

## PRIVACY AND CONFIDENTIALITY OF PATRON RECORDS

One major concern of libraries is the privacy and confidentiality of patron records. These records can include circulation records, web use logs and general patron information, such as names, street addresses and social security numbers. The passage of the [USA PATRIOT Act](#) (H.R. 3162) has given this concern a new urgency. In response to the Act, the American Library Association (ALA) has resolved that:

“...(ALA) opposes any use of governmental power to suppress the free and open exchange of knowledge and information or to intimidate individuals exercising free inquiry...ALA considers that sections of the USA PATRIOT Act are a present danger to the constitutional rights and privacy rights of library users”

Source: [Resolution on the USA Patriot Act](#)

If libraries adhere to this resolution, then the following actions should be taken to ensure that patron privacy is protected:

### 1. Maintain a current, written policy concerning the confidentiality of patron records

A written policy on patron records can be used as a training and reference guide for library staff and as a policy statement to answer any community or patron questions. A library’s written policy should be easily accessible in either a print or an electronic format.

### 2. Ensure that library procedures are secure regarding patron records

Libraries may need to thoroughly revisit and revise the procedures they follow when handling and storing confidential library information. Consider both print and electronic storage mechanisms. Should circulation records automatically purge after each transaction (including hold and overdue/lost items)? Should web logs be minimized or possibly disabled? Consider how long to retain each type of patron record.

### 3. Understand Maryland State Law concerning the privacy of patron records

Libraries and librarians should become informed of the Maryland State Government Code Ann. § 10-616 regarding [Access to Public Records](#).

### 4. Train library staff on issues of confidentiality and privacy

A well-crafted written policy concerning the confidentiality of patron records can be used as a basis for any library staff training. Additional materials, such as checklists and activities are readily available online and in ALA monographs.

#### Radio Frequency Identification (RFID) in Libraries: Benefits and Privacy Concerns

Radio Frequency Identification is a term for devices that use radio waves to track and identify individual items. RFID tags are placed in items and a reader picks up the radio frequencies emanating from the tags. RFID tags are currently in use in automatic toll collection systems, wireless car keys and livestock and military armament tracking devices. Several prominent national, state and city library systems have begun using RFID tags to secure and track library collections and materials. In RFID technologies, unlike bar code

systems, the reader does not require a clear line of sight, meaning that radio waves can be read through a variety of materials, including walls. Placed in books, RFID tags can transmit whatever detail is encoded, such as a title, author and/or an ISBN and can be read at a variety of ranges depending on the power of the reader. The cost for RFID tags is currently four to five times greater than using a combination of the more traditional bar code and magnetic strip.

The use of RFID technology in libraries provides a number of substantial benefits, but also poses some privacy concerns. RFID promises to decrease repetitive use syndromes, to speed library checkout and to hasten the library inventory process (see "[RFID and Libraries: Both Sides of the Chip](#)").

### Privacy Concerns

The concern with RFID systems in libraries is that tags containing static information can be easily read by unauthorized readers. Anyone with a powerful enough reader could covertly identify the items a person is carrying or even what items a person owns in a home or an office. This opens up privacy issues known as "tracking" and "hotlisting." Tracking is the ability to track the movement of a book (and consequently, the person carrying the book) by correlating multiple readings of the tag. Hotlisting is the process of creating a database of particular books and their tag numbers (hotlist) and, by unauthorized readings, determine who is checking out items from that list. [Molnar and Wagner](#) state that, "Hotlisting is problematic because it allows an adversary to gather information about an individual's reading habits without a court order" and, "With current architectures, hotlisting is possible: each book has a single static identifier, and this identifier never changes over the book's lifetime."

To counter the potential invasion of privacy, libraries employing RFID technology should consider using any of a number of strategies. Libraries may simply choose to disable RFID tags once they leave the library. Libraries can install short-range radio tags, which can be read only up to a distance of one foot. Another viable option is to avoid using a single static identifier and instead use different library item identifiers to make hotlisting more difficult. Encryption would not prevent unauthorized readings, but would make the data illegible.

If a library decides to use RFID, a good first step is to inform their patrons, so that they may make an informed choice in their borrowing decisions.



### Works Cited in this article:

Molnar, David and David Wagner. "Privacy and Security in Library RFID Issues, Practices and Architectures." *Electronic Frontier Foundation*, Oct. 2004, [https://w2.eff.org/Privacy/Surveillance/RFID/molnar\\_paper.pdf](https://w2.eff.org/Privacy/Surveillance/RFID/molnar_paper.pdf). Accessed 27 June 2017.

"Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users." 2005. American Library Association, 2005,

<http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11891>. Accessed 27 June 2017.

Schneider, Karen G. "RFID and Libraries: Both Sides of the Chip." [RFID](#). *American Library Association*, 19 Nov. 2003, <http://www.ala.org/offices/sites/ala.org.offices/files/content/oif/ifissues/rfidbothsideschip.pdf>. Accessed 27 June 2017.

Carson, Bryan M. "State and Territorial Library Privacy Laws." *The Law of Libraries and Archives*, 24 Sept. 2007, <http://people.wku.edu/bryan.carson/librarylaw/circulation+privacy+laws.html>. Accessed 27 June 2017.

"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001." *FindLaw.Com*, Oct. 2001, <http://files.findlaw.com/news.findlaw.com/cnn/docs/terrorism/hr3162.pdf>. Accessed 27 June 2017.

Further Reading:

Balas, Janet L. "Should There Be an Expectation of Privacy in the Library?" *Computers in Libraries* 25.6 (2005): 33.

Carlson, Scott. "[New High-tech Labels Help Libraries Track Books, but Worry Privacy Advocates](#)." 6 Aug. 2004. *Chronicle of Higher Education*, 6 Aug. 2004. Accessed 29 June 2017.

Coombs, Karen A. "Walking a Tightrope: Academic Libraries and Privacy." *Journal of Academic Librarianship* 30.6 (2004): 493-497.

Coyle, Karen. "Make Sure You Are Privacy Literate." *Library Journal* 127.16 (2002): 55-57.

Feder, Barnaby J. "How to Find That Needle Hopelessly Lost in the Haystack." *New York Times* (Late Edition (East Coast)). New York, N.Y.: Sep. 29, 2003. pg. C.1.

Huff, James. "Patron Confidentiality, Millennium Style." *American Libraries* 30.6 (1999): 86-88.

"[RFID Tags](#)." *RFID Journal*, (n.d.). Accessed 29 June 2017.

Saffo, Paul. "Convenience Trumps Privacy." *CIO Magazine*, Fall/Winter 2003.

Strickland, Lee S. and Laura E. Hunt. "Technology, Security and Individual Privacy, New Tools, New Threats and New Public Perceptions." *Journal of the American Society for Information Science and Technology* 56.3 (2005): 221-234.

Want, Roy. "RFID: A Key to Automating Everything." *Scientific American* 290.1 (2004): 56-65.