask, said Kevin Ashton, a brand manager at Procter & Gamble and director of the center.[70] But few retailers that are testing RFID tags in the United States and Europe are disabling the tags, according to opponents of the technology.[71]

Opt-In & Consent

“As soon as an RFID tagged product becomes the property of the consumer and has officially left the supply chain, that same tagging becomes a potential invasion of privacy,” Martin Butler, founder and president of the Butler Group, stated in his *Opinionwire* newsletter.[72]

At least one major retailer in Europe is taking a different approach to privacy. Germany's largest retail chain, Metro AG, will only collect information from RFID tags if a customer opts in and asks to be included in a program that notifies them of specials on products they frequently buy. Metro is currently testing RFID tags on bottles of Pantene shampoo at its Future Store in Rheinberg near Dusseldorf. Metro is also working with IBM Corp. to develop a device to disable the tags when shoppers leave the store.[73]

The strongest finding of public opinion survey research on RFID conducted in the United States, Europe and Asia by the Auto-ID Center is that consumers must have a choice. "This choice must take two forms," states Helen Duce, director of the Auto-ID European Centre at the University of Cambridge. "First, it must be clear when and where the technology is being used. Second, there must be an option to 'kill' the tag at point of sale."[74]

The principle of empowering consumers to "opt-in" requires informed consent. That is the notion behind the Platform for Privacy Preferences (P3P) protocol that requires Internet users to reveal their privacy preferences *before* they are allowed to access information on a Web site. Even some RFID proponents believe consumers need a comparable "RFID bill of rights," as noted author, Simson Garfinkel, an MIT graduate and member of the Auto-ID Center's privacy advisory council, told a privacy association.[75]

Pillars of Privacy

The informational privacy concerns surrounding RFID may be effectively addressed if its use is in accordance with Fair Information Practices, the internationally recognized principles that serve as the minimum privacy standards applicable to all personal information collection, not only to RFID.[76] The international community of Data Protection Commissioners has issued a resolution regarding RFID deployment based on Fair Information Practices (attached as Appendix A).[77] Those principles also form the basis of data protection schemes around the world, including Canada's personal information protection law. At least three principles that are central pillars of informational privacy protection have been recognized by the RFID industry that must be respected by any deployment and use of RFID systems:[78]

- **Notice and consent –** The right to know whether a product contains an EPC RFID tag, and whether an RFID reader is being used in a public place. Participation in an RFID application should be strictly voluntary. Collection of data under informed consent means covert capture of information should not be permitted. Informed consent is recognized as the primary tool available to individuals to protect their privacy from technological invasion.

- **Choice –** The right to have the RFID tag in a purchased product deactivated without cost.

- **Control –** The right to have personal identity information kept separate from information identifying an object.

But those three requirements are only a portion of the Fair Information Practices. Adherence to all those practices is essential to achieve full informational privacy. Those principles have been outlined in previous discussion papers issued by the Ontario Information and Privacy Commissioner[79] and (in brief) include:

- **Collection Limitation Principle**: Requires limits to the collection of personal information and the obtaining of any data by lawful and fair means with the knowledge or consent of the subject. This principle is a consumer's first line of defence and is essential to enable negotiation about the terms of use and disclosure of personal information.[80]

- **Data Quality Principle**: Stipulates that personal data should be relevant to the purposes for which they are to be used and should be accurate, complete and up-to-date.

- **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes.

- **Use Limitation Principle**: Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified under the preceding purpose specification principle except with consent or by legal authority.

- **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure.

- **Openness Principle**: There should be a general policy of openness about developments, practices and policies with respect to personal data.

- **Individual Participation Principle**: An individual should have the right to ascertain or confirm whether a data controller has data relating to him or her and to challenge that data.

- **Accountability Principle**: A data controller should be accountable for complying with measures that give effect to the principles stated above.

The RFID position paper, released by EPIC, identifies additional practices that should be prohibited in order to fully protect consumers:

- Merchants must be prohibited from forcing or coercing customers into accepting live or dormant RFID tags in the products they buy.

- There should be no prohibition on individuals to detect RFID tags and readers and disable tags on items in their possession.

- RFID must not be used to track individuals absent informed and written consent of the data subject. Human tracking is inappropriate, either directly or indirectly, through clothing, consumer goods, or other items.

- RFID should never be employed in a fashion to eliminate or reduce anonymity. For instance, RFID should not be incorporated into currency.[81]

New Label Laws for Smart Labels?

A U.S. consumer advocacy group – Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) – has asked the U.S. Congress to consider adopting new federal labeling legislation aimed specifically at RFID. The *RFID Right to Know Act of 2003* would require complete disclosure and mandatory labels on any consumer products containing RFID devices.[82]

Conclusion: Good Privacy Is Good Business

Technology-driven transactions, or e-commerce, should not involve a tradeoff in which consumers relinquish widening amounts of their privacy in return for greater convenience.

Businesses should not grudgingly deal with privacy merely because new legislation, such as the federal *Personal Information Protection and Electronic Documents Act* [83](PIPEDA), requires it. There are many benefits to privacy beyond the need to protect customer data to avoid damage to a business's reputation. Businesses need to address the privacy concerns ignited by RFID if the potential economic benefits of the technology are to be realized.

Businesses that put customers in control of their online privacy options increase consumer faith in the online world – and promote greater acceptance of e-commerce.[84] Good privacy management requires a centralized approach involving every area of a firm; indoctrination; organizational re-engineering – including data management processes; and implementation of long-term compliance strategies.

Ultimately, though, the issue comes down to consumer empowerment and trust. "Companies rolling out RFID must have a clear and rigidly enforced policy on the deactivation of their tracking mechanisms, as having a cost-effective supply chain will be pretty meaningless if nobody trusts you enough to buy from you,"[85] states Martin Butler.

Simply put, privacy protection is good for business.[86]

Appendix 'A' — International Conference of Data Protection & Privacy Commissioners

Resolution on Radio-Frequency Identification
Final Version
20 November 2003

Following a proposal by the Data Protection and Access to Information Commissioner Brandenburg, the Independent Center for Privacy Protection Schleswig-Holstein, Germany, the Spanish Data Protection Agency and the Data Protection Commissioner of the Canton Zug, Switzerland, the International Conference resolves that:

Radio-frequency identification (RFID) technology is increasingly being deployed for a variety of purposes. While there are situations in which this technology can have positive and benign effects, there are also potential privacy implications. RFID tags are so far primarily used to identify and manage objects (products) to control the supply chain or to protect the authenticity of the product brand; however, they could be linked with personal information such as credit card details and even used to collect such information, or to locate or profile persons possessing tagged objects. This technology could allow for the tracing of individuals and for linking collected information with existing databases.

The Conference highlights the need to consider data protection principles if RFID tags linked to personal information are to be introduced. All the basic principles of data protection and privacy law have to be observed when designing, implementing and using RFID technology. In particular:

a) any controller – before introducing RFID tags linked to personal information or leading to customer profiles – should first consider alternatives which achieve the same goal without collecting personal information or profiling customers;

b) if the controller can show that personal data are indispensable, they must be collected in an open and transparent way ;

c) personal data may only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve (or carry out) this purpose, and

d) whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags.

These principles should be taken into account when designing and using products with RFID.

The remote reading and activating of RFID tags, without any reasonable opportunity for the person in possession of the tagged object to influence this process, would raise additional privacy concerns.

The Conference and the International Working Group on Data Protection in Telecommunications will monitor closely the technological developments in this field in greater detail in order to ensure the respect for data protection and privacy in the context of "ubiquitous computing".

Explanatory Note:

Radio-frequency identification tags (RFID tags) are currently being tested and increasingly being used as a more advanced form and possible replacement of bar codes ("smart labels"). The size of these microchips is about one-third of a millimetre (and smaller – "smart dust"). Most of them operate as passive transponders (without batteries) by listening to radio signals sent by transceivers (RFID readers) and using the energy of the received radio signal to reflect and answer it. Active RFIDs have a greater range (depending on the readers used). Since prices for RFID microchips and readers are dropping their widespread deployment becomes increasingly economically viable. RFID tags are likely to become essential drivers of ubiquitous (or pervasive) computing. Due to their storage and capacity for interactive communication they are far more powerful than bar codes. In addition they provide for unique identification of each tagged unit whereas bar codes are identical for every unit of the same product.

RFID tags can be used to install "smart shelves" in stores in order to better manage the supply chain and facilitate the replenishments of goods or supplies (e.g., the case of Gillette razors). They may also be used for easy (contact-less) payment at the point of sale especially if linked with credit cards. Furthermore, an employer may use the technology to tag his property in order to reduce theft by employees. They could be linked with video surveillance cameras to check employee as well as customer behaviour. Specific documents may be tagged to be traced more easily in an office. Identity cards as well as travel documents (passports, visas) may be equipped with RFID tags. More recently, the European Central Bank has announced that Euro notes will be issued with RFID tags in order to fight counterfeiting and money laundering as well as to control circulating notes. Washable RFID tags can be embedded in clothes ("wearable computing") in order to prevent or detect counterfeiting of specific brands and to prove the authentic manufacture of the product. Other possible applications range from car keys (immobilizers) to container management.

The RFID technology has numerous privacy implications. This is obvious in the case of implanted microchips. But also in the more widespread case of tagged objects and goods, undoubtedly the information transmitted also refers to the person carrying or wearing (or otherwise associated with) a tagged item or a "constellation" of brands, thereby revealing the individual's taste. Therefore personal data can be processed and transmitted or read with the help of RFIDs or at least such object-related information can easily be linked with personal information (e.g. , when a credit card is used for buying the tagged item). RFID tags have the potential of tracking the movements of a person who possesses or handles tagged objects. Plans to afford technical devices legal protection against circumvention may prevent data subjects from disabling or deactivating RFID tags which function in a privacy-unfriendly way (e.g., after having paid and left the shop).

Since this issue has led to a growing public debate in a number of countries, it is recommended that the International Conference addresses the related privacy problems at this stage in order to encourage privacy-friendly solutions which have been proposed. The International Working Group on Data Protection in Telecommunications, at its 34th meeting in Berlin on September 2 and 3, 2003, has expressed its support for this proposal.

References & Further Reading

Katherine Albrecht, “RFID: Tracking Everything Everywhere,” *Denver University Law Review*, Summer 2002.

Mark Baard, “Radio Tag Debut Set for This Week,” *Wired*, September 15, 2003. www.wired.com/news/print/0,1294,60408,00.html

“Claim: RFID Will Stop Terrorists,” *Wired*, Aug. 8, 2003. www.wired.com/news/privacy/0,1848, 59624,00.html

Ann Bednarz and Denise Dubie, “RFID helps improve asset visibility,” *Network World*, July 18, 2003. www.itworldcanada.com/index.cfm/ci_id/45953.htm

Colin J. Bennett and Rebecca Grant. *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: University of Toronto Press, 1999.

Jane Black, “Playing Tag with Shoppers’ Anonymity,” *Business Week Online*, July 21, 2003. www.businessweek.com/technology/content/jul2003/tc20030721_8408_tc073.htm

Christopher Boone and Meredith Whalen, “Benetton Unites with RFID: IDC Predicts Low Adoption in Retail Until 2005,” *IDC Flash*, #29131, Framingham, Mass.: International Data Corp., March 2003.

Kevin Bonsor, “How Smart Labels Will Work,” *How Stuff Works*, http://electronics.howstuffworks.com/smart-label.htm

Richard Bray, “Radio ID tags track inventory,” *Summit: Canada’s Magazine on Public Sector Purchasing*, February 2003, p. 3. www.summitconnects.com/Articles_Columns/PDF_Documents/060108.pdf

“Breakthrough on 1-cent RFID Tag,” *RFID Journal*, December 2, 2002.

David Brock, “The Electronic Product Code (EPC): A Naming Scheme for Physical Objects,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, January 2001.

California. State Senate Subcommittee on New Technologies. *Hearing on RFID and Privacy*, “Testimony of Kevin Ashton, Executive Director Auto-ID Center,” August 18, 2003.

Canada. Department of Communications and Department of Justice, *Privacy and Computers*, Ottawa: Information Canada, 1972.

Canada. The Privacy Commissioner of Canada. “A Day in the Life…or how to help build your superfile,” *Annual Report 1995-96*, Ottawa: 1996. Online Fact Sheet at www.privcom.gc.ca/fs-fi/02_05_d_01_e.asp

David Canton, “RFID technology raises privacy issues,” *The London Free Press*, September 6, 2003.

CASPIAN, “RFID Site Security Gaffe Uncovered by Consumer Group,” July 7, 2003. http://www.nocards.org/press/pressrelease07-07-03_1.shtml

“RFID Right to Know Act of 2003,” http://www.nocards.org/rfid/rfidbill.shtml

“Consumer Group Unveils RFID Labeling Legislation,” June 11, 2003. http://www.nocards.org/press/pressrelease06-11-03.shtml

Ann Cavoukian & Mike Gurski. “Privacy In a Wireless World.” Speech notes, Toronto; Ontario Information and Privacy Commission, April 2001.

Ann Cavoukian & Tyler Hamilton, *Privacy Payoff: How Successful Businesses Build Customer Trust*, Toronto: McGraw-Hill Ryerson, 2002.

Winston Chai & Richard Shim, “Benetton Takes Stock of Chip Plan,” *CNET News.com*, April 7, 2003 http://news.com.com/2100-1020-995744.html?tag=fd_top

“Japan: Shopping Habits Tracked by RFID,” *CNETAsia*, May 9, 2003. http://asia.cnet.com/newstech/systems/0,39001153,39129324,00.htm

Clyde Crews Jr., “Put Controls on Emerging ‘Surveillance State,’ *The Detroit News*, Series on Losing Liberty: Privacy, June 23, 2003.

Claudia H. Deutsch & Barnaby J. Feder, “A Radio Chip in Every Consumer Product,” *New York Times*, February 25, 2003. http://nytimes.com/2003/02/25/technology/25THEF.html

Helen Duce, “Public Policy: Understanding Public Opinion,” *Executive Briefing*, University of Cambridge, Auto-ID Center: February 2003.

Joe Dunlap et. al., “If You Build It, They Will Come: EPC Forum Market Sizing Analysis,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, February 2003, CAN-AutoID-BC-007. Prepared by Accenture.

Jim Eagle, “RFID: The Early Years 1980-1990,” 2001. http://members.surfbest.net/eaglesnest/rfidhist.htm

Electronic Privacy Information Center, "Radio Frequency Identification (RFID) Systems," Washington, D.C., August 11, 2003. www.epic.org/privacy/rfid/

Klaus Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, New York: John Wiley & Sons Ltd., 2003. 2nd Ed. (Translated from German).

Alorie Gilbert & Richard Shim, "Wal-Mart Cancels 'Smart Shelf' Trial," *CNET News.com*, July 9, 2003 http://news.com.com/2100-1019_3-1023934.html?tag=fd_lede1_hed

"Gillette Confirms RFID Purchase," *RFID Journal*, January 7, 2003. www.rfidjournal.com/article/articleprint/258/-1/1/

"Glowing Beads Make Tiny Bar Codes," *Technology Research News*, April 3, 2003.

Carol Gould, ed., *The Information Web: Ethical and Social Implications of Computer Networking*, San Francisco: Westview Press Inc., 1989.

Tyler Hamilton. "Nowhere to Hide," *The Toronto Star*, Special Report on Privacy. Jan. 8, 2001.

"Hitachi Unveils Smallest RFID Chip," *RFID Journal*, March 14, 2003. http://216.121.131.129/article/articleprint/337/-1/1/

Paul Hoskins, "Retail Future: Painless Checkout, Knowing Scanners," *Reuters*, May 14, 2003. www.forbes.com/home_europe/newswire/2003/05/14/rtr970418.html

"Intellident Selected by Marks & Spencer to Tag 350 Million Items of Clothes," Intellident, 2003. www.intellident.co.uk/Press/PressReleases/1051624519

Deborah G. Johnson, *Computer Ethics*, Englewood Cliffs, N.J.: Prentice-Hall, 1985.

Junkbusters Corp., "RFID Devices and Privacy," April 8, 2003. http://www.junkbusters.com/rfid.html

J.M. Kahn, R.H. Katz and K.S.J. Pister, "Mobile Networking for Smart Dust," *ACM/IEEE International Conference on Mobile Computing and Networking* (MobiCom 99), Seattle, WA., August 17-19, 1999.

Cedric Laurent et. al., *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments*, Washington, D.C. and London: EPIC & Privacy International, September 2003. http://www.privacyinternational.org/survey/phr2003/

Toby Lester. "The Reinvention of Privacy," *The Atlantic Monthly*, March 2001, pp. 27-39.

Wayne Madsen, *Handbook of Personal Data Protection*, New York: Stockton Press, 1992.

Janis Mara, "Euro Scheme Makes Money Talk," *Wired*, July 9, 2003. www.wired.com/news/print/0,1294,59565,00.html

Jennifer Maselli, "Privacy Group Focuses On RFID," *RFID Journal*, August 26, 2003.

Andy McCue, "Privacy Fears Over RFID Must Come Before Profit," *Silicon.com*, August 26, 2003. http://silicon.com/news/500022/1/5730.html

Declan McCullagh, "RFID Tags: Big Brother in Small Packages," *CNET News.com*, January 13, 2003.

"Michelin to Embed Electronic ID Tags in Tires," *Reuters*, January 14, 2003 http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=2045403

"Microsoft to Develop Software for Radio Tags," *Reuters*, June 10, 2003 http://asia.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=2905169

Gregory Miller. "Building Privacy and Security Solutions into the Technological Architecture." Presentation to the Federal Trade Commission of the United States, Public Workshop. *The Mobile Wireless Web, Data Services and Beyond: Emerging Technology and Consumer Issues*. Dec. 11, 2000. Available at: http://www.ftc.gov/bcp/workshops/wireless/comments/miller.htm

MIT Auto-ID Center, *Technology Guide*. www.autoidcenter.com/new_media/brochures/Technology_Guide.pdf

"Bringing Down Tag Costs." http://www.autoidcenter.org/

Alex Niemeyer, Minsok Pak and Sanjay Ramaswamy, "Smart Tags For Your Supply Chain," *The McKinsey Quarterly*, 2003 (Number 4).

Ontario. Office of the Information and Privacy Commissioner, *Consumer Biometric Applications: A Discussion Paper*, Toronto: September 1999. http://www.ipc.on.ca/.

"Privacy Protection Makes Good Business Sense," Toronto: October 1994. http://www.ipc.on.ca/

"Privacy Alert: A Consumer's Guide to Privacy In the Marketplace," Toronto: May 1994. http://www.ipc.on.ca/

"Opposition to RFID Tracking Grows," *RFID Journal*, Jan. 20, 2003 http://www.rfidjournal.com/article/articleview/275/1/1/

Organisation for Economic Co-operation and Development, *Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data*, Paris: OECD, September 1980.

Kris Pister, “Smart Dust: Autonomous sensing and communication in a cubic millimeter,” Berkeley: University of California at Berkeley, 2001. www-bsac.eecs.berkeley.edu/~pister/SmartDust/

Peter Reuell, “You are being watched: Everyday activities leave trail of electronic data,” January 5, 2003.

Mark Roberti, “What Other Retailers Can Learn From Prada,” *RFID Journal*, July 2002.

Simon Romero. “Locating Devices Gain In Popularity But Raise Concern,” *The New York Times*, March 4, 2001, A1.

Linda Rosencrance, “Update: Benetton Details Decision on ID Clothing Tags,” *ComputerWorld*, April 7, 2003.

Rachel Ross, “Logged On For Life,” *The Toronto Star*, @Biz, September 8, 2003, D1.

Sanjay Sarma, “Towards the 5¢ Tag,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, November 2001. www.autoidcenter.org/publishedresearch/MIT-AUTOID-WH-006.pdf

Sanjay Sarma, Stephen Weiss and Daniel Engels, “RFID Systems and Security and Privacy Implications,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, November 2002. www.autoidcenter.org/publishedresearch/MIT-AUTOID-WH-014.pdf

Sanjay Sarma, David Brock and Kevin Ashton, “The Networked Physical World: Proposals for Engineering the Next Generation of Computing, Commerce & Automatic-Identification,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, October 2000.

Tom Ahlkvist Scharfeld, “An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design,” *Master Thesis*, Submitted to Massachusetts Institute of Technology, August 2001.

Julia Scheeres, “No Cyborg Nation Without FDA’s OK,” *Wired*, October 8, 2002. www.wired.com/news/print/0,1294,55626,00.html

Frederick Scholl and Jay Hollander, “The Changing Privacy and Security Landscape,” *Business Communications Review*, May 2003, pp. 54-57.

Ross Sealfon, *US RFID-Enabled Handheld Device Forecast and Analysis, 2002-2007: Defining RFID*, Framingham, Mass.: International Data Corp., Doc# 29854, August 2003.

Richard Shim, “Security Firm Aims To Ease RFID Concerns,” *CNET News.com*, August 28, 2003.

"Sony, Philips to Test RFID Platform," *RFID Journal*, May 8, 2003.

John Stermer, "Radio Frequency ID: A New Era for Marketers?" ACNielsen, *Consumer Insight*, Winter 2001. http://www.acnielsen.com/pubs/ci/2001/q4/features/radio.htm

"Stop Technology from Destroying Privacy," *The Detroit News*, Editorial, June 23, 2003.

Bill Strautman, "RFID tag retention rate as good as regular tags," *The Western Producer*, April 7, 2003. www.producer.com/articles/20030403/livestock/20030403ls05.html

Lawrence Surtees, *Nowhere to Hide: Privacy Implications of Wireless Location Technology*, Toronto: IDC Canada, Bulletin CA025TLH, March 2001.

United States. Department of Housing and Urban Development. "Homeless Management Information Systems (HMIS) Data and technical Standards Notice," *Federal Register*, 68:140, Washington, D.C.: July 22, 2003, pp. 43430-43454.

Bob Violino, "RFID Opportunities and Challenges," *RFID Journal*, 2002.

James Weir, "RFID Tags and IT Services," *IDC Study*, Framingham, Mass.: International Data Corp., #MS01K, April 2003.

Jeff Wilson, "RFID Benefits Can Outweigh Higher Cost," *IT Focus*, September 1, 2002. ITWorld Canada.com. www.itworldcanada.com/index.cfm/ci_id/16255.htm

John Wolff, *RFID Tags – An Intelligent Bar Code Replacement*, IBM Global Services: 2001.

Junko Yoshida, "Euro Bank Notes to Embed RFID Chips by 2005," *EE Times*, December 19, 2001 http://www.eetimes.com/story/OEG20011219S0016

Zebra Technologies, "RFID: The Next Generation of AIDC," *Application White Paper*, Vernon Hills, Ill.: 2003. http://www.zebra.com/whitepapers/11315Lr2RFIDTechnology.pdf

Notes

1. See: Canada. The Privacy Commissioner of Canada. "A Day in the Life…or how to help build your superfile," *Annual Report 1995-96*, Ottawa: 1996. Online Fact Sheet at www.privcom.gc.ca /fs-fi/02_05_d_01_e.asp; and: Tyler Hamilton. "Nowhere to Hide," *The Toronto Star*, Special Report on Privacy. Jan. 8, 2001.

2. "Stop Technology from Destroying Privacy," *The Detroit News*, Editorial, June 23, 2003.

3. Peter Reuell, "You are being watched: Everyday activities leave trail of electronic data," January 5, 2003.

4. Rachel Ross, "Logged On For Life," *The Toronto Star*, @Biz, September 8, 2003, D1.

5. See: David Canton, "RFID technology raises privacy issues," *The London Free Press*, September 6, 2003; and: Mark Baard, "Radio Tag Debut Set for This Week," *Wired*, September 15, 2003. www.wired.com/news/print/0,1294,60408,00.html.

6. See: Alex Niemeyer, Minsok Pak and Sanjay Ramaswamy, "Smart Tags For Your Supply Chain," *The McKinsey Quarterly*, 2003 (Number 4).

7. Ann Bednarz and Denise Dubie, "RFID helps improve asset visibility," *Network World*, July 18, 2003. www.itworldcanada.com/index.cfm/ci_id/45953.htm

8. Cited in: MIT Auto-ID Center. "The New Network: Identify Any Object Anywhere Automatically," Cambridge, Mass.: Massachusetts Institute of Technology, May 2002.

9. See: Jim Eagle, "RFID: The Early Years 1980-1990," 2001. http://members.surfbest.net/eaglesnest/rfidhist.htm

10. Tom Ahlkvist Scharfeld, "An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design," *Master Thesis*, Submitted to Massachusetts Institute of Technology, August 2001, p. 9.

11. MIT Auto-ID Center, *Technology Guide*. www.autoidcenter.com/new_media/brochures/Technology_Guide.pdf

12. "Hitachi Unveils Smallest RFID Chip," *RFID Journal*, March 14, 2003. http://216.121.131.129/article/articleprint/337/-1/1/

13. For an advanced and comprehensive engineering treatment of RFID technology, see: Klaus Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, New York: John Wiley & Sons Ltd., 2003. 2nd Ed. (Translated from German).

14. Kevin Bonsor, “How Smart Labels Will Work,” *How Stuff Works*, http://electronics.howstuffworks.com/smart-label.htm

15. Scharfeld, *op.cit*., p. 11; and: Bonsor, *op. cit*., p. 3.

16. Zebra Technologies, “RFID: The Next Generation of AIDC,” *Application White Paper*, Vernon Hills, Ill.: 2003. http://www.zebra.com/whitepapers/11315Lr2RFIDTechnology.pdf

17. Electronic Privacy Information Center, “Radio Frequency Identification (RFID) Systems,” Washington, D.C., August 11, 2003, p. 2. www.epic.org/privacy/rfid/

18. Electronic Privacy Information Center, “Radio Frequency Identification (RFID) Systems,” Washington, D.C., August 11, 2003. www.epic.org/privacy/rfid/

19. “Glowing Beads Make Tiny Bar Codes,” *Technology Research News*, April 3, 2003; and: EPIC, *Ibid*., p. 5.

20. MIT Auto-ID Center. “Bringing Down Tag Costs.” www.autoidcenter.org

21. See: J.M. Kahn, R.H. Katz and K.S.J. Pister, “Mobile Networking for Smart Dust,” ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 99), Seattle, WA., August 17-19, 1999; and: Kris Pister, “Smart Dust: Autonomous sensing and communication in a cubic millimeter,” Berkeley: University of California at Berkeley, 2001. www-bsac.eecs.berkeley.edu/~pister/SmartDust/

22. In addition to MIT, those university members include: the University of Cambridge in the United Kingdom, the University of Adelaide in Australia, Keio University in Japan, Fudan University in China and the University of St. Gallen of Switzerland.

23. David Brock, “The Electronic Product Code (EPC): A Naming Scheme for Physical Objects,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, January 2001. Sanjay Sarma, David Brock and Kevin Ashton, “The Networked Physical World: Proposals for Engineering the Next Generation of Computing, Commerce & Automatic-Identification,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, October 2000. See also: Mark Baard, “Radio Tag Debut Set for This Week,” *Wired*, September 15, 2003. www.wired.com/news/print/0,1294,60408,00.html

24. Brock, *Ibid*.

25. Ann Bednarz and Denise Dubie, “RFID helps improve asset visibility,” *Network World*, July 18, 2003. www.itworldcanada.com/index.cfm/ci_id/45953.htm

26. Declan McCullagh, “RFID Tags: Big Brother in Small Packages,” *CNET News.com*, January 13, 2003.

27. Sanjay Sarma, “Towards the 5¢ Tag,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, November 2001. www.autoidcenter.org/publishedresearch/MIT-AUTOID-WH-006.pdf; and: “Breakthrough on 1-cent RFID Tag,” *RFID Journal*, December 2, 2002.

28. Joe Dunlap et. al., “If You Build It, They Will Come: EPC Forum Market Sizing Analysis,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, February 2003, CAN-AutoID-BC-007 (Prepared by Accenture), p. 7.

29. Ross Sealfon, *US RFID-Enabled Handheld Device Forecast and Analysis, 2002-2007: Defining RFID*, Framingham, Mass.: International Data Corp., Doc# 29854, August 2003.

30. Dunlap et. al., op. cit., p. 8.

31. John Wolff, *RFID Tags – An Intelligent Bar Code Replacement*, IBM Global Services: 2001.

32. Jeff Wilson, “RFID Benefits Can Outweigh Higher Cost,” *IT Focus*, September 1, 2002. ITWorld Canada.com. www.itworldcanada.com/index.cfm/ci_id/16255.htm

33. Bill Strautman, “RFID tag retention rate as good as regular tags,” *The Western Producer*, April 7, 2003. www.producer.com/articles/20030403/livestock/20030403ls05.html

34. Cited in: *Ibid*.

35. “Michelin to Embed Electronic ID Tags in Tires,” *Reuters*, January 14, 2003. http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=2045403

36. “Gillette Confirms RFID Purchase,” *RFID Journal*, January 7, 2003. www.rfidjournal.com/article/articleprint/258/-1/1/

37. James Weir, “RFID Tags and IT Services,” *IDC Study*, Framingham, Mass.: International Data Corp., #MS01K, April 2003.

38. “Microsoft to Develop Software for Radio Tags,” *Reuters*, June 10, 2003 http://asia.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=2905169

39. Paul Hoskins, “Retail Future: Painless Checkout, Knowing Scanners,” *Reuters*, May 14, 2003. www.forbes.com/home_europe/newswire/2003/05/14/rtr970418.html

40. “Intellident Selected by Marks & Spencer to Tag 350 Million Items of Clothes,” Intellident, 2003. www.intellident.co.uk/Press/PressReleases/1051624519

41. Winston Chai & Richard Shim, “Japan: Shopping Habits Tracked by RFID,” *CNETAsia*, May 9, 2003. http://asia.cnet.com/newstech/systems/0,39001153,39129324,00.htm

42. Mark Roberti, “What Other Retailers Can Learn From Prada,” *RFID Journal*, July 2002.

43. Junko Yoshida, “Euro Bank Notes to Embed RFID Chips by 2005,” *EE Times*, December 19, 2001 http://www.eetimes.com/story/OEG20011219S0016

44. Janis Mara, “Euro Scheme Makes Money Talk,” *Wired*, July 9, 2003. www.wired.com/news/print/0,1294,59565,00.html

45. Mara, *Ibid.*

46. Electronic Privacy Information Center, “Radio Frequency Identification (RFID) Systems,” Washington, D.C., August 11, 2003, p. 3. www.epic.org/privacy/rfid/

47. See: Boycott Benetton Website at http://boycottbenetton.org and Boycott Gillette Website at: www.boycottgillette.org. Both sites were created by the anti-RFID group Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN).

48. Christopher Boone and Meredith Whalen, “Benetton Unites with RFID: IDC Predicts Low Adoption in Retail Until 2005,” *IDC Flash*, #29131, Framingham, Mass.: International Data Corp., March 2003.

49. Benetton Group, “News Release,” Ponzano, Italy: April 4, 2003; Winston Chai & Richard Shim, “Benetton Takes Stock of Chip Plan,” *CNET News.com*, April 7, 2003 http://news.com.com/2100-1020-995744.html?tag=fd_top; and: Linda Rosencrance, “Update: Benetton Details Decision on ID Clothing Tags,” *ComputerWorld*, April 7, 2003.

50. “Opposition to RFID Tracking Grows,” *RFID Journal*, Jan. 20, 2003. http://www.rfidjournal.com/article/articleview/275/1/1/

51. “Boycott Gillette,” www.boycottgillette.org

52. Alorie Gilbert & Richard Shim, “Wal-Mart Cancels ‘Smart Shelf’ Trial,” *CNET News.com*, July 9, 2003 http://news.com.com/2100-1019_3-1023934.html?tag=fd_lede1_hed

53. See: John Stermer, “Radio Frequency ID: A New Era for Marketers?” ACNielsen, *Consumer Insight*, Winter 2001. http://www.acnielsen.com/pubs/ci/2001/q4/features/radio.htm

54. See: Jane Black, “Playing Tag with Shoppers’ Anonymity,” *Business Week Online*, July 21, 2003. www.businessweek.com/technology/content/jul2003/tc20030721_8408_tc073.htm

55. Rene Laperriere. “The Quebec Model of Data Protection: A Compromise between Laissez-faire and Public Control in a Technological Era.” In: Bennett and Grant. *Visions of Privacy: Policy Choices for the Digital Age*. Toronto: 1999, p. 183.

56. Lawrence Surtees, *Nowhere to Hide: Privacy Implications of Wireless Location Technology*, Toronto: IDC Canada, Bulletin CA025TLH, March 2001; and: Simon Romero. "Locating Devices Gain In Popularity But Raise Concern," *The New York Times*, March 4, 2001, A1.

57. See: Ontario. Information and Privacy Commissioner of Ontario. *Consumer Biometric Applications: A Discussion Paper*, Toronto: September 1999. www.ipc.on.ca

58. Canada. Department of Communications and Department of Justice, *Privacy and Computers*, Ottawa: Information Canada, 1972.

59. Deborah G. Johnson, *Computer Ethics*, Englewood Cliffs, N.J.: Prentice-Hall, 1985, p. 66, cited in: James Moor, "How to Invade and Protect Privacy With Computers," in: Carol Gould, ed., *The Information Web: Ethical and Social Implications of Computer Networking*, San Francisco: Westview Press Inc., 1989, pp. 60-1.

60. http://www.privacyrights.org/ar/RFIDposition.htm

61. See: Junkbusters Corp., "RFID Devices and Privacy," April 8, 2003. www.junkbusters.com/rfid.html

62. Dan Moniz, cited in: Janis Mara, "Euro Scheme Makes Money Talk," *Wired*, July 9, 2003. www.wired.com/news/print/0,1294,59565,00.html. A recent proposal by the U.S. government to require all shelters to collect data on homeless people also raises the haunting spectre of tracking indigents with RFID tags. See: United States. Department of Housing and Urban Development. "Homeless Management Information Systems (HMIS) Data and technical Standards Notice," *Federal Register*, 68:140, Washington, D.C.: July 22, 2003, pp. 43430-43454.

63. The intrusive and unconstitutional TIA project was supervised by convicted Iran-Contra conspirator , retired Vice-Admiral John Poindexter.

64. Cited in: Mark Baard, "Claim: RFID Will Stop Terrorists," *Wired*, Aug. 8, 2003. www.wired.com /news/privacy/0,1848,59624,00.html

65. Clifford Horowitz, cited in: Richard Bray, "Radio ID tags track inventory," *Summit: Canada's Magazine on Public Sector Purchasing*, February 2003, p. 3. www.summitconnects.com/Articles_Columns/PDF_Documents/060108.pdf

66. Clyde Crews Jr., "Put Controls on emerging 'surveillance state,' *The Detroit News*, Losing Liberty: Privacy Series, June 23, 2003.

67. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf, Richard Shim, "Security firm aims to ease RFID concerns," *CNET News.com*, August 28, 2003.

68. http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/

69. Sanjay Sarma, Stephen Weiss and Daniel Engels, “RFID Systems and Security and Privacy Implications,” *MIT Auto-ID Center White Paper*, Cambridge, Mass: Massachusetts Institute of Technology, November 2002. www.autoidcenter.org/publishedresearch/MIT-AUTOID-WH-014.pdf; and see: California. State Senate Subcommittee on New Technologies. Hearing on RFID and Privacy, “Testimony of Kevin Ashton, Executive Director Auto-ID Center,” August 18, 2003.

70. Cited in: Mark Baard, “Radio Tag Debut Set for This Week,” *Wired*, September 15, 2003. www.wired.com/news/print/0,1294,60408,00.html

71. Baard, *Ibid*.

72. Martin Butler, *Opinionwire*, cited in: Andy McCue, “Privacy Fears Over RFID Must Come Before Profit,” *Silicon.com*, August 26, 2003. http://silicon.com/news/500022/1/5730.html

73. Baard, *Ibid*; and: Paul Hoskins, “Retail Future: Painless Checkout, Knowing Scanners,” *Reuters*, May 14, 2003. www.forbes.com/home_europe/newswire/2003/05/14/rtr970418.html

74. Helen Duce, “Public Policy: Understanding Public Opinion,” *Executive Briefing*, Auto-ID European Centre, University of Cambridge, Cambridge, United Kingdom, Auto-ID Center: February 2003. CAM-AUTOID-EB-002, p. 10.

75. Simson Garfinkel, Presentation to International Association of Privacy Professionals, cited in: Jennifer Maselli, “Privacy Group Focuses On RFID,” *RFID Journal*, August 26, 2003.

76. Organisation for Economic Co-operation and Development, *Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data*, Paris: September 1980. Canada adopted the OECD guidelines in 1984. The text is available in: Wayne Madsen, *Handbook of Personal Data Protection*, New York: Stockton Press, 1992, pp. 992-96.

77. See final RFID resolution in Appendix A

78. See: California. State Senate Subcommittee on New Technologies. *Hearing on RFID and Privacy*, “Testimony of Kevin Ashton, Executive Director Auto-ID Center,” August 18, 2003.

79. See: Ontario. Information and Privacy Commissioner of Ontario. *Consumer Biometric Applications: A Discussion Paper*, Toronto: September 1999, pp. 27-32. www.ipc.on.ca

80. *Ibid*., p. 27.

81. http://www.privacyrights.org/ar/RFIDposition.htm,

Note: this paper also provides an excellent analysis of some of the misconceptions regarding RFIDs.

82. Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), "RFID Right to Know Act of 2003," www.nocards.org/rfid/rfidbill.shtml; and: CASPIAN, "Consumer Group Unveils RFID Labeling Legislation," June 11, 2003. www.nocards.org/press/pressrelease06-11-03.shtml

83. Canada. *The Personal Information Protection and Electronic Documents Act* (PIPED Act), Statutes of Canada 2000, Chapter 5. The Act, which initially applies to federally regulated companies such as telephone companies and banks as of Jan. 1, 2001, will apply to all businesses by 2004. PIPEDA will give individuals greater control over their personal information by requiring organizations to obtain consent to collect, use or disclose information about a person.

84. Tools are available to help businesses assess their online privacy policies. Ontario's Information and Privacy Commissioner joined forces with PriceWaterhouseCoopers LLC of Toronto and Guardent Inc., a Waltham, Mass.-based computer security firm, to develop and provide free software to help companies judge how well they manage their customers' personal information by comparing their processes with international privacy principles. Copies and an instruction manual are available at the Ontario Information and Privacy Commissioner's Web site at www.ipc.on.ca

85. Cited in: McCue, *op. cit*.

86. Ontario. Office of the Information and Privacy Commissioner, "Privacy Protection Makes Good Business Sense," Toronto: October 1994. http://www.ipc.on.ca/. See also: Ann Cavoukian & Tyler Hamilton, *Privacy Payoff: How Successful Businesses Build Customer Trust*, Toronto: McGraw-Hill Ryerson, 2002.