

RFID in Libraries: Privacy and Confidentiality Guidelines

Radio Frequency Identification (RFID) technology collects, uses, stores, and broadcasts data. Components of RFID systems include tags, tag readers, computer hardware (such as servers and security gates) and RFID-specific software (such as RFID system administration programs, inventory software, etc.).

RFID technology can enable efficient and ergonomic inventory, security, and circulation operations in libraries. Like other technologies that enable self-checkout of library materials, RFID can enhance individual privacy by allowing users to checkout materials without relying on library staff.

Because RFID tags may be read by unauthorized individuals using tag readers, there are concerns that the improper implementation of RFID technology will compromise users' privacy in the library.¹ Researchers have identified serious general concerns about the privacy implications of RFID use, and particular privacy concerns about RFID use in libraries.² Libraries implementing RFID should use and configure the technology to maintain the privacy of library users.

The Council of the American Library Association adopted the "Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles" (Appendix A) and requested the development of guidelines for the implementation of RFID technology in libraries.

Basic Privacy & Confidentiality Principles

Protecting user privacy and confidentiality has long been an integral part of the intellectual freedom mission of libraries.³ The right to free inquiry as assured by the First Amendment depends upon the ability to read and access information free from scrutiny by the government or other third parties. In their provision of services to library users, librarians have an ethical obligation, expressed in the *ALA Code of Ethics*,⁴ to preserve users' right to privacy and to prevent any unauthorized use of personally identifiable information. As always, librarians should follow these principles when adopting any new technology.

Policy Guidelines

When selecting and implementing RFID technology, librarians should:

- Use the RFID selection and procurement process as an opportunity to educate library users about RFID technology and its current and future use in the library and society as a whole. A transparent selection process allows a library to publicize its reasons for wanting to implement an RFID system while listening to its users and giving them a larger voice in the public debate over RFID technology.
- Consider selecting an "opt-in" system that allows library users who wish to use or carry an RFID-enabled borrower card do so while allowing others to choose an alternative method to borrow materials. Because all members who share integrated library systems may not wish to implement an RFID system, this option also may be necessary for library consortia.

- Review and update appropriate privacy policies and procedures to continue protecting users' privacy, in accordance with Article III of the *ALA Code of Ethics and Privacy: An Interpretation of the Library Bill of Rights*.⁵
- Ensure that institutional privacy policies and practices addressing notice, access, use, disclosure, retention, enforcement, security, and disposal of records are reflected in the configuration of the RFID system. As with any new application of technology, librarians should ensure that RFID policies and procedures explain and clarify how RFID affects users' privacy. The *ALA Guidelines for Developing a Library Privacy Policy*⁶ can assist libraries in drafting appropriate policies.
- Delete personally identifiable information (PII) collected by RFID systems, just as libraries take reasonable steps to remove PII from aggregated, summary data.
- Notify the public about the library's use of RFID technology. Disclose any changes in the library's privacy policies that result from the adoption of an RFID system. Notices can be posted inside the library and in the library's print and online publications.
- Assure that all library staff continue to receive training on privacy issues, especially regarding those issues that arise due to the implementation and use of RFID technology.
- Be prepared to answer users' questions about the impact of RFID technology on their privacy. Either staff at all levels should be trained to address users' concerns, or one person should be designated to address them.

Best Practices

As with any new application of technology, librarians should strive to develop best practices to protect user privacy and confidentiality. With respect to RFID technology, librarians should:

- Continue their longstanding commitment to securing bibliographic and patron databases from unauthorized access and use.
- Use the most secure connection possible for all communications with the Integrated Library Systems (ILS) to prevent unauthorized monitoring and access to personally identifiable information.
- Protect the data on RFID tags by the most secure means available, including encryption.
- Limit the bibliographic information stored on a tag to a unique identifier for the item (e.g., barcode number, record number, etc.). Use the security bit on the tag if it is applicable to your implementation.
- Block the public from searching the catalog by whatever unique identifier is used on RFID tags to avoid linking a specific item to information about its content.

- Train staff not to release information about an item's unique identifier in response to blind or casual inquiries.
- Store no personally identifiable information on any RFID tag. Limit the information stored on RFID-enabled borrower cards to a unique identifier.
- Label all RFID tag readers clearly so users know they are in use.
- Keep informed about changes in RFID technology, and review policies and procedures in light of new information.

Talking to Vendors about RFID

When dealing with vendors, librarians should:

- Assure that vendor agreements guarantee library control of all data and records and stipulate how the system will secure all information.
- Investigate closely vendors' assurances of library users' privacy.
- Evaluate vendor agreements in relationship with all library privacy policies and local, state, and federal laws.
- Influence the development of RFID technology by issuing Requests for Proposals requiring the use of security technology that preserves privacy and prevents monitoring.

The Request For Information developed by the San Francisco Public Library provides a helpful list of sample questions (Appendix B) to ask when talking to vendors about privacy and their RFID products.

¹ Lori Bowen Ayre, "Wireless Tracking in the Library: Benefits, Threats, and Responsibilities," *RFID: Applications, Security, and Privacy*, Garfinkle and Rosenberg, eds. (Addison-Wesley, 2006)

² David Molnar and David Wagner, Privacy and Security in Library RFID: Issues, Practices, and Architectures, CCS'04, October 25-29, 2004 Washington, D.C.

³ <http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/introduction/introduction.htm>

⁴ <http://www.ala.org/oif/policies/codeofethics>

⁵ <http://www.ala.org/oif/policies/interpretations/privacy>

⁶ <http://www.ala.org/oif/iftoolkits/privacy/guidelines>