

53.11

At the 2005 ALA Midwinter Meeting, the ALA Council adopted CD#19.1, Radio Frequency Identification (RFID) Technology and Privacy Principles.

At the 2005 ALA Annual Conference, the Council Policy Monitoring Committee recommended that the following policy abstract be added to ALA Policy Manual as follows:

53:11 RFID Privacy Principles

All businesses, organizations, libraries, educational institutions, and non-profits that buy, sell, loan, or otherwise make available books and other content to the public utilizing RFID technologies shall:

1. Implement and enforce an up-to-date organizational privacy policy that gives notice and full disclosure as to the use, terms of use, and any change in the terms of use for data collected via new technologies and processes, including RFID.
2. Ensure that no personal information is recorded on RFID tags which, however, may contain a variety of transactional data.
3. Protect data by reasonable security safeguards against interpretation by an unauthorized third party.
4. Comply with relevant federal, state, and local laws as well as industry best practices and policies.
5. Ensure that the four principles outlined above must be verifiable by an independent audit.

(See "Policy Reference File": Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles: 2004-2005 CD 19.1)

**RESOLUTION ON
RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY
AND PRIVACY PRINCIPLES**

WHEREAS, Radio Frequency Identification (RFID) is a technology that uses various electronic devices, such as microchip tags, tag readers, computer servers, and software, to automate library transactions; and

WHEREAS, the use of RFID technology promises to improve library operations by increasing the efficiency of library transactions, reducing workplace injuries, and improving services to library users; and

WHEREAS, many libraries are adopting or in the process of adopting RFID technology to automate library circulation, inventory management, and security control; and

WHEREAS, consumers, consumer groups, librarians, and library users have raised concerns about the misuse of RFID technology to collect information on library users' reading habits and other activities without their consent or knowledge; and

WHEREAS, protecting user privacy and confidentiality has long been an integral part of the mission of libraries; and

WHEREAS, the ALA Code of Ethics states, "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted"; and

WHEREAS, *Privacy: An Interpretation of the Library Bill of Rights* states that "The American Library Association affirms that rights of privacy are necessary for intellectual freedom and are fundamental to the ethics and practice of librarianship," and calls upon librarians "to maintain an environment respectful and protective of the privacy of all users"; and

WHEREAS, the ALA Intellectual Freedom Committee recognizes the importance of developing policies and guidelines for appropriate implementation of RFID technology in light of the profession's commitment to preserving user privacy and its concern for preserving the trust of library users; and

WHEREAS, the ALA Intellectual Freedom Committee and the ALA Office for Information Technology Policy, recognizing the immediate need to draft privacy principles to protect and promote ALA's values, joined with the Book Industry Study Group (BISG) to form a working group dedicated to developing a set of privacy principles to govern the use of RFID technology by all organizations and industries related to the creation, publication, distribution, and retail sale of books and their use in libraries; now, therefore, let it be

RESOLVED, that the American Library Association endorse the "BISG Policy Statement Policy #002: RFID — Radio Frequency Identification Privacy Principles" (Exhibit I) developed by the IFC and the OITP with the BISG and other working groups; and be it further

RESOLVED, that ALA affirm established privacy norms within and across the business, government, educational, and nonprofit spectrum, specifically acknowledging two essential privacy norms:

- Data transferred among trading partners related to customer and/or patron transactions shall be used solely for related business practices and no unauthorized transaction shall be permitted.
- Data related to customer and/or patron transactions shall not compromise standard confidentiality agreements among trading partners or information users; and be it further

RESOLVED, that the ALA adopt the following "RFID Privacy Principles" developed by the IFC and OITP with the BISG RFID working group:

All businesses, organizations, libraries, educational institutions and non-profits that buy, sell, loan, or otherwise make available books and other content to the public utilizing RFID technologies shall:

- 1) Implement and enforce an up-to-date organizational privacy policy that gives notice and full disclosure as to the use, terms of use, and any change in the terms of use for data collected via new technologies and processes, including RFID.
- 2) Ensure that no personal information is recorded on RFID tags which, however, may contain a variety of transactional data.
- 3) Protect data by reasonable security safeguards against interpretation by any unauthorized third party.
- 4) Comply with relevant federal, state, and local laws as well as industry best practices and policies.
- 5) Ensure that the four principles outlined above must be verifiable by an independent audit; and be it further

RESOLVED, that the ALA continue to monitor and to address concerns about the potential misuse of RFID technology to collect information on library users' reading habits and other activities without their consent or knowledge; and be it further

RESOLVED, that the ALA develop implementation guidelines for the use of RFID technologies in libraries.

Submitted by the Intellectual Freedom Committee and the Office for Information Technology Policy Advisory Committee

Endorsed in principle by Intellectual Freedom Round Table
Endorsed in principle by the Social Responsibilities Round Table
Endorsed in principle by the ALA Committee on Legislation



BISG Policy Statement

Policy #002: RFID - Radio Frequency Identification Privacy Principles

Approved : September 23, 2004

Overview

We, the industries and organizations related to the creation, publishing, distribution, and retail sales of books and their use in libraries, strive to ensure confidentiality when we collect any personally identifiable information about our users. This ideal holds as we consider, adopt and/or implement any new technology, such as RFID (Radio Frequency Identification). The right to privacy is essential to the exercise of free speech, free thought, and free association. Lack of privacy and confidentiality chills users' choices, suppressing access to ideas. The possibility of surveillance, whether direct or through access to records of speech, research and exploration, undermines a democratic society.

While the potential of RFID for cost savings, reduction in workplace injuries, and new efficiencies are enormous, it is equally important to answer the privacy concerns that have already been raised by consumers, consumer groups and legislative bodies. We recognize that when technical capabilities are combined with competitive business pressures "to know and capture the customer," -- as well as national security concerns -- the capability to meet consumer, citizen and legislated privacy mandates becomes increasingly difficult. Thus, the potential for misuse and abuse of personal information and loss of trust become major public policy issues.

These guidelines represent the approach our industries and organizations will take to reduce the potential for misuse of personal information and to avoid the loss of trust of consumers and library users. Since some forms of RFID technology are already in use in some libraries, and may be explored by many others as well as in different areas of the publishing value chain (at such time as it makes economic and consumer sense), we believe that now is the time to publish these guidelines.

We would like to emphasize that the scope and purpose of these guidelines is not to restate the well-developed principles of privacy protection that have been defined over the past thirty years, both in the US and overseas. These guidelines are meant to address specifically the new aspects of privacy protection, and respect for personal information that are generated by the implementation of RFID technology, even as it changes and evolves over time.

In asserting our adherence to these RFID privacy principles we also affirm our respect for established privacy norms within and across the business, government, educational and non-profit spectrum. For example:

- Data transferred among trading partners related to customer and/or patron transactions shall be used solely for related business practices and no unauthorized transaction shall be permitted.
- Data related to customer and/or patron transactions shall not compromise standard confidentiality agreements among trading partners or information users.

These privacy norms are intended to include all current practices to ensure safe and secure data transfer such as in the use of electronic (EDI) transactions.

As with all policies created by the Book Industry Study Group, we encourage wide spread distribution and dissemination. Any edits or alterations to improve but not limit the policy are also encouraged and supported by the Book Industry Study Group. Any altered policy must still contain and sustain the spirit in which these principles were established.

RFID Privacy Principles

All businesses, organizations, libraries, educational institutions and non-profits that buy, sell, loan, or otherwise make available books and other content to the public utilizing RFID technologies shall:

- 1) Implement and enforce an up-to-date organizational privacy policy that gives notice and full disclosure as to the use, terms of use, and any change in the terms of use for data collected via new technologies and processes, including RFID.
- 2) Ensure that no personal information is recorded on RFID tags which, however, may contain a variety of transactional data.
- 3) Protect data by reasonable security safeguards against interpretation by any unauthorized third party.
- 4) Comply with relevant federal, state, and local laws as well as industry best practices and policies.
- 5) Ensure that the four principles outlined above must be verifiable by an independent audit.

This policy has been developed and released by the Book Industry Study Group in cooperation with the American Library Association, Office of Information Technology and the Office for Intellectual Freedom, as well as the National Information Standards Organization

Glossary / Terms

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, typically composed and therefore defined by three components: an antenna, a silicon microchip unit containing memory storage and an encapsulating material. Generally speaking, a tag is unlike a barcode (which have been the scanning option of choice in libraries) because tags do not require a direct line of sight for reading and you can read more than 1 tag simultaneously. This ensures that multiple items can be left untouched and scanned at the same time through hard material such as a CD casing or book cover. A standard library frequency setting should be 13.56 MHz (an approved frequency of operation under U.S. FCC regulations).

Passive Radio Frequency Identification (RFID) Tag has no power source and no on-tag transmitter built onto it. The read range of a passive tag is directly related to the size of the tag, and is typically less than 10-metres and is more 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 media formats.

Active Radio Frequency Identification (RFID) Tag has both an on-tag power source and an active transmitter. 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. They are usually used in manufacturing, such as tracking equipment and other high value assets, toll collection systems, or for logistics where the tag may be reused.

Radio Frequency Identification (RFID) Reader varies in shape from being a portable handheld terminal to fixed devices positioned at strategic points such as at library entrance ways or loading bays in manufacturing or distribution centers. The 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.

Read-Only Tag refers to the form of RFID tags that have an identification code recorded at the time of manufacture or when allocated to an object. Once programmed, the data on the read only tag cannot be modified or appended, but can be read many times.

Read-Write Tag refers to the form of RFID tags that 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.

Bibliography

American Library Association

Privacy and Confidentiality Resources

(http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/Intellectual_Freedom3/Intellectual_Freedom_Issues/Privacy_and_Confidentiality.htm)

American Library Association,

Privacy Toolkit

(<http://www.ala.org/oif/iftoolkits/privacy>)

United States Department of Health, Education and Welfare

Records, Computers and the Rights of Citizens, Summary and Recommendations (1973)

(<http://aspe.hhs.gov/datacncl/1973privacy/Summary.htm>)

United States Federal Trade Commission, "Chapter III: Fair Information Practice Principles," Privacy Online: A Report to Congress (June 1998)

<http://www.ftc.gov/reports/privacy3/fairinfo.htm#Fair%20Information%20Practice%20Principles>

Organization for Economic Cooperation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Sept. 1980):

<http://www.oecd.org/EN/document/0..EN-document-0-nodirectorate-no-4-10255-0.00.html#title1>

Code of Fair Information Practices

<http://cse.stanford.edu/class/cs201/handouts/h29.pdf>

Privacy Act of 1974

http://www.epic.org/privacy/laws/privacy_act.html (text of bill)

http://www.usdoj.gov/04foia/04_7_1.html (background and updates)

<http://www.consumerprivacyguide.org/law/pa.shtml> (consumer guide)

Briefing Materials on the European Union Directive on Data Protection

http://www.cdt.org/privacy/eudirective/EU_Directive.html#HD_NM_1

Center for Democracy and Technology Guidelines on Privacy

<http://www.cdt.org/privacy/guide/basic/generic.html>

Organization for Economic Cooperation and Development

<http://www.cdt.org/privacy/guide/basic/oecdguidelines.html>

Privacy Rights Clearinghouse, A Checklist of Responsible Information-Handling Practices:

<http://www.privacyrights.org/fs/fs12-ih2.htm>

Computer Professionals for Social Responsibility, Electronic Privacy Principles:

<http://www.cpsr.org/program/privacy/privacy8.html>

United States Federal Trade Commission, *Privacy Tips*:

<http://www.ftc.gov/bcp/online/pubs/alerts/privtipsalrt.htm>