Laura J. Smart

Considering RFID

Benefits, limitations, and best practices

Radio frequency identification (RFID) tagging is an alternative to bar coding for physical access to library materials. The technology is rather new for libraries, although it has been used in retail and warehousing applications since the 1980s.[1] It promises to streamline operations by enabling faster self-checkout and self-returns, improving shelf management and inventory control, and providing better theft protection. Yet RFID is controversial because of privacy issues. It is possible, but not yet practical, to use it to track a person's movements and reading habits. Privacy concerns have been dismissed by Dornan and Schuyler,[2] but the debate rages. Academic librarians need to be aware of the technology and its implications to evaluate and possibly implement it. The purpose of this article is to describe the benefits and limitations of the technology and the current state of library best practices.

How RFID works

An RFID system may consist of several components: tags, tag readers, tag programming stations, circulation readers, sorting equipment, and tag inventory wands. RFID tags are, essentially, very small radio receivers with a microchip. The microchip is programmed with distinctive information about the item which can be directly imported from an integrated library system (ILS) at the tag programming station. It is possible to include many types of information on the tag (such as book title, patron circulation information, date/time stamps), but a tag would typically contain only barcode information.

Security can be handled in two ways. Security gates can query the ILS to determine an item's security status, or the tag attached to an item may contain a security bit that would be turned on and off by circulation or self-checkout reader stations. Security gates can then detect whether or not the item has been properly checked out of the library. When users return items, the security bit is reset and the item record in the ILS is automatically updated. In some RFID solutions, a return receipt can be generated. At this point, materials can be roughly sorted into bins by the return equipment. Inventory wands provide a finer detail of sorting. This tool can be used to put books into shelf-ready order. It can also be taken to the stacks to detect out-of-place items.

Benefits of RFID

Richard Boss provides a cost/benefit comparison of RFID systems.[3] The first benefit is faster circulation operations. Unlike barcodes, which require a clear line of sight, the tags can be read regardless of how the item is placed on the circulation reader. Also, multiple items can be read simultaneously. This could reduce long lines at busy circulation desks.

The second benefit is increased self-checkout. Users do not have to line up barcodes carefully for a successful transaction. The units have a simple interface, which can make it easier for patrons to serve themselves. Circulation staff can be free to perform other public service work.

Laura J. Smart is electronic resources cataloger at California State Polytechnic University-Pomona

The third benefit mentioned by Boss is reliable security. Vendors claim that the theft detection rate of RFID is high, although there is not yet any evidence that it is better than electromagnetic systems. At least those RFID systems that can query the ILS can indicate precisely what items are moving out of the library. This is great for replacing stolen items.

The fourth benefit is faster inventorying. Shelf-reading becomes automated and more accurate. Library staff can simply walk down the aisles and detect out-of-order materials. The number of lost and missing items in the library should decrease. The inventory wand can also be used in collection development and weeding projects.

Another benefit is longevity. Most RFID vendors guarantee tags for the lifetime of the book. Finally, RFID self-checkout systems have potential to reduce repetitive strain injuries for circulation staff. During recent public hearings, the San Francisco Public Library reported that RFID circulation systems use fewer hand motions than current circulation systems.

Limitations to RFID systems

There are several limitations to RFID systems. Privacy concerns have garnered much of the media attention surrounding RFID (ALA provides a Web page with many links to sites that describe the potential privacy threats).[4] Other disadvantages are cost, lack of documented return on investment, and security weaknesses.

Cost is prohibitive. Plain tags are priced between 50 and 70 cents apiece. Prices for special media tags for optical discs and video tape range from 99 cents to $1.50. Customized labels with a library logo further increase the cost. This quickly adds up when a collection is substantial. A mid-sized academic library would spend $280,000 to convert 400,000 items to RFID with plain 70-cent tags—and this does not include equipment or labor costs. The prices of RFID tags are likely to decrease in the future, however.

Return on investment has not been sufficiently documented in the library literature, and the evidence provided to date is anecdotal. For example, the University of Nevada, Las Vegas (UNLV) has reported saving $40,000 in replacement costs for the 500 "lost" items it found after tagging its 657,611 item collection.[5] The Mastics-Moriches Community Library in the state of New York carried out a time and cost analysis to compare the use of Electronic Article Surveillance (EAS) and RFID systems for circulation and found that the latter saved them approximately 85 percent in labor time.[6]

A closer look at security threats

After cost issues comes security and privacy weaknesses. RFID tags are typically placed on the back inside cover of a book. Enterprising thieves could easily remove the tags and subvert the security gates. This problem is mitigated somewhat by using customized labels for the tags, which make the RFID tags appear more like a book plate.

Another security threat is frequency blocking. Boss reports that some tags can be blocked by wrapping them in household foil. But blocking may not always be so deliberate. Some libraries report interference when library items have RFID tags affixed in the same position on every item. If tags overlap, then the signal is blocked. Libraries have been working around the problem by using templates to affix the tags in alternating positions during processing.

Commercial blockers are readily available. Ari Jules from RSA Security has developed a blocker tag that seems to have the potential to alleviate unauthorized tag reading.[7] The creators claim it will not circumvent theft-detection devices, but the blocking device has not yet been proven in market. Libraries may get themselves into a world of constant hardware upgrades to cope as blockers grow stronger and more sophisticated.

There are several additional security and privacy threats within library RFID system architectures. University of California, Berkeley electrical engineers David Molnar and David Wagner have identified these as hotlisting, hardware identification numbers, eavesdropping, and unauthorized tag writing.[8] In hot-

listing, an adversary reads the tag on a book then copies the information to a personal database. This list of books can then be used with a gate reader. The FBI, for example, could get the tag information for every local copy of *The World Almanac*. They would know whenever somebody carrying that item walked by a gate in a public place. Hotlisting is possible because tag information remains stable over the lifetime of a book. Even if tag data is write-protected and encrypted, there is still information on each tag at the hardware level. Each tag must have a unique identifier if many tags are to be read simultaneously. This is to mitigate radio signal collision.

Eavesdropping can occur because the signal between tag and reader is wireless and unencrypted. Unauthorized tag writing can occur if a library uses rewritable tags. An attacker could wait for a legitimate reader to unlock a tag and then send its own write commands before the legitimate reader. Molnar says, "if a security bit is unlocked, an adversary can cause false alarms for legitimately checked out books … if an item identifier is unlocked, the adversary may overwrite it causing confusion and potentially a lost book."[9]

RFID vendors are beginning to acknowledge the security flaws in library RFID architectures. Library Automation Technologies has developed an encryption envelope for communications between tags and tag readers. This technology is available for licensing at a low cost, however, vendors have been slow to respond, says Eric Ipsen, director of business development.

RFID and privacy

The privacy threats most often referred to in the library literature are the linking of personal information with specific library materials and the tracking of individual movements. We can label these threats as unauthorized access to the ILS and unauthorized tag reading. Unauthorized access to the ILS is not likely in current library practice. Most library databases are secured. Only personnel with a legitimate need to know have the right to use patron information, which is probably password protected. The link between reader and book only exists during the time an item is circulating, since many libraries do not retain those records.

Unauthorized tag reading requires access to a tag reader. It would take effort to acquire one, and, once acquired, it would have to operate on the correct frequency. Library RFID solutions work on the 13.56 MHz frequency band. Regular commercial RFID readers work on a different frequency and would be useless in the library. An illegal or home-grown reader might work, but it would be limited by the amount of information programmed on to the RFID tag. If only the bar code information is there, how could the adversary violate a patron's freedom to read?

Unauthorized reading is also not practical for tracking an individual's movements. It would take a dragnet of readers with stronger frequencies spread out over a wide geographic area to work effectively for this purpose. However, a single unmarked gate would pose a privacy threat if patrons were unaware that their belongings were being monitored.

All of these privacy and security threats are labor intensive. The controversy stems from the *potential* of RFID technologies to erode privacy and civil liberties. RFID is increasingly being used in commercial applications, and in its ubiquity lies its danger. As the technology evolves, stronger readers could emerge and start popping up everywhere like cell phone signal transmitters.

Developing best practices

Library RFID systems currently practice "security through obscurity." Best practices are emerging, however. Organizations such as Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), Privacy Rights Clearinghouse, the Electronic Frontier Foundation (EFF), and the American Civil Liberties Union (ACLU) have been raising the alarm about RFID.[10] Yet, libraries such as the UNLV library; Santa Clara, California Public Library; and Cerritos, California Public Library have implemented RFID systems with little fanfare. It was not until fall 2003

that library RFID entered the public consciousness when the San Francisco Public Library announced plans to investigate RFID systems. The EFF and ACLU went on record with their opposition.[11] This came on the heels of an August 2003 California state senate committee informational hearing on RFID technology.[12] Since then, California legislators attempted to pass a senate bill to limit the types of information associated with RFID in retail and library applications. Several other states, notably Utah and Massachusetts, have considered similar legislation. There have also been calls for legislation on the federal level.

Librarians are not waiting for a legislative mandate to create best practices. At the American Library Association 2004 Midwinter Meeting, the Privacy Rights Clearinghouse and EFF recommended that libraries include RFID in their privacy policies, limit the type of information on the tags, inform patrons that the information is being collected and why, and have auditable security measures.[13] Berkeley Public Library created a brief list of RFID recommendations that were used in selecting a vendor. They are informing patrons about RFID use, limiting the tag to barcode information, banning wireless communication between gates and tags, reinforcing the security of the ILS, and not using RFID tags on patron identification cards.[14] Ontario public libraries have a comprehensive set of guidelines that include instructions on how to update a library privacy policy to include RFID.[15]

Radio frequency identification tags in libraries have the potential to improve physical access to library materials. There are many benefits but also many limitations to the technology. RFID has significant privacy implications. Security flaws are embedded at the tag level and adequate technological solutions have not yet been developed, although interest in regulating the technology is increasing. The prevalence of RFID technology is only increasing now that big interests such as Wal-Mart and the United States military have mandated that their suppliers use RFID to track shipments.

RFID will not be going away. Librarians will need to continue monitoring the technology and maintain their professional obligation to protect patron privacy if they are going to choose RFID.

Notes

1. Association for Automatic Identification and Mobility. *Radio Frequency Identi cation (RFID) homepage,* www.aimglobal.org/technologies/rfid (accessed 10 February 2004).

2. David Dornan, "Technically speaking: RFID poses no problem for patron privacy," *American Libraries* (Dec. 2003): 86. Michael Schuyler, "View from the top left corner: RFID: helpmate or conspiracy?" *Computers in Libraries* 24, (Jan. 2004): 22.

3. Richard Boss, "RFID technology for libraries," *Library Technology Reports* (Nov/Dec 2003): 8–10.

4. American Library Association Office for Intellectual Freedom, *RFID: Radio Frequency Identi cation Chips and Systems,* www.ala.org/ala/oif/ifissues/rfid.htm (accessed 19 February 2004).

5. Scott Carleson, "Talking tags: new high tech labels help libraries track books, but worry privacy advocates," *Chronicle of Higher Education* August 6, 2004 chronicle.com/free/v50/i48/48a02901.htm (accessed 15 August 2004)

6. Brigit Lindl, "Radio tagged books: why librarians should switch on their radios," *Research Information* June 2004, www.researchinformation.info/rimayjun04radiotagged.html (accessed 2 July 2004)

7. Ari Juels, Ronald L. Rivest, and Michael Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, in: V. Atluri, ed., *10th ACM Conference on Computer and Communications Security*. New York: ACM Press; 2003.

8. David Molnar and David Wagner. "Privacy and security in library RFID: issues, practices and architectures," *ACM CCS 2004* (in publication), 8–9, www.cs.berkeley.edu/~dmolnar/library.pdf (accessed 15 June 2004).

9. Ibid.

(Continued on page 42)

Leslie Madden, reference librarian, Georgia Institute of Technology.

Western European Studies Section

Vice-chair/Chair-elect: *Sebastian Hierl*, bibliographer for English and romance Literatures, University of Chicago; *Bryan Skib*, coordinator of graduate library collections, University of Michigan.

Secretary: *Laura Dale Bischof*, librarian for German and Western European history, University of Minnesota; *David Lincove*, history, political science and philosophy librarian, Ohio State University.

Member-at-Large: *Heather Ward*, humanities librarian, University of Oregon; *Sarah Wenzel*, reference coordinator, Humanities Library, Massachusetts Institute of Technology.

Women's Studies Section

Vice-chair/Chair-elect: *Kelly Barrick Hovendick*, interim head, reference, Syracuse University Library.

Secretary: *Cynthia Johnson*, director of reader services, Pratt Institute; *Susan Kane*, reference librarian/women studies librarian, University of Washington.

Member-at-Large: *Pamela Mann*, Mexican American/Latino studies librarian, University of Texas; *Diane Gwamanda*, head of access services, University of Houston.

(Recreation continued from page 12)

Minnesota Wild are scheduled to play the Detroit Redwings on April 10th at the Excel Energy Center in downtown St. Paul.

And the Minnesota Timberwolves, led by last year's NBA Most Valuable Player, Kevin Garnett, play the Denver Nuggets in basketball at the Target Center in downtown Minneapolis on April 8th.

Whether you are interested in getting some exercise, taking a stroll down the river, or taking in world-class sporting events, you will find many attractions to keep you fit, relaxed, and entertained. Enjoy your time in the fabulous Twin Cities!

(RFID continued from page 16)

10. Consumers Against Supermarket Privacy Invasion and Numbering, et al., *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations,* November 20, 2003, www.privacyrights.org/ar/RFIDposition.htm (accessed 21 June 2004).

11. Electronic Frontier Foundation, *EFF Comments to San Francisco Public Libraries*, www.eff.org/Privacy/Surveillance/RFID/20031002_sfpl_comments.php (accessed 10 February 2004).

12. California Senate, Energy, Utilities and Communications Committee, Subcommittee on New Technologies, *Informational Hearing: RFID Technology and Pervasive Computing* (Sacramento, 2003), www.sen.ca.gov/ftp/SEN/COMMITTEE/STANDING/ENERGY/_home/08-18-03agenda.htm (accessed 07 June 2004).

13. Beth Givens, "RFID implementation in libraries: some recommendations for best practices" (paper presented at the Midwinter Meeting of the American Library Association, San Diego, January 2004), www.privacyrights.org/ar/RFID-ALA.htm (accessed 15 June 2004).

14. Berkeley Public Library, *Best Practices for RFID Technology*, berkeleypubliclibrary.org/BESTPRAC.pdf (accessed 15 June 2004).

15. Ann Cavoukian, *Guidelines for Using RFID Tags in Ontario Public Libraries*, Toronto, Ontario: Information and Privacy Commissioner/Ontario. (June 2004), www.ipc.on.ca/docs/rfid-lib.pdf (accessed 21 June 2004).