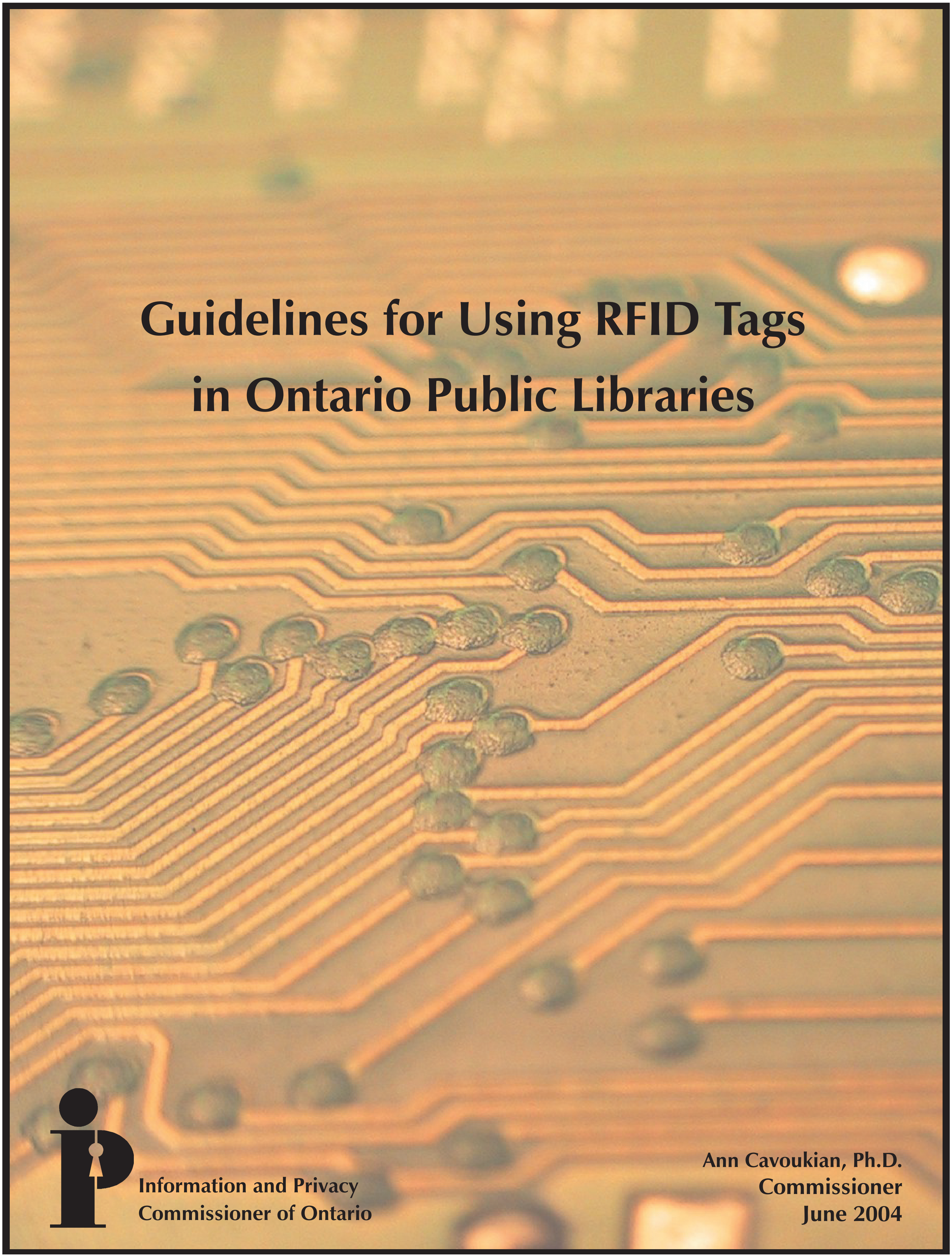

# Guidelines for Using RFID Tags in Ontario Public Libraries

Information and Privacy
Commissioner of Ontario

Ann Cavoukian, Ph.D.
Commissioner
June 2004

# Acknowledgements

These *Guidelines* build upon three previous initiatives:

- the Ontario Library Information and Technology Association's (OLITA) information piece entitled, *Implementing RFID: Opportunities for Libraries*;
- the Office of the Information and Privacy Commissioner of Ontario (IPC) position paper entitled, *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*; and
- an IPC meeting with the OLITA Members' Council that explored Ontario library concerns about RFID tags and other electronic privacy issues on December 5, 2003.

Employees of the IPC also visited the Pickering Library (Petticoat Creek Branch) to view the recent implementation of RFID technology and met with the Toronto Reference Library's Director of Information Technology & Bibliographic Services to get a greater understanding of RFID capabilities and precautions.

Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, gratefully acknowledges the work of Pasha Peroff and Patricia D'Costa in preparing this report.

This publication is also available on the IPC website.

**Information and Privacy**
**Commissioner of Ontario**

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

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

# Table of Contents

# Introduction

Libraries in Ontario have expressed a particular interest in receiving customized guidelines to complement their current consideration and use of Radio Frequency Identification (RFID) technology. RFID technology is seen as a means to improve efficiency levels at library checkouts, to speed up inventory checks as well as to reduce the risk of repetitive strain injuries to library staff members. These guidelines are based on the view that the use of a Radio Frequency Identification system (as with most technologies) is appropriate within limited, controlled and well-defined circumstances.

Libraries must balance the advantages of using RFID technology with the potential privacy intrusions such technology can bring. RFID technology can be configured to ensure the privacy of library patrons is maintained.

The following *Guidelines* are intended to assist vendors and library employees responsible for RFID technology in developing implementation plans that take into account privacy protections within libraries' RFID systems.

Ontario Public Libraries are subject to the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). For public libraries, these guidelines must therefore be used in conjunction with the Act, which sets out specific responsibilities in terms of the collection, use and disclosure of personal information.

# Definitions

Within these Guidelines:

*Personal Information* is defined in section 2 of the *Act* as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex and age. If RFID technology retains characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information" under the *Act*.

*Record* also defined in section 2 of the *Act*, means any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record.

***Radio Frequency Identification (RFID) technology*** refers to a system that incorporates all physical, electronic or digital elements that enable RFID tags and readers to collect, use and store required data. Elements include tags, readers, computer hardware (such as servers), and RFID-specific software.

***Radio Frequency Identification (RFID) Tag*** is a small piece of material, composed of three components: a small antenna, a wireless "transducer" which may also be linked to a single silicon microchip unit containing memory storage and an encapsulating material which can be attached or inserted into many different materials.[1] Generally speaking, a tag is different from a barcode (which has been the scanning option of choice in libraries) because tags do not require a direct line of sight for reading. This ensures that multiple items can be scanned without physical contact of the scanner to the item, including transmission through hard materials such as CD casings or book covers. A standard library radio frequency setting should be 13.56 mhz (as suggested under U.S. FCC regulations).

***Passive Radio Frequency Identification (RFID) Tag*** has no power source and no on-tag transmitter built onto it, which gives a passive tag a range of less than 10-metres and makes it sensitive to regulatory and environmental constraints. Passive tags are generally the lowest in cost making them suitable for use in large inventories of books and other library media.[2]

***Active Radio Frequency Identification (RFID) Tag*** has both an on-tag power source and an active transmitter. Active tags are connected to their own battery. They can be read at much higher ranges, up to several kilometres away. However, they are larger and more expensive than

[1] *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*, released February 2004, www.ipc.on.ca/docs/rfid.pdf, P.6

[2] Ibid, P.8

passive tags. Active RFID tags are not suitable for libraries (as will be discussed later on). They are usually used for manufacturing, such as tracking components on an assembly line, or for logistics where the tag may be reused.[3]

Radio Frequency Identification (RFID) Readers vary in size and shape from portable handheld terminals to fixed devices positioned at strategic points such as library entranceways or circulation desks. A reader is equipped with antennas for sending and receiving signals, a transceiver and a processor to decode data. With ***passive tags***, the ***RFID reader*** transmits an energy field that activates the tag and powers its chip, enabling it to transmit or store data. ***Active tags*** may be programmed to transmit signals, so that data may be captured by multiple readers and distributed throughout a facility.[4]

***Chip Tags*** are ***RFID tags*** that contain an integrated circuit chip. Tags incorporating a chip 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.[5]

***Read-Only Chip*** refers to a chip that can be implanted within an ***RFID tag*** that has an identification code recorded at the time of manufacture or when allocated to an object. Read-only tags are therefore much cheaper and are typically used in ***passive tags***.[6]

***Read-Write Chip*** refers to a chip, implanted within an ***RFID tag that*** can have its memory changed, or written to, many times. Because they enable their ID codes to be changed, read-write chips offer greater functions but at a greater cost.[7]

[3] Ibid, P.8

[4] Ibid, P.9

[5] Ibid, P.7

[6] Ibid, taken from Bonsor, p. 3

[7] Ibid, P.8, taken from Bonsor, p. 3

## Broader Statements and Assumptions

These guidelines are presented in the context of the following assumptions:

- All libraries should have an effective privacy policy in place.
- All libraries should supply appropriate education and training to ensure compliance with an appropriate employee conduct policy.
- Other technology that is being considered for use within the library space is outside the scope of these guidelines.
- These guidelines do not address the use of smart cards (patron cards) that might include RFID technology.[8]
- These guidelines do not deal with the collection of personal information through means other than RFID technology.
- Appropriate notification around the use of RFID technology within the library is considered a basic expectation. This can consist of prominent signs that state: "This library uses RFID technology. No personal information is collected."
- Libraries should aim for openness and standardization with other libraries when implementing RFID technology. This is to ensure that functions vital to effective library services are not restricted due to proprietary system design or software.
- Libraries should ensure that the use and security of any RFID technology is subject to regular audits. The audit should also address the institution's compliance with the operational policies and procedures. An external body may be retained in order to perform the audit. Any deficiencies or concerns identified by the audit should be addressed immediately.
- Library employees and vendors should be aware that their activities are subject to audit and that they may be called upon to justify any wrongful use of patron information or RFID technology.
- Libraries should regularly review and evaluate their RFID program to ascertain whether it is still justified. This evaluation should occur in conjunction with other audits.

[8] For guidelines on smart cards please refer to: "Multi-Application Smart Cards: How to do a Privacy Assessment", IPC/Ontario, www.ipc.on.ca/docs/multiapp.pdf

# Collection of Personal Information

- Any recorded data, or other records of an identifiable individual, qualify as “personal information” under the *Act*. Libraries must determine if they have the authority to collect this personal information in accordance with the *Act*.

- Pursuant to Section 28 (2) of the *Act*, no person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

# Considerations prior to implementing and using RFID technology within a library[9]

An assessment should be conducted on the effects of the proposed RFID technology on personal privacy, and the ways in which any adverse effects can be mitigated.

Libraries should ensure that privacy issues are addressed at the design stage to ensure that RFID technology is introduced in a manner that minimizes privacy intrusions. This should include defined privacy requirements in any contracts with third-party vendors.

[9] Based on, "Guidelines for Using Video Surveillance Cameras in Public Places", Information and Privacy Commissioner of Ontario, October 2001, www.ipc.on.ca/docs/video-e.pdf

# Best practices for the acquisition and deployment of RFID Technology[10]

Once a decision has been made to use RFID technology, a library should develop and implement a comprehensive written policy for the operation of the system. This policy should be included in the library's RFI/RFP to ensure full knowledge of the requirements for the deployment of the RFID program. This policy should include:

- The rationale and objectives for implementing RFID technology.
- The use of the system's equipment, including the location of readers and which personnel are authorized to operate the system.
- The institution's obligations with respect to the notice, access, use, disclosure, retention, security and disposal of records in accordance with the *Act*.
- The designation of a senior staff member to be responsible for the institution's privacy obligations under the *Act* and its policy.
- A requirement that the institution will maintain control of, and responsibility for, the RFID program at all times.
- A requirement that any agreements between the institution and service providers state that the records dealt with or created while delivering RFID technology will remain under the control of the library and subject to the *Act*.
- A requirement that employees and service providers review and comply with the policy and the *Act* while performing their duties and functions related to the operations of RFID technology.
- Employees should be subject to discipline if they breach the policy or the provisions of the *Act* or other relevant statutes. Where a service provider fails to comply with the policy or the provisions of the *Act*, it would be considered a breach of contract leading to penalties up to and including contract terminations.
- Employees of institutions and employees of service vendors/providers should sign written agreements regarding their duties under the policy and the *Act*, including an undertaking of confidentiality.

[10] Ibid

- A requirement that there is a process in place to appropriately respond to any inadvertent disclosure of personal information.

- The incorporation of the policy into the training and orientation programs of a library. Training programs addressing staff obligations under the *Act* should be conducted on a regular basis.

- The policy should be reviewed and updated regularly, at least once every two years.

## Notification, Access, Use, Disclosure, Retention, Security and Disposal of RFID records[11]

Any information obtained by way of RFID technology may only be used for the purposes of the stated rationale and objectives. Information should not be retained or used for any other purposes.

- In the event that you are collecting patron information in a way you have not collected such information before, notification will be necessary to convey a library's new intentions before disclosing or accessing such personal information using RFID technology.

- In addition, notification requirements under section 29 (2) of the municipal *Act* include informing individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used and the title, business address and telephone number of someone who can answer questions about the collection. This information can be provided at the location on signage and/or by other means of public notification such as pamphlets.

- Institutions should be as open as possible about the RFID program in operation, and upon request, should make available to the public information on the rationale for RFID technology, its objectives and the policies and procedures that have been put in place. This may be done in pamphlet or leaflet form. A description of the program on an institution's Web site might also be an effective way of disseminating this information.

- Only personnel in control of the system, or those properly authorized in writing by those personnel according to the institution's employee conduct policy, should have access to the system that controls the RFID technology within the library, ensuring that any access to personal information is not available for public viewing.

- Ensure that all patron information that is linked via an RFID tag to any media is de-linked upon return of media item(s) by a patron.

- Ensure that all patron information databases are, by default, de-linked from any tag information database or tag memory chip. Patron information should only be linked to tags and tag databases upon checkout of media. Upon the return of any media items by the patron, the patron and media data should again become de-linked.

- Personal information about the patron should not be stored on the RFID tag's chip within the library media.

[11] Ibid

- Libraries should only implement the use of passive RFID tags. Passive tags, as mentioned in the Definitions section, only respond when activated by a reader since passive tags do not possess batteries and therefore cannot be tracked by satellite. Conversely, the use of active tags must be avoided as they can continually send out broadcasts of any data stored within the tag's chip, making the tag easy to scan externally.

- In the event that libraries consider the inclusion of patrons' personal information on a tag, privacy protection tools such as encryption and blocker technology must also be looked at.[12]

- Libraries should ensure that systems are designed to provide access to library employees only.

[12] 'Kill switches', which would be able to erase all stored data on a tag upon exit of the library is a tool most likely considered for commercial use and has little practicality in a library setting.

# Other Resources[13]

The personal information collected for use by the RFID program, and the institution's policies and practices respecting personal information, are subject to the privacy protection provisions of the *Act*.

Prior to implementing an RFID program or, for that matter, any new program with privacy implications, institutions should seek legal advice and consult with their Freedom of Information and Protection of Privacy Co-ordinator. Management Board Secretariat's Information and Privacy Office is a useful resource for Co-ordinators.

The Information and Privacy Commissioner of Ontario monitors compliance using the privacy protection provisions in the *Act*. If an institution intends to introduce, significantly modify or expand an RFID program, they should consult with the Office of the Information and Privacy Commissioner of Ontario.

[13] Ibid

## Future Challenges

Although RFID technology provides numerous benefits to library operations, setting a controlled and well-defined course of action will ensure that privacy and security protections are effective. However there are several challenges facing the effective use of RFID technology within libraries.

At this stage in Ontario with only some libraries venturing into RFID programs, an appropriate system of interoperability with non-RFID using libraries will be required. Libraries using RFID technology will have to deploy both bar codes and RFID tags for easy use within any inter-library loan program.

With new technology there is always the potential danger that innovations will lead to the ability to bypass RFID privacy and security measures. Keeping up to date on the latest circumvention methods will therefore be necessary.

Of course, future challenges are difficult to foresee but implementing the above guidelines will help to provide libraries with fundamental security and privacy protections, complementing the benefits that RFID technology provides.

Information and Privacy
Commissioner of Ontario

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

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