

# Chapter 4

## *RFID and Global Privacy Policy*

*Stephanie Perrin*<sup>1</sup>

---

### *Introduction*

This chapter addresses the privacy and data protection issues presented by RFID, largely in view of existing human rights policy and constitutional protection, data protection law, and fair information practices. As described in other chapters, RFID poses privacy problems that are arguably the most fundamental we have encountered in many years. If so few people understand how the telephone signaling system works and so many make uninformed decisions about such issues as caller ID or data retention, how will the public be able to make educated decisions about a sophisticated technology like RFID? In this new world of machine-to-machine (M2M) communications, it is not even clear that the paradigms on which we rest our interpretations of privacy are adequate. This chapter examines some new ways of defining privacy in North America, Europe, and elsewhere.

Privacy and consumer advocates are calling for regulation, codes of best practice, and technological fixes that give them back a measure of control over RFIDs. They are trying to slow down the rollout of these transformative technologies so that the public can get involved in the dialogue. That call for discussion and policy development is not being heeded in a coherent way, and although the Data Commissioners of Europe, through the

---

<sup>1</sup> Stephanie Perrin is a recipient of the Electronic Frontier Foundation Pioneer Award for her role as a global privacy advocate.

Data Protection Working Party, are studying the topic and will likely issue a report in 2005<sup>2</sup>, there is as yet no formal guidance from regulators. This chapter sketches out a few realistic scenarios and looks at what the existing law, policy, and best practice might say about privacy protection. Although the core concepts are similar, the diversity in the detail of the various laws precludes our providing anything more than highlights, and certainly this chapter should be considered a policy discussion, not legal advice.

---

## *Definitions of Privacy*

In a global context, “privacy” is understood in different ways by different individuals, across many cultures and sectors. Each author in this volume may well refer to privacy in a slightly different way. This chapter fleshes out some of the meanings.

Privacy has traditionally been discussed along two vectors:

- As a fundamental human right, including the right to be free from unreasonable search and seizure or intrusion
- As protection of personal information

The principal data protection instruments referred to in this chapter are the European Data Protection Directive 95/46/EC (1995), which sets the mandatory standards for the legislative framework in each European member state; the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) (2000), which does the same thing for Canada and its provinces; and the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980, ), which underpin much of the U.S. privacy law. Various definitions of personal information exist within global legislation and other instruments, and the subtleties of these definitions could make a big difference when applied to RFID.

---

<sup>2</sup> RFID was on the Workplan of the Article 29 Group, a working party of data commissioners that is constituted under the European Directive 95/46. [http://europa.eu.int/comm/internal\\_market/privacy/workinggroup/wp2004/wpdocs04\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2004/wpdocs04_en.htm). . A call for comment on the issue, closing on March 31, 2005, was issued in late winter 2005.

## Definitions of Personal Information

The following are definitions related to personal information:

- **European Directive 95/46/EC: Personal Data**<sup>3</sup>. “Shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity...”; also
- **Processing of Personal Data**. “Shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.”
- **Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)**. “Personal information” is defined as “information about an identifiable individual, but does not include the name, title, or business address or telephone number of an employee of an organization.”
- **OECD Guidelines**. “Personal data” is defined as “any information relating to an identified or identifiable individual (data subject).”
- **Safe Harbor Arrangement: Personal Data**. “Personal data” and “personal information” are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form”.

## History of Current Privacy Paradigm

In the 1970s, fears about loss of privacy focused on large, centrally held databases containing files about named or numbered individuals. People conceptualized the threat in terms of information in a file. As the Web and its

---

<sup>3</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

attendant search engines have developed, we have only slightly modified our thinking about personal information or personally identifiable information and the way it is kept. The concept of personal information being dangerous when held centrally in a “file” is rather quaint, given the power of today’s networks and search engines.

Now there are holes in this conceptual framework. On the one hand, if RFIDs contribute information about individuals to large databases, the link with the individuals is often not specific enough for some of these definitions to be useful. On the other hand, if the feed from an RFID is not considered personal information because it is not linked to a name or an identifying number, it can still be combined with other data to provide personal information. PIPEDA expressly addresses this hole by defining personal information as “information about an identifiable individual” without specifying who identifies that individual, or how. This anticipates a world where data is agglomerated, crumb by crumb, from a host of different data holders, until sufficient attributes are present to re-identify the individual associated with the data-stream..<sup>4</sup>

University of Texas Professor Dr. David Phillips described the problem in his article “Privacy Policy and PETS”<sup>5</sup>. In his introduction to the problem of disambiguating the notion of privacy, he says:

*“We may identify at least four relatively distinct types of privacy concern and label them, for the sake of convenience, ‘freedom from intrusion’, ‘negotiating the public/private divide’, ‘identity management’ and ‘surveillance’. Each way of thinking and talking about privacy will favor particular definitions of, and solutions to, the privacy problem. Obviously, these concerns are interrelated.”*

Comment: DMITRI, this quote is longer than 50 words.

Phillips places the traditional definition of privacy, stated by privacy advocate Dr. Alan Westin, as individuals’ right “to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others” within Identity Management<sup>6</sup>. However, the problem of “surveillance” and its meaning appears to encompass the larger societal privacy threats posed by RFIDs:

*“In its idealized form, panoptic surveillance individualizes each member of the population, and permits the observations and recording of each individual’s activities, then collates these individual observations across the*

Comment: DMITRI, this quote is longer than 50 words.

<sup>4</sup> [www.privcom.gc.ca/legislation/02\\_06\\_01\\_01\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp).

<sup>5</sup> In *New Media and Society*, vol6(6):691-706. London, Thousand Oaks, CA, and New Delhi, 2004.

<sup>6</sup> Phillips, D. 693-695, citing Westin, A, 1967, *Privacy and Freedom*, New York, Atheneum.

*population. From these conglomerated observations, statistical norms are produced relating to any of a multitude of characteristics. These norms are then applied back to the subjected individuals, who are categorized and perhaps acted upon, either with gratification or punishment, according to their relation to the produced norm."*

RFID is a transformative technology because it brings about the potential for constant individual identification and the automatic sorting of individuals, named or otherwise, into groups. "Group privacy" is a newer concept, but one that will be increasingly important in a world of M2M communications. Who goes to Starbucks? RFIDS will make it easy to know, when we all carry tagged loyalty cards..

### *Fear of a Central Database*

Work on the privacy framework in the 1960s was stimulated by a vision popular among IT specialists and government officials—that of a central database of citizen information. In the generation since then, we have averted our eyes from the rampant proliferation of databases such as those held by credit reporting bureaus, banks, insurance companies, major retailers, and information management companies such as Axiom and LexisNexis. The growth of these disparate databases has been well documented in *Database Nation* (cf. Garfinkel, S. (2000) Sebastapol, CA, O'Reilly). In 2005 these databases have grown into what we feared in the 1960s: the specter of an all-knowing, all-seeing, central database. However, it is manifesting not as one database but as many different databases interlinked around the globe. Governments that spent the equivalent of billions of dollars making sure records were not linked through single numbers, like the Social Insurance Number in Canada, are once more looking at ways to facilitate searching between interoperable platforms and linking data reliably to particular individuals—ostensibly in the name of fighting organized crime and terror.

People still react negatively to the loss of control over their own personal information, believing they have a right to present their unique face to the world, in their own terms. This may be in denial of the facts of the twenty-first century, as has been pointed out by various commentators, perhaps most infamously by Scott McNealy, the CEO of Sun Microsystems, when he said, "You have zero privacy anyway, get over it."<sup>7</sup>

Comment: Should this be a complete footnote?

<sup>7</sup> [www.wired.com/news/politics/0,1283,17538,00.html](http://www.wired.com/news/politics/0,1283,17538,00.html).

In previous generations, when bankers dealt with a customer for a loan, they based their decision primarily on personal knowledge of the individual and the forms that the individuals filled out. Today neither the human being requesting the loan nor the bank manager has much influence on the decision. Databases, predictive software programs, and inexpensive telecommunications have facilitated a world where decisions are made remotely by machines fed an ever-increasing stream of data, with little human intervention. Everyone banks, but very few know about the companies that manage their financial transactional data, and the relationship between those data processors and the state.

From a policy perspective, it is not clear that society and democracies have yet adjusted to this current scenario. People do not fully understand how the information infrastructure works, and the high levels of concern for privacy that we see in virtually all the polling data<sup>8</sup> demonstrate strongly contradictory behavior. While few people are actively protecting their privacy, the level of concern is rising every year, leading to a profoundly unstable situation such that a scandal in the press could precipitate sudden change in consumer behavior. . In fact, this scandal hit in February 2005 when it became publicly know that Choicepoint, one of the largest and most successful data brokers in the world, with 64 billion files, sold personal information to a criminal ring of ID thieves posing as small businesses. This scandal has prompted calls for legislation, Congressional hearings, complaints to the Federal Trade Commission, private actions and investigations from State Attorneys General<sup>9</sup>.

Now RFID bring to us an “Internet of things,” on which objects talk about their owners or handlers, thus feeding powerful new databases. Industry proponents protest that the chips are not big enough to be intelligent, but the chips’ “chatter,” even if it is only in monosyllables, brings to a new level a world in which humans hold increasingly less power and information holds increasingly more. In discussions about “trust” and “security”, the emphasis is on building trusted systems. But does this mean we no longer trust humans?

---

<sup>8</sup> For a view of the evolution of privacy concern, see Alan Westin’s work in association with Harris Interactive, as described on the Privacy and American Business Web site, [www.pandab.org](http://www.pandab.org). Although the surveys are proprietary, Dr. Westin has written about them since the early 1990s, and he said of the recent survey results described at the Privacy and American Business conference in Washington in June 2004, and at the Ottawa University conference “The Concealed I” March 4, 2005 that concerns continue to rise and self-professed privacy fundamentalists now stand at 37% of the US population.

<sup>9</sup> The latest news on the Choicepoint scandals can be found at the Electronic Privacy Information Center’s Choicepoint page [www.epic.org](http://www.epic.org). Robert O’Harrow Jr.’s book “*No Place to Hide*” appeared in January 2005, and contains useful updates on the database industry in the post-911 environment. (Free Press, New York)

---

## *Mapping the RFID Discovery Process*

Consider the following “real-life” RFID applications:

- Alice has an employee badge, which contains her employee ID number and a set of building access privileges.
- Bob, a patient, has an implant containing data on his health conditions, medication, and identity.
- Carol’s dog Rover has a pet-tracking tag, which gives Carol’s name, address, and phone number or a number that is matched in a database to that same personal information.
- Dora’s leather jacket has a manufacturer’s tag, which contains a unique product number that is linked to the date of purchase.
- Ed buys a packet of razor blades, whose tag has product, price, and retail destination information on it.
- Fred works with a shipping container that is used and reused to transport frozen dinners. The container’s tag is identified with the manufacturing plant ID, store destination, contents, and date the container is filled.

The first three applications contain explicitly personal information. Every time these tags are read, personal information is emitted. The reader’s ability to detect the presence of a tag is an indicator that an identifiable individual is at that geographical location at a precise moment.

Carol’s dog’s tag is a good example of personal tracking by proxy. If Carol is the only one who walks Rover, readers that track the dog tag will have a reliable record of her movements. Assuming Rover is not in the habit of rambling around on his own, his information becomes tracked one-to-one with Carol’s, regardless of what personal information or numbering is contained in the tag.

In Dora’s case, the tag in her jacket will, over time, become associated with Dora, the individual who wears it. If she is wearing the jacket as she walks past a reader every morning to enter a building, she will soon build up a profile of pseudonymous information, with the pseudonym being the unique identifier of the jacket. Identify Dora

once, and the entire record of comings and goings becomes transparent. Associate the RFID with an image from a video camera, and the jacket and Dora become reliably linked with a visual image. These facts contradict the argument that RFID will be anonymous. If she buys a coffee each morning, readers in the coffee shop will know her by her jacket.tag.

Unless we make a point of regularly trading our clothes, wallets, and favorite possessions with others in order to foil the system, RFID-tagged personal possessions will soon be reliable authenticators of identity because of their close association with unique individuals.

Ed's RFID-enabled package of razor blades has become the subject of numerous press stories. The activist group Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)<sup>10</sup> found that a manufacturer was using hidden cameras activated by the RFID chips as merchandise left the shelf. The experiment was discovered in both in Britain, where a store filmed customers to deter shoplifting, and in the United States, where a chip was being used as a prototype for inventory tracking.

Fred's reusable container is the often-cited example of an almost totally innocuous use of RFID that will save a lot of time and money in inventory control and shipping, with few implications for personal privacy. However if the crate is read in context with other chipped devices (e.g., Fred's employee card, the truck that he is assigned to drive on this shift, individually tagged articles and tools such as a trolley he is assigned for work), the threat of employee surveillance is very real.

Such crates might be candidates for high-end, rewriteable chips, and if they could register every time they were touched by specific employees, as part of an apparently innocuous time-tracking control system (useful for controlling melting and warming, in the case of frozen and refrigerated food handling), there are implications for the humans involved. For example, tool inventory control is a major cost for many service industries, so tools that remember where they have been and what they did there may become hot sellers. The value of tool tracking may be considered to be higher than the dignity of the workmen who use them,

To date, the public discussion on privacy issues has not focused on employee surveillance and tracking. But particularly in Europe, where unions are stronger than in the United States, it promises to be an issue.

## Functions and Responsibilities for Chips, Readers, and Owners

In the ontology of data protection law and policy, the RFID itself may be a storage device containing an individual's personal information (e.g., a shopper card number, employee number, or the identity of a dog's owner). It also can be a personal information-emitting device if, when illuminated by a transmitter receiver, it broadcasts such information. Depending on the uniqueness of its own number or product code, it may also become a numeric identifier reliably associated with a human being, not just an item of merchandise; the number of a breast implant, for instance, or a pacemaker, soon might be more reliable as a numeric identifier of an individual than the current U.S. Social Security number.

An RFID reader is simultaneously a data-collection instrument, promiscuously gathering information from each RFID that responds to its broadcast, and a transmitter or broadcaster of information, as it sends its data through the information network. The databases connected to these networks hold, use, and disclose the gathered information. Here the information may be used for wholly different purposes than those envisaged by the party that installed the RFID device and these new uses are likely not apparent to the carrier of the device. We cover these aspects later in the chapter as we discuss the application of data protection law.

---

### *Privacy as a Fundamental Human Right*

To date, public discussion of privacy and RFID has been at a superficial level, focusing on the effective range of readers and the ability to disable the tags. This limited scope mirrors the discussion of privacy in North America, which has been similarly focused on opt-in versus opt-out and "notice and choice." This discussion not only understates the subtleties of data protection, it also misses more fundamental issues about individual rights.

The annual report "Privacy and Human Rights," published by the Electronic Privacy Information Center<sup>11</sup> in cooperation with Privacy International<sup>12</sup>, details the constitutional privacy and data protection statutes of over 80

---

<sup>10</sup> See [www.spychips.com](http://www.spychips.com).

<sup>11</sup> The PHR report for 2004 is available online at [www.epic.org](http://www.epic.org).

countries. Although countries approach privacy differently, the United Nations' Universal Declaration of Human Rights enunciates the fundamental right to privacy in the following sections<sup>13</sup>:

*PREAMBLE*

*"Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world..."*

Does the right to dignity stated in the Preamble include the right not to have your possessions, wallet, vehicle, or your person equipped with a device that can be read without your knowledge or consent?

*Article 12.*

*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

What is "arbitrary interference"? Can one make the argument that intelligent devices interfere with this right to enjoy home, family, and correspondence in peace? When our currency, computer technology, clothes, and appliances all sport communicating devices that tag and track us, does it seem plausible that this article has been violated? What law would protect us from interference and from attacks based on faulty data from our possessions and devices?

*Article 13.*

*"Everyone has the right to freedom of movement and residence within the borders of each state."*

Does freedom of movement mean anonymous movement and assembly, free from tracking devices? Does it imply the right to travel on trains or subways without having to use RFID-enabled tickets or passes that respond to every reader they encounter on the trip? Does it mean that public spaces cannot be wired with readers to track and analyze us?

*Article 17.*

---

<sup>12</sup> [www.privacyinternational.org](http://www.privacyinternational.org).

<sup>13</sup> [www.un.org/Overview/rights.html](http://www.un.org/Overview/rights.html).

*“(1) Everyone has the right to own property alone as well as in association with others.*

*(2) No one shall be arbitrarily deprived of his property.”*

What does the right to own property imply? Until recently, it was nearly impossible for those selling goods to put strings on them, to have the goods report back whether in fact they were being used according to warranty requirements, to determine whether lending or copying policies were being respected, or to have the goods identify themselves to facilitate recall. These “strings” are potentially feasible with RFID, and the liability and theft issues will reduce the possibility that these features will be turned off. How many consumers are willing to forego warranty protections to have a little privacy?

In recent years, we have seen the ownership of computer software change in subtle ways to the point that we now really only license the software for a few years. We are in such dynamic contact with the licensor for security and technical updates that the software may be useless after the license expires. Could the same transformation of ownership be rolled out for other types of goods? We can envisage such Faustian bargains being offered in the near future; certainly the health industry is already interested in RFID-enabling prescription drugs to ensure expiry date accuracy, track repeats, facilitate recall, limit liability, and address a host of other public policy issues such as prescription drug abuse. If the only way a patient can be sure her anti-depressants are the real thing and not cheap counterfeits is to accept them in a smart, sealed, authenticated container, she will have bargained away her health privacy to be read by whoever scans her purse.

*Article 18.*

*“Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.”*

Article 18 provides the right to practice freedom of religion worldwide. In Canada, religious freedom is protected by the Charter of Rights and Freedoms, and recent cases before the Canadian Supreme Court suggest that recourse to the Charter over RFID use may be successful<sup>14</sup>. In the United States, the Constitution provides

---

<sup>14</sup> A recent case claiming the right to put up ceremonial huts on the balconies of apartment buildings was successful (see *Syndicat Northcrest v. Amselem*, [www.lexum.umontreal.ca/csc-scc/en/rec/html/2004scc047.wpd.html](http://www.lexum.umontreal.ca/csc-scc/en/rec/html/2004scc047.wpd.html)); a case is pending concerning the Sikh practice

such protection, and it not be long before a case arises involving RFID—many Christian sects have already identified RFID as the “mark of the beast” identified in the Book of Revelation. Whether or not a suit would be successful, it certainly must be heard; developers of the bar code even inserted the number 666 into the standard, so the argument has been made easy for believers in this particular chapter of the Christian Bible. The point that religious groups are raising is lost on many in the technology community: human beings have a right to live their lives without intermediation by material things, because in many religions the material world is construed as a barrier between man and the spiritual world. People with this viewpoint do not want talking possessions, regardless of how convenient these are to retailers.

The U.N. Declaration is high level and over 50 years old. Nevertheless, the sooner RFID proponents recognize that individual autonomy, freedom of movement, human dignity, and religious expression are all threatened by widespread deployment of this otherwise extremely useful technology, the sooner we will have a fruitful discussion. In North America, we have spent the past 15 years painstakingly removing asbestos and urea-formaldehyde insulation materials from buildings after the risks to humans were discovered. We don't want to be spending the next 20 removing RFID from the communications architecture we are busy building today after people decide they want their material possessions to remain mute and unable to participate in controlling their lives.

## Constitutional Rights

The member states of the European Union have for some time been required to respect the European Convention on Human Rights (ECHR) or face being taken to the European Court of Human Rights. Each country that has ratified the Convention has also put in place its own legislation, which in many cases is stronger and more specific than the Convention's.

A recently enacted law in the United Kingdom provides that all U.K. legislation must respect the ECHR. Some of the new member states of the European Union, such as Poland and Latvia, have new constitutions that go fur-

---

of carrying ceremonial daggers, even in public schools (see <http://www.canlii.org/qc/jug/qccs/2002/2002qccs12551.html>); Currently the Ontario Superior Court is hearing a case concerning the right to refuse to provide a picture in the motor vehicle license database. These cases illustrate the success of religious freedom cases under the Charter—the last involving a Christian who cites arguments based on the book of Revelations.

ther because they were drafted in the light of recent experience in which human rights were not respected. The Polish constitution<sup>15</sup> is a good example and would no doubt provide grounds for a challenge of compulsory RFID in matters that fall under its domain. Poland is also an interesting example of the specific issues that arise in cultural context because of the emphasis on labor and union rights, a legacy of the important role the labor movement played in bringing down the Communist regime.

Most discussion of RFID privacy issues in the EU directive has concerned consumers, but employees will in fact be subject to surveillance and tracking through RFID badges and ubiquitous readers as well as throughput tracking reported by the goods themselves. In Europe, works councils have been successful in disabling such surveillance mechanisms in earlier incarnations of the technology, and Courts have supported the privacy rights of workers.

The passage in December 2000 of the Charter of Fundamental Rights of the European Union<sup>16</sup> restates in law the basic concepts found in the Convention on Human Rights in the sections on "Dignity" and "Freedom." The EU also included the right to legislated data protection with oversight by an independent authority as an element in the Treaty Establishing a Constitution for Europe<sup>17</sup>.

But given all the analysis in our possession now, can we predict what data protection law would say about RFIDs?

---

### *Privacy Through Data Protection Law and Fair Information Practices*

It is hard to imagine how the right to privacy can be respected if there are no detailed rules for managing personal information. Nevertheless, privacy activists often argue that data protection law actually helps debase the fundamental human right to privacy: If we follow a mere set of rules about how data will be managed once it is collected, will we forget that not collecting data in the first place should be our goal? If personal data is never

---

<sup>15</sup> See [www.oefre.unibe.ch/law/icl/pl00000\\_.html](http://www.oefre.unibe.ch/law/icl/pl00000_.html) for an English version of the Constitution of Poland.

<sup>16</sup> [www.europarl.eu.int/charter/default\\_en.htm](http://www.europarl.eu.int/charter/default_en.htm).

gathered, it is irrelevant how well confidentiality is managed, who may access it under what circumstances, or under what circumstances an individual might legitimately be denied access to his or her own personal information. Increasingly, European privacy experts are calling for collection limitation or data scarcity—the “forgotten principle”—to be more respected, because the task of auditing and supervising the management of vast collections of data is immense..

However, the fair information practices (FIPS) on which most data protection law is based are generally recognized as just that—fair—and the privacy and civil liberties communities have been calling for RFID to be deployed only if FIPS are followed.

**Comment:** This is a good spot to link to the declaration which I believe is included in the book

## A Brief History of FIPS

The 1973 Report of the U.S. Health, Education and Welfare Department described the worrisome findings of an extensive review of data processing. The authors recommended that a Code of Fair Information Practices be established:

*“The Code of Fair Information Practices is based on five principles:*

1. *There must be no personal-data record-keeping systems whose very existence is a secret.*
2. *There must be a way for a person to find out what information about the person is in a record and how it is used.*
3. *There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person’s consent.*
4. *There must be a way for a person to correct or amend a record of identifiable information about the person.*
5. *Any organization creating, maintaining, using, or disseminating records of identifiable per-*

---

<sup>17</sup> Official Journal of the European Community 169, 18. 7.2003, p.1.

*sonal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.*<sup>18</sup>

In 1980, the Organization for Economic Cooperation and Development (OECD) in Paris released its “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,”<sup>19</sup> which set the standard for FIPS for the next 20 years. Reaffirmed as appropriate for protecting privacy in the context of Electronic Commerce at a Ministerial Conference on Electronic Commerce in 1998, these FIPS have become the basis of many data protection laws. In Canada, they were the foundation of a national standard for the protection of personal information (CAN/CSA Q-830), which was developed by the Canadian Standards Association and became a national standard in 1996. The recent Personal Information Protection and Electronic Documents Act of Canada (2000)<sup>20</sup> incorporates that standard as the set of FIPS that must be met.

The Act’s ten principles are:

- Accountability
- Identifying purposes
- Consent
- Collection limitation
- Limiting use, disclosure, and retention
- Accuracy
- Safeguards
- Openness
- Individual access

---

<sup>18</sup> See U.S. Department of Health, Education and Welfare, Secretary’s Advisory Committee on Automated Personal Data Systems. *Records, Computers, and Rights of Citizens* viii (1973)

<sup>19</sup> [www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM](http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM).

<sup>20</sup> Statutes of Canada, C 5, <http://laws.justice.gc.ca/en/P-8.6/>.

- Challenging Compliance

Accepted as adequate data protection by the European Union for the purposes of onward transmission of EU personal data, the standard has had a significant impact on the work on Privacy Guidelines of the Asia Pacific Economic Cooperation (APEC) group.

There are of course corresponding provisions in the EU Data Protection Directive, but the document is organized differently. The Directive also differentiates certain types of data whose processing is prohibited (“sensitive” data), which includes “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life” (article 8 (1)).

The following analysis of the rights under data protection law follows the structure of the ten principles of the Canadian Standard CAN/CSA Q-830, now required by law in PIPEDA<sup>21</sup>, and adds relevant requirements from the *EU Data Protection Directive 95/46*.<sup>22</sup>

## Accountability

The concept of accountability is a constant in data protection law. Someone is responsible, perhaps liable, for ensuring data protection, and that person must be made available to requestors and complainants. In the European context, this person is called the “data controller”. The accountable person, under the Canadian law, has a number of duties, including:

- Maintaining responsibility for information that has been transferred to third parties for processing, which must be protected through contractual means
- Implementing policies and procedures to give effect to all the principles, including training staff and developing information to explain the policies and procedures to the public

---

<sup>21</sup> Statutes of Canada, <http://laws.justice.gc.ca/en/P-8.6/>.

<sup>22</sup> Many other relevant statutes could and should be included, particularly in the area of medical and financial privacy where confidentiality clauses may have a decisive impact on using RFID to contain personal information, but this narrative is complex enough.

But this form of accountability is complicated when applied to RFID. When does an individual or organization cease to be accountable for the RFID—either the information contained within it or the stream of location data that it generates?

A recent Federal Court of Appeal decision in Canada<sup>23</sup> confirmed that the Court does view an organization as having a primary responsibility to inform individuals about the implications of a decision to accept a particular information bargain—for example, the decision to allow their name, address, and phone number to appear in the phone book and in all subsequent uses of that information resulting from that public disclosure.

### **Responsibility in Individual RFID Scenarios**

Under current and theoretical RFID policy, who is ultimately responsible for the data in Alice's employee badge, Bob's medical implant, Dora's leather jacket, and Ed's razor blades?

Alice's employee badge will in all likelihood remain the property of the organization she works for, not of Alice the employee, so that organization will be responsible for the information on it as well as any information it broadcasts to a reader. If the technology interoperates with every reader Alice happens to pass, would she have a valid complaint that the company was not protecting her personal information? Could the company transfer the responsibility for the card and the information on it to Alice, making it her responsibility to prevent the card from accidentally disclosing its information to a reader?

Because this form of RFID technology is passive, requiring little or no action on the part of the holder of the chip, this is a fundamental question. It is one thing for the employee to be responsible for a card that needs to be put into a slot to be read or up against a reader for a proximity contactless smart card. If the device can be read even if the employee takes no action, can the accountability be passed along to the employee? Only if the employee gets a foil-lined wallet to go with the card, I would say.

Bob's patient implant is even more problematic because the information is more likely to be sensitive, he cannot remove it or wrap it in foil, and in all likelihood, the accountable organization is a healthcare provider, hospital, or device manufacturer (such as a heart pacemaker) with which he will not have an ongoing relationship.

The device may be meant to be read by a broad spectrum of future players in his healthcare relationships, so the chip is likely to interoperate with any reader in range. How can we maintain accountability here? Is Bob responsible? Suppose he is too ill to know what is going on? If the data is read by alien machines against his will and harm is done, who is liable—the chip manufacturer or the reader of the machine?

This brings us to the question of the readers. Arguably, the organization that puts the information into the RFID has already done so, presumably with the consent of the individual. From then on, the individual who has custody of the device might be considered responsible. The custodian of the RFID information (although not the lookup database) is now the individual, in the case of all the examples we listed above. (We won't complicate matters by mentioning appliances, cars and car parts, and building materials that could be associated with individuals but are durable goods that are not intrinsically personal.)

If the individual comes in range of a reader, is the operator of the network to which it is attached accountable for the information it collects? Clearly, it is, at least according to the Canadian law. It will be the responsibility of the organization, and the persons accountable within that organization, to ensure compliance with the Canadian law, or all of the FIPS. A reader must collect only the data that it is supposed to collect and that it is authorized by law, policy, or a contractual arrangement to collect.

Proponents of RFID deployment tout benign scenarios such as chips on packages and a self-checkout that scans them. What happens if the persistent RFID in Dora's leather jacket (which she has not disabled because she wants to keep the warranty) is read every time she checks out her groceries or goes through the ATM door? Who is responsible or accountable for the information gathered? The creator of the RFID, Dora, or the organization responsible for the reader?

The discussion of using kill switches and permitting opt in/opt out does not focus on this fundamental problem. If you do not opt out, are you committed to transmitting whatever information could be transmitted, to every reader that is capable of reading it? Today's Internet web browsers follow this principle: Accept cookies once, and expect them to be read by anyone who can read them. Once you agree to have your customer information shared with other "quality companies for marketing," that information is out the barn door.

---

<sup>23</sup> Englander v. Telus, see <http://decisions.fca-caf.gc.ca/fca/2004/2004fca387.shtml>.

Under Canadian and European law, including the European Direct Marketing Directive, future users will need some kind of evidence of valid consent, but that consent may be looped if the wording is broad enough. It is doubtful this permissive approach will work for RFID, particularly where sensitive information is concerned.

As for the question of accountability, the data controller or original programmer of the RFID must ensure that the device with personal information in it is labeled with the identity of the organization that is responsible for it. The reader must be identifiable so that individuals can access their data or complain if they find their data being read without their consent.

### Identifying Purposes

*The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.*<sup>24</sup>

**Comment:** Please cite the source of this quote.

This section goes on to stipulate that the individual must be able to find out the purposes, and when new purposes are identified after collection, the organization must gain new consent. The idea that purposes for collection, use, and disclosure must be specified to the individual before the information is gathered is a constant in data protection law. In some law, it is part of informed consent; in others, as in the OECD Guidelines and PIPEDA, it is a separate principle. In the Canadian law, section 5(3) states further, "An organization may collect, use, and disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." This is likely to spark complaints, especially when readers unrelated to the original purpose of the RFID tag are gathering information for new, unanticipated purposes. If Dora's jacket were used as a link to her identity in cash sales at a department store or if Carol's dog's ID were to be used as a proxy to identify her at a weekend rock concert, there is a good chance a court would view reliance on these linkages as opportunistic and the purpose of gathering such data for unstated purposes as something a reasonable person would not find appropriate.

---

<sup>24</sup> PIPEDA

## Consent

*The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.*<sup>25</sup>

**Comment:** Please cite the source of this quote.

Unambiguous consent is required for the legitimate processing of data under Article 7 of the Directive, unless there is a clear contract, the processing is necessary for compliance with a legal obligation, the processing is undertaken in the public interest, or the processing is necessary for the legitimate interests of the controller. Under Canadian law, consent is required for the separate actions of collection, use, and disclosure of personal information with specific exceptions under each of these actions as required for law enforcement, fraud investigation, and other legitimate reasons. These two legal regimes take different routes to permit some routine use and disclosure of personal information without the express consent of the individual. If it were not the case, business would come to a halt with the never-ending process of seeking consent.

In the context of the Internet, P3P was an attempt to automate decision making with respect to cookies, enabling an individual's Internet browser to automatically negotiate with Web sites the circumstances under which the individual would agree to accept cookies and thus potentially be tracked and identified. It was not entirely successful, although individuals set the preferences themselves and could intervene since they were operating the browser. How do we negotiate consent in the RFID scenarios, where communication may be taking place without the person's knowledge?

Alice is not in a position to give meaningful consent to the performance of her ID card. She has to carry it with her to get into work, so if it interoperates with other readers, she has no control over it.

Bob may not have a choice about whether to receive a chip either, if having one is required to check into a hospital or have his medical devices covered by his insurer. Carol may be required to put a chip in her dog's ear to comply with local bylaws. The only way for these applications to comply with the law is for the devices not to contain personal information themselves. Furthermore, there must be a way to destroy the consistent pseudonymity in order to avoid the proxy problem.

<sup>25</sup> PIPEDA; inappropriate uses are specified in section 7.

## Limiting Collection

*The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.<sup>26</sup>*

Comment: Please cite the source of this quote.

We have discussed the central problem of stopping RFID from communicating. This provision is clear, it is mandatory, and legitimate collection is dependent on having a reasonable purpose. Mechanisms to limit collection would include screening out transmissions from non-targeted chips, dumping data immediately if it is not necessary to keep it, and removing identifiers to render data nonpersonal.

The problem of group surveillance that David Phillips has described will be one of the big new issues in RFID deployment scenarios. Dr. Latanya Sweeney of Carnegie Mellon demonstrated years ago how simple it is to re-identify supposedly anonymized health records<sup>27</sup>; and her work and techniques will certainly be relied on to find out what we can learn from RFID reporting.

## Limiting Use, Disclosure, and Retention

*Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.<sup>28</sup>*

Comment: Please cite the source of this quote.

Canadian law further specifies that procedures must be developed to govern the permissible retention of information and its safe destruction and disposal. If the accountability were passed to the individual carrying the RFID, the problem of data retention would no longer belong to the issuing organization. Similarly, if somehow the responsibility for preventing transmission from the RFID could be passed to the owner, the problem of ongoing disclosure carrying on forever could theoretically be passed to the owner.

<sup>26</sup> PIPEDA

<sup>27</sup> [www.ncc.org.uk/technology/index.htm](http://www.ncc.org.uk/technology/index.htm).

<sup>28</sup> PIPEDA

Data protection law puts the emphasis on the responsibilities of the collector, however, so it seems unlikely that readers in an RFID architecture will be allowed to gather data indiscriminately and keep it indefinitely, regardless of whether the individuals concerned are consciously exercising their rights. There will have to be a way to purge irrelevant data from systems promptly.

## Accuracy

*Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.<sup>29</sup>*

**Comment:** Please cite the source of this quote.

This determination is based on the needs of the individual and the original purpose of the data capture. Writing new information to a tag that serves the purposes of the organization but not necessarily the individual would not be acceptable, even if it could be argued it was more accurate. The Directive says something slightly different in the Data Quality section:

*(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.*

Whether a tag can be hacked and the data can be altered will be of major concern for retailers and those attempting to deter theft, maintain good inventory control, and provide reliable information in areas such as medical procedures. Alice's employee badge might have limited attraction for bad actors, unless she works in a nuclear facility. Bob's patient tag will have to be extremely reliable if medical staff uses to gather information about allergies and medical emergency conditions, for example. The issues in terms of data protection will arise when individuals contest the accuracy of the information on the chip, or their registration on a reader that they claim not to have experienced.

## Safeguards

*Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.<sup>30</sup>*

**Comment:** Please cite the source of this quote.

The Directive provides detail about the security of processing in Article 17, including a requirement to ensure that processing by another party is bound by contract and that the processor acts only on instructions from the controller. Both instruments refer to “having regard to the state of the art”, and the Directive goes further to state that the requirements for third-party processors must be in writing.

**Comment:** Both what? What does “having regard to the state of the art” mean?

In our scenarios, the importance of determining who is accountable is relevant. If an organization retains responsibility for the chip in an item (or a person), it is obliged to put in writing the safeguards required for processing under either the Directive or the Canadian law. There may be further requirements to anonymize data under either the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the German legislation, in cases of medical data. The limits in the potential for such anonymization in situations of persistent pseudonymity are very real, arguing for the use of technologies other than RFID that are capable of hiding identity yet providing secure assurance of statements, such as contactless smart cards containing digital credentials<sup>31</sup> or digitally signed assertions.

Even without requirements for anonymization, there is a requirement to encrypt data and protect it from casual interception. The only way for an organization to escape such obligations is to transfer custody of the RFID data to the individual, a bargain consumers would be unwise to accept.

### Openness

*An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.*<sup>32</sup>

**Comment:** Should this sentence be a quote?

The Canadian law goes on to provide specific information that must be made available, such as the coordinates of the accountable officer; ways to get access to information; a description of data held and an account of use; information that explains policies, standards or codes; and the personal information that is made available to related organizations or subsidiaries. Similar provisions exist in the Directive, in section IV, *Information to Be*

<sup>29</sup> PIPEDA

<sup>30</sup> PIPEDA

<sup>31</sup> Pioneered by Dr. David Chaum over 20 years ago, use of blind signatures is an innovation in public key cryptographic technology that promises to provide anonymity for individuals. See “Security without Identification Card Computers to make Big Brother Obsolete.” [www.chaum.com/articles/Security\\_Without\\_Identification.htm](http://www.chaum.com/articles/Security_Without_Identification.htm).

<sup>32</sup> PIPEDA

*Given to the Data Subject* and *IX Notification*. Data subject rights are nearly identical to the Canadian standard, but the requirements in *Notification* go further and detail requirements to notify the supervisory authority of certain types of processing.

Article 18 states that the controller must notify an individual before carrying out “any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.” Certain exemptions apply, but if a Data Commissioner were to insist on prior notification of RFID systems, it seems logical it could be done. It will be important to see how the Article 29 Working Group decides on this issue.

Article 19 clarifies the information that must be provided, including on proposed transfers to third countries. Article 20 stipulates that certain operations are subject to prior checking with the data protection authorities and that member states will decide which operations present specific risks and therefore require prior checking. In North America and certain Asia-Pacific countries, this act of prior checking is usually encompassed in the process of Privacy Impact Assessment (PIA). This is becoming an integral part of business process in many jurisdictions and is now increasingly mandatory. Governments are requiring PIA reports and risk analyses before granting IT funding<sup>33</sup>.

### *Individual Access*

*Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.*<sup>34</sup>

**Comment:** Should these sentences be a quote?

Article 12 of the Directive provides equivalent rights, including the right to have “knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15.” Another important right is the right not just to change incorrect data but to communicate changes to third parties who may have received incomplete or inaccurate data; this right appears in most data

<sup>33</sup> Further information including policy, e-learning tools, and detailed templates can be found online at [www.tbs-sct.gc.ca/pubs\\_pol/ciopubs/pia-pefr/paip-pefr\\_e.asp](http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp) A good model of how regulatory compliance can be rolled out is at the U.S. Census Bureau Web site, at [www.census.gov/po/pia/](http://www.census.gov/po/pia/); in this case, it is the response to the E- Government Act of 2002. Such a process could be applied to RFID deployment and expedite the required notification under data protection laws.

<sup>34</sup> PIPEDA

protection law and is a significant problem in implementation where there are distributed data systems and accountability may be in question, as is the case with RFID deployments.

It is safe to say that individual access is one of the topics in data protection policy and law that has been studied the least. The volume of requests varies enormously from jurisdiction to jurisdiction. Companies do not tend to publish the statistics of use, and they may blend formal access requests with customer service statistics. Data commissioners usually conduct inquiries in confidence, so while there may be global statistics on information requests, we do not have good country-by-country statistics on who is asking for their information, what they are getting, and what the cost of compliance is.

We do know that campaigns to access personal data have been launched in response to specific media events and privacy stories in the press, and if this happened with RFID deployment, it would be difficult to gather the data in some cases. Returning to the scenarios, if Alice wanted to ask for all the data associated with her employee card, she could do the following:

- Request a printout, explained in plain English, of what is on her card
- Request all records of her ingress and egress at building and site facilities, including parking if it were on the same card, and cafeteria access and billing
- Request all records of the sharing of her data with third parties
- Request procedural and technical documentation that would allow her to understand which readers in the wider population might be capable of reading all or parts of her card and send requests to those parties

Bob or his caregiver with power of attorney could do the same with the implanted chip, and this would be a likely scenario if any medical foul-ups caused harm to Bob. If Dora suspected that her jacket was being used to associate her with certain locations, stores, or product choices, she could first obtain a readout of the tag from the store that sold her the coat and then request all records relating to that identifier and/or her name and credit card information held by any parties she suspects might have records about her.

We have said very little about Ed and the razor blades thus far, but consumer complaints about how the system works in high-volume scenarios such as grocery checkout must be considered as a basic cost. It will not be

enough to provide readers in the store or shopping baskets that show the price of goods, Consumers will want to see the records of their purchases, know with whom the information is shared and how long it is kept, and examine their store profile. Because the volume of consumer requests is erratic and highly dependent on trends such as media reports and scandals, this cost is hard to predict.

## Challenging Compliance

*An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.*<sup>35</sup>

Comment: Should this sentence be a quote?

All data protection laws that mandate independent supervisory authorities provide a variant of this right. The Canadian PIPEDA is broader than most in that anyone can complain, regardless of whether their information is the subject of the complaint, so consumer groups and technical experts could file complaints under Canadian law and even take a case for damages to the Federal Court. In Europe, the actual provisions of each law differ slightly, so it is likely that a pan-European campaign of complaints organized by consumer groups would have slightly different results in each jurisdiction. Data protection authorities in Europe have the power to stop a practice and block data flows, although this power has been little used. Given that the Directive will soon be up for review again, it is likely that there will be some consumer investigation of whether the Data Protection Authorities are fulfilling their mandates.

Many organizations in the United States are working on RFID issues, but it is important to note that they are networking with global consumer organizations. The National Consumer Council of the United Kingdom, for instance, has held a colloquium on RFID (see *Calling in the Chips* at [www.ncc.org.uk/technology/index.htm](http://www.ncc.org.uk/technology/index.htm)) and will be publishing a book entitled *The Glass Consumer* in early 2005. Because the council is working with Consumers International, a global network of grassroots consumer organizations, this project will have impact on consumer awareness of the issues.

---

<sup>35</sup> PIPEDA

---

## Conclusions

It is impossible to predict future actions of the stakeholders in the data protection community—namely the data protection authorities, the individuals who exercise their rights, and governments that respond to issues with regulations and standards development activities. The preceding analysis gives some indication of potential arguments and interpretations that could be made. Perhaps the most useful way of summarizing the potential for developments is to return to the scenarios once again and sketch out some high-risk complaints that could precipitate action.

If Alice is a member of a union, it is very likely that there will be action to find out how employee cards are being used to track and monitor employees. Large companies very often negotiate privileges for their employees, from health benefits packages to discounts on goods and services and transportation. It will be tempting to use the same card to authorize such activities, potentially yielding a rich stream of linked personal information.

Bob and the patient chip will be the topic of malpractice suits, religious human rights arguments, and in jurisdictions where there is funded healthcare, debates about national identity or health cards. Since most jurisdictions recognize that the health sector is significantly behind in the use of IT to cut costs and streamline services, this is a longer-range threat, but one that is bound to command public attention.

Pet tagging devices are already deployed, and many humane societies are calling for mandatory tagging to facilitate locating owners of lost pets. The mad cow disease problem has prompted mandatory tagging in farm animals. Study of this phenomenon, little discussed in mainstream media, should give us clues as to how the patient chip could be used.

Clothing tagging was one of CASPIAN's first targets, and it resonates with the public. A stalking scenario involving a child would put this on the public radar; imagine that a 14-year-old athlete is tracked entering and leaving a pool and a stalker abuses access to the data stream and follows her. Of course, the same thing could happen with a video surveillance feed and facial recognition systems, but RFID, being less visible and harder to conceptualize, may frighten the population more. This will be the case if bad actors start to travel about with portable readers.

Item-level tagging is clearly the major target of consumer activists at the moment, from the standpoint of accuracy, usability, profiling, discrimination, and invasion of privacy.

The reusable container is a sleeper in the debate thus far, partly because it appears unions have not woken up to the issue and deployments have not focused on persistent goods such as tool inventories. True M2M communications is a threat to workers from the perspective of job quality, surveillance, and dignity. It is likely to surface in response to the significant job cuts that most manufacturers and retailers hope to achieve through RFID deployment.

Stay tuned. This privacy debate has only just begun.