Chapter 6

RFID in Libraries

Deborah Caldwell-Stone

Abstract

The implementation of radio frequency identification (RFID) technologies by U.S. libraries is noteworthy for the controversy that resulted when organizations like the Electronic Frontier Foundation and the ACLU protested libraries' adoption of RFID and argued that the privacy risks posed by RFID were so great that libraries should avoid adopting RFID technology altogether. Nearly a decade later, RFID is an accepted technology in libraries, thanks in part to the profession's adoption of best practices that minimize the technology's potential to erode library users' privacy.

The National Information Standards Organization (NISO) has since published a document, RFID in U.S. Libraries*, that contains recommended practices intended to facilitate the use of radio frequency identification in library applications. Though the document includes privacy within its charge, it does not include or discuss the best practices adopted by the library profession.*

This article reviews the controversy surrounding the use of RFID technologies in U.S. libraries and the steps taken by the library profession to resolve those issues. It evaluates and discusses the privacy recommendations made by NISO's RFID Working Group on RFID in U.S. Libraries.

Overview

Radio frequency identification technology enables the tracking and monitoring of physical items by attaching an RFID tag or transponder to an item. Each tag consists of an internal antenna and a computer chip that stores data. When the tag is scanned or interrogated by a reading device equipped with its own antenna, the tag communicates its data wirelessly via radio waves to the reader.

The range at which an RFID tag is read depends upon the tag design, the method of communication between the tag and the reader, and the radio frequency at which the RFID application operates. "Passive" tags do not have a power source and cannot transmit information unless powered by the energy contained in the radio signal transmitted by the RFID reader; the read range of passive tags is relatively short. "Active" RFID tags are powered by a battery or other power source and are able to transmit their signal over large distances.

The tags employed in library applications are high-frequency (HF) passive tags that operate at 13.56 MHz and can be read at distances from eight inches to two meters, depending on the size and the power of the antenna employed by the reader.[1] Tags are typically programmed with a unique identifier and a security bit, but can also contain other kinds of information, such as the book title, ISBN, library identifier, date and time stamps, and shelf locations.[2]

In libraries, RFID applications are used to automate circulation and collection management tasks. Systems developed by RFID vendors can now check in, sort, and deliver items to a designated shelving cart. Tags affixed to books, periodicals, CDs, DVDs, and other library items identify circulating materials, and readers can be incorporated into staff workstations, patron self-check stations, security gates, shelf readers, book drops, and automated sorting systems.[3]

RFID offers significant benefits to libraries. Because RFID tags do not require a clear line of sight and allow multiple items to be read in a stack, far less time and human effort are spent on processing materials. Patrons using RFID-enabled self-check stations and automated sorting equipment further free up library staff for essential work. Handheld RFID readers can be moved along the shelving units to read the tags attached to books on the shelves,

allowing for more efficient and frequent inventory of the library's collection. And by eliminating the need for the repetitive movements required by traditional barcode scanning technology, RFID can help reduce the incidence of repetitive stress injuries among staff and the costs associated with lost time and workers' compensation payments.[4]

As of 2009, 1,500 libraries employ RFID applications in 2,500 facilities.[5]

A Controversy in Libraryland

In October 2003, the San Francisco Library Commission approved plans to adopt RFID tags to manage its circulating collection. The decision was not expected to be controversial. A few libraries had been implementing RFID for circulation and inventory management since the 1990s without much notice or controversy, including such prominent institutions as the University of Nevada at Las Vegas, Santa Clara Public Library, and the Seattle Public Library.[6] On the day of the announcement, however, the Electronic Frontier Foundation (EFF), a civil liberties group, filed a formal statement with the commission criticizing the decision. It argued that the use of RFID tags in the library would facilitate the tracking of individuals and their reading materials and infringe on library users' rights to privacy and freedom of expression.[7]

The EFF protest came soon after a hearing convened by the California State Senate in August 2003 that aired concerns about the potential of RFID to harm individuals' privacy rights.[8] The legislative hearing was spurred, in part, by news reports about several major retailers' plans to use hidden RFID tags to monitor shoppers' behavior.[9] The announcement that the San Francisco Public Library would be placing RFID tags on its books and audiovisual materials drew the attention of EFF and placed the issue of RFID and library users' privacy before the public.

Other civil liberties and privacy groups soon joined EFF's campaign to oppose the use of RFID tags in the San Francisco Public Library. In January 2004, Beth Givens of the Privacy Rights Clearinghouse and Pam Dixon of the World Privacy Forum attended the American Library Association's 2004 Midwinter Meeting with EFF's senior counsel, Lee Tien. The trio presented their concerns about the use of RFID in the library to the ALA Intellectual Freedom Committee and asked that ALA assess RFID technologies and their potential to harm library users' privacy rights.[10]

The Library Community Responds

Privacy advocates' claims that the RFID tags in libraries posed an unacceptable risk to borrowers' privacy elicited divergent responses from the library profession.

VTLS, a vendor of library RFID technologies, published a white paper setting out the arguments in favor of implementing RFID in libraries and explaining why privacy advocates' claims were unfounded. The article emphasized three main points:

- RFID tags used in library applications do not have an embedded power source and are inactive unless they are within the range of a reader.
- RFID tags used in library applications have a very short read range of 18 inches.
- RFID tags store only data that is equivalent to bar codes. No personally identifiable information is kept on the tag.[11]
- Library technology consultants, systems librarians and other vendors also defended RFID. They argued that RFID offered adequate security for library users' privacy and maintained that RFID was an inefficient and labor-intensive method for surveilling patrons' reading choices.[12]
- Other librarians and experts examining RFID were not so sanguine. They acknowledged the enormous benefits that could be realized by implementing RFID technologies in the library, but concluded that library RFID applications raised significant privacy concerns. They identified several problems:
- The security flaws that allow RFID tags to be read by any reader are part of the tag's architecture and cannot easily be remedied.
- Claims that the RFID tag's short read range prevents illicit surveillance ignore the trajectory of technology improvements; RFID readers can be expected to improve and become more powerful within a fairly short time period.
- Similarly, while the infrastructure to support surveillance of library RFID tags outside the library may not yet exist, increasing implementation of RFID technology in both government and commercial applications and the rise of pervasive and ubiquitous computing will eventually make such surveillance a realistic possibility.[13]

The core issue, in the view of these librarians, is RFID's potential to become a means of surveilling library users.[14] Any technology that facilitates surveillance of a patron's activities and reading habits raises significant ethical issues for a profession committed to protecting the library user's right to privacy.

Privacy Concerns Inherent in RFID Applications

The characteristics that make RFID tags so useful for circulation and collection management in libraries—the ability to uniquely identify a single item and transmit that data wirelessly when interrogated by a reader—are precisely the

characteristics that raise significant privacy and security concerns about the use of RFID in libraries. Tags attached to books can transmit the data stored on the tag without being observed and without the knowledge of the person possessing the book. If the tag is read at different times or in different locations by a compatible reader, then the person's activities and locations can be identified, tracked, and compiled without that person's knowledge.

In commercial and retail uses of RFID tags, these privacy concerns could be addressed by deactivating or removing the tag from the item. Library RFID applications, however, require that the tag on the book remain live so that the tag can be reused to charge the book in and out of the library and to inventory the book.[15]

In 2004, electrical engineers David Molnar and David Wagner investigated the privacy risks associated with the two types of tags used for most library RFID applications, tags compliant with ISO 15693 and ISO 18000-3, the standards established by the International Standards Organization (ISO) to define the physical interface and commands for RFID tags and readers operating at a frequency of 13.56 MHz. Their research identified five possible means of compromising the privacy of library users:

- Library RFID tags do not employ passwords or other access controls, and can be read at will. Thus, any information stored on the tag can be skimmed by any RFID reader that complies with the tag's protocols. The greater the amount of information on the tag, the greater the possibility of identifying the particular book or the person in possession of it.
- Even with minimal information on the tag, a reader can be used to obtain the tag's primary identifier. The unique number can then be used to track or monitor the movement of the book attached to the tag and the person possessing it.
- One surveillance exploit acquires a tag's unique identifier in advance to create a "hotlist" of books, then monitors all tagged items leaving the library or passing through a particular checkpoint to discover who is carrying the hotlisted book.
- Tracking and hotlisting can occur even if a password or other security measure is used to secure the data on the tag. RFID tags employ a unique identifier at the hardware level, the collision avoidance ID, that prevents the tag from interfering with other tags' radio signals. The collision avoidance ID is broadcast any time a tag is interrogated by a reader and can be used to track or hotlist the tag.
- Finally, it is possible to eavesdrop on the wireless communication between the tag and the library's tag reader unless the communications are encrypted.[16]

All of these exploits require that the device used to read the RFID tag be within the tag's read range; for library RFID tags, that range is generally about two meters but can be as high as 3.5 meters, depending on the power of the reader.[17] Thus, while scenarios that envision tracking books via readers mounted to cars or aircraft are not possible, the read ranges for library RFID tags are sufficient to allow surreptitious reading by devices concealed in doorways, walls, and furnishings located in close environments.[18] And while the current lack of an RFID infrastructure attenuates the privacy threats posed by these exploits, evolving technology and the growing adoption of RFID could quickly make these threats real.[19]

Professional Ethics and Privacy-Invading Technologies

Librarians have long recognized that privacy is essential to freedom of inquiry. If individuals know or suspect that their intellectual activities are subject to examination by the government or other third parties, they are unlikely to fully exercise their constitutional right to read and receive ideas, information, and points of view.

The ALA Code of Ethics thus explicitly calls on librarians to protect the library user's right to privacy and confidentiality. This obligation requires librarians to uphold and protect the right to privacy and confidentiality in the library by adopting policies, procedures, and practices that reinforce and confirm library patrons' belief that their library use will be kept confidential and free from unauthorized scrutiny.

RFID, with its potential for compromising library users' privacy, therefore presents a significant ethical challenge for libraries. The resolution of such challenges does not require that libraries forgo or abandon new technologies. Rather, it requires librarians to seek out information about the new technology; understand its benefits, risks, and problems; and identify and resolve potential policy tradeoffs before implementing the technology.

In the wake of the controversy over San Francisco Public Library's decision to adopt RFID, librarians Karen Schneider and Lori Ayre criticized libraries for implementing RFID without thoroughly examining the technology and its potential problems. Schneider urged librarians to undertake a searching review of RFID that emphasized protecting user privacy and security while providing for full disclosure and accountability on the part of the library.[20] Ayre argued that the library community needed to ensure that adoption of RFID was done in a manner consistent with established privacy principles, as libraries' use of RFID would serve to legitimize the use of the technology in the wider society.[21] Both authors urged librarians to develop best practices for library RFID applications

that would model an ethical approach to RFID that preserves user privacy.

Privacy Guidelines and Consensus

In response to the appeals from privacy advocates and librarians concerned about RFID's impact on library users' privacy, ALA's Intellectual Freedom Committee (IFC) and Office for Information Technology Policy (OITP) committed to identifying key privacy issues associated with RFID and to work with interest groups concerned with influencing RFID privacy protections. ALA representatives began to work cooperatively with a task force convened by the Book Industry Study Group (BISG), a trade association representing groups involved in manufacturing, publishing, and distributing books. The task force's goals were to examine issues common to booksellers, manufacturers, and libraries and to draft privacy principles for use of RFID that would guide the use of RFID by BISG's members and associated organizations.[22]

In September 2004, the task force completed its work and published its privacy guidelines as BISG Policy Statement POL-02, *Radio Frequency Identification*. These policy principles required book industry groups to adopt and enforce a privacy policy that discloses the terms of use for data collected via RFID; ensure that no personal information is recorded on RFID tags (though the policy allows a variety of transactional data); protect data by reasonable security safeguards; comply with industry best practices and relevant federal, state, and local laws; and ensure that compliance with the four principles can be verified by an independent audit.[23]

The IFC and OITP incorporated these guidelines into the *Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles* and presented the resolution to the ALA Council for adoption as a first step in addressing the ethical concerns raised by libraries' use of RFID.[24] The resolution endorsed the BISG policy statement as a whole, adopted the specific privacy guidelines contained in the BISG policy statement, and mandated that ALA develop implementation guidelines for the use of RFID technologies in libraries. The ALA Council adopted the *Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles* at the ALA's 2005 Midwinter Meeting.[25]

As directed by the council resolution, the Intellectual Freedom Committee began to develop guidelines and best practices for the use of RFID in libraries.[26] During the process, the IFC solicited comments from ALA leaders and members to ensure that the guidelines would help libraries both to benefit from RFID deployment and to protect the privacy of library users. The final document, *RFID in Libraries: Privacy and Confidentiality Guidelines*, outlined policy guidelines for libraries adopting RFID. The document offered guidance on developing written privacy policies for implementing RFID in the library and identified several key best practices:

- Notify users about the library's use of RFID technology.
- Label all RFID tag readers clearly so users know they are in use.
- Protect the data on RFID tags by using encryption, if available.
- Limit the information stored on the RFID tag to a unique identifier or barcode.
- Block the public from searching the catalog by the unique identifier.
- Store no personally identifiable information on any RFID tag.[27]

ALA's adoption of privacy guidelines and best practices for RFID provided the library community with the tools it needed to address most of the concerns of privacy advocates and library users. The fundamental recommendations for libraries implementing RFID technology—providing notice, practicing transparency, limiting the information carried on the tag, and ensuring the security of the RFID application—are now a consensus baseline. Works providing guidance for librarians considering RFID recommend that libraries implementing RFID adopt policies consistent with the 2005 *Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles* and follow the recommendations outlined in the 2006 *RFID in Libraries: Privacy and Confidentiality Guidelines*.[28]

NISO Offers A New Model for RFID in Libraries

In December 2007, the National Information Standards Organization (NISO) issued *RFID in U.S. Libraries*, authored by a working group that included four RFID vendors, two software application providers, two librarians from libraries using RFID technology, and two consultants representing book industry related organizations. The publication sets forth NISO's "Recommended Practices" to facilitate the use of RFID in library applications. According to NISO, these recommended practices are intended to be a best practice or guideline for methods, materials, or practices used by an industry and are supposed to represent a leading-edge practice, an exceptional model, or a proven industry practice.

Viewed as a "best practice" or "guideline," *RFID in U.S. Libraries* is an unusual document. In addition to its primary goal of recommending standards and a data

model to facilitate interoperability between different vendors' library RFID systems, the document offers a discussion of the benefits of RFID across the publishing supply chain. Libraries are regarded as one link in this "book publishing value chain," along with publishers, printers, manufacturers, distributors, wholesalers, retailers, and technology vendors. Consequently, the document recommends the adoption of a library RFID tag that can be used across the entire life cycle of a book or other library material, utilizing a data model that not only serves the needs of libraries, but also serves the needs of publishers, printers, wholesalers, jobbers, retailers, and even sellers of used books.[29]

As a result, the recommended data model includes fields for many optional data objects in addition to the mandatory primary identifier or barcode used by libraries. Among these are fields for the title of the work, an ISBN or UCC code, shelf location or call number, the supply chain stage, a supplier ID, order and invoice numbers, and supplier identification data. To ensure the future utility of the tag, the data model mandates that no controls be placed on any current or future use of these data fields, so that conceivably a book's RFID tag could provide information about the book's title, the owning library, and its bibliographic information, all without accessing the library's integrated library system (ILS).

The document also examines and assesses the privacy concerns associated with the use of RFID technologies. As a document intended to offer "best practices" for library RFID applications, its discussion of privacy issues is notable for what it does not contain:

- The document does not consider or discuss the unique privacy concerns of the U.S. library, which loans materials to patrons with a promise of confidentiality.
- It fails to reference the primary ALA statement addressing RFID implementation in libraries, *RFID in Libraries: Privacy and Confidentiality Guidelines*.
- It does not discuss fundamental recommendations such as the recommendation that libraries store only a unique identifier or barcode on the RFID tag in order to protect user privacy.

Instead, the document minimizes privacy issues associated with RFID as "mostly science fiction" and reprints, nearly verbatim, the VTLS-sponsored white paper published back in 2003 as a response to privacy advocates' concerns about RFID in the library.[30] The sole recommendation is that RFID tags comply with the privacy guidelines contained in *BISG Privacy Policy POL-002*, with an emphasis on the provision that no personal information is recorded on RFID tags.[31]

This lone recommendation is accompanied by a brief history of BISG Privacy Policy POL-002 that presents the BISG policy as the result of a joint ALA/BISG initiative and as the sole policy concerning privacy and RFID adopted by ALA. Internal ALA documents, such as reports from the ALA Intellectual Freedom Committee and the full text of the *Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles* provide a different account. These documents identify the policy as an initiative of the Book Industry Study Group and clarify that the endorsement of the BISG policy as a whole and the adoption of portions of the BISG policy were part of a larger effort that called for the development of specific RFID privacy guidelines for the library profession.[32]

As with the recommended data model, the privacy recommendations contained in *RFID in U.S. Libraries* reflect the needs of the commercial entities that make up the supply chain and not the needs and concerns of libraries and librarians. The minimal privacy standards recommended by the NISO document support commercial RFID applications that require greater amounts of data to be stored on the tag. Library-specific privacy standards that recommend limiting the data on the tag to a unique identifier, such as ALA's *RFID in Libraries: Privacy and Confidentiality Guidelines*, are neither considered nor included as a recommended practice because they are seen as a barrier to the adoption of an RFID tag that can be used across the publishing supply chain.

Conclusion

The discussion of privacy issues included in *RFID in U.S. Libraries* suggests that a deep divide exists between the library profession and the members of the working group responsible for drafting *RFID in U.S. Libraries*. The working group appears to not fully share librarians' concern about RFID's potential to invade library users' privacy, nor does it appear to accept librarians' own assessment of the role of libraries in society. As a result, the data models and recommended privacy practices promulgated for libraries look to future commercial use of RFID technologies by publishers, manufacturers, wholesalers, and retailers.

This result calls to mind the political and economic theory known as "regulatory capture," a model in which government regulation reflects the influence of special interests, and operates for their benefit.[33] The standards and privacy recommendations contained in RFID in U.S. Libraries reflect the influence of the vendors, software providers, and book industry advocates that dominate the working group, and appear to serve their interests at the expense of librarians' ethical concerns and obligations.

Librarians thus need to ask whether standards and best practices that regard libraries as part of a retail

supply chain serve the best interests of libraries and their users. Libraries are not retail establishments, and librarians are not sales clerks. Rather, libraries are institutions whose mission is to serve the public good by making available information and ideas, and librarians are professionals who assure access to that information by defending the freedom to read and the right to privacy. Best practices for RFID in the library should not only facilitate use of the technology but also promote the library's distinctive mission and preserve users' privacy rights. They should not be compromised in order to serve the needs of vendors, manufacturers, wholesalers, retailers, and publishers, whose mission is to maximize profits on behalf of their shareholders.

Furthermore, librarians must ask whether recommended best practices for library RFID applications should look forward to uncertain future uses of RFID in the publishing supply chain, or address the present uses and known privacy and security vulnerabilities of library RFID tags. This inquiry is especially important given the publishing industry's slow adoption of RFID technology and libraries' increasing emphasis on e-books and other online media downloads that make no use of RFID. Standards and recommended practices can be revised and re-written to accommodate new RFID applications, but privacy, once lost, is not easily recovered.

In making these points, I do not mean to imply that librarians should not work with the book industry on establishing data models for library RFID applications or should forgo consideration of an RFID tag that can be used across various industries and organizations and permit interoperability between library RFID applications. Instead, librarians should assume a leadership role in developing best practices and standards for RFID, both inside and outside the library, as part of their ethical obligation to protect library users' privacy. Such standards should make privacy protection a primary goal, and not a secondary goal, when implementing RFID. This is especially important in the United States, where, with minor exceptions, there are no statutes or regulations that govern the use of RFID technologies.[34]

In a 2003 interview, librarian Karen Schneider eloquently summarized the challenge RFID poses for the library profession:

> What are we witness to as librarians? We have a chance here—not simply on behalf of library users and librarians, but also for society at large—to present an ethical approach to RFID and similar technologies, to actually present a framework for how to do this and preserve privacy in an increasingly non-private world. And conversely, if we don't develop best practices, I think we are acceding to an increasingly commercialized, non-private world and we're losing the opportunity to do something that we've done very well, which is to find intellectual freedom and privacy issues in a particular technology and speak to them very clearly a way that the public can understand.[35]

Her concerns remain relevant today.

Notes

1. Lori Bowen Ayre, "Wireless Tracking in Libraries: Benefits, Threats, and Responsibilities," in RFID: Applications, Security, and Privacy, ed. Simson Garfinkel and Beth Rosenberg, 229–243 (Upper Saddle River, NJ: Addison-Wesley, 2005); Alan Butters, "RFID Systems, Standards, and Privacy within Libraries," The Electronic Library 25, no. 4 (2007): 430–439; David Molnar and David Wagner, "Privacy and Security in Library RFID Issues, Practices, and Architectures," in Proceedings of the 11th ACM Conference on Computer and Communications Security, ed. Birgit Pfitzmann and Peng Liu, 210–219 (New York: ACM, 2004).
2. Ayre, "Wireless Tracking in Libraries"; Laura Smart, "Considering RFID: Benefits, Limitations, and Best Practices," College and Research Library News 66, no. 1 (Jan. 2005): 13–16, 42.
3. Alan Butters, "Radio Frequency Identification: An Introduction for Library Professionals," Aplis 19, no. 4 (2006): 164–174.
4. Richard W. Boss, RFID Technology for Libraries, June 30, 2009. www.lita.org/ala/mgrps/divs/pla/plapublications/platechnotes/rfidtechnology.cfm (accessed Aug. 10, 2010); Karen Schneider, "RFID and Libraries: Both Sides of the Chip,"(testimony presented at the Committee on Energy and Utilities, California Senate, Nov. 19, 2003), www.ala.org/ala/aboutala/offices/oif/ifissues/rfidbothsideschip.pdf (accessed Sept. 14, 2010).
5. Boss, RFID Technology for Libraries.
6. Smart, "Considering RFID."
7. Electronic Frontier Foundation, "Statement to the San Francisco Library Commission," Oct. 1, 2003, www.eff.org/files/filenode/rfid/sfpl_comments_oct012003.pdf (accessed Sept. 14, 2010).
8. Alorie Gilbert, "California Probes RFID Technology," Globe and Mail, Aug. 11, 2003.
9. David Ewalt, "Wal-Mart Shelves RFID Experiment," Information Week, July 14, 2003.
10. Office for Intellectual Freedom, Intellectual Freedom Manual, 8th ed. (Chicago: American Library Association, 2010).
11. Vinod Chachra and Daniel McPherson, Personal Privacy and Use of RFID Technology in Libraries, Oct. 31, 2003, www.vtls.com/media/en-US/brochures/vtls_fastrac_privacy.pdf (accessed Sept. 14, 2010).
12. Boss, RFID Technology for Libraries; Butters, "RFID Systems, Standards, and Privacy within Libraries"; David Dornan, "Technically Speaking: RFID Poses No Problem for Patron Privacy," American Libraries, Dec. 2003: 86.
13. Walt Crawford, "Technology, Privacy, Confidentiality, and Security," in "Policy and Library Technology," Library Technology Reports 41, no. 2 (March–April 2005): 24–30;

Schneider, "RFID and Libraries"; Smart, "Considering RFID."
14. Ibid.
15. Molnar and Wagner, "Privacy and Security in Library RFID Issues"; Scott Muir, "RFID Security Concerns," Library Hi Tech 25, no. 1 (2007): 95–107.
16. Molnar and Wagner, "Privacy and Security in Library RFID Issues."
17. Butters, "RFID Systems, Standards, and Privacy within Libraries."
18. Butters, "Radio Frequency Identification"; Molnar and Wagner, "Privacy and Security in Library RFID Issues."
19. Smart, "Considering RFID."
20. Schneider, "RFID and Libraries."
21. Ayre, "Wireless Tracking in Libraries."
22. Office for Intellectual Freedom, Intellectual Freedom Manual.
23. Book Industry Study Group, Radio Frequency Identification, BISG Policy Statement POL-002, Sept. 2004, www.bisg.org/docs/BISG_Policy_002.pdf (accessed Sept. 14, 2010).
24. "History: RFID in Libraries: Privacy and Confidentiality Guidelines" in Intellectual Freedom Manual, Eighth Edition, compiled by the Office for Intellectual Freedom,288-292 (Chicago: American Library Association, 2010).
25. Ibid. at 289-90; see also "Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles," Jan. 19, 2005, www.ala.org/ala/aboutala/offices/oif/statementspols/ifresolutions/rfidresolution.cfm (accessed Sept. 19, 2010).
26. Ibid. at 291–292.
27. Ibid.; see also 284–287.
28. Connie K. Haley, Lynne A. Jacobsen, and Shai Robkin, Radio Frequency Identification Handbook for Librarians (Westport, CT: Libraries Unlimited, 2007); Diane Marie Ward, The Complete RFID Handbook (New York: Neal Schuman, 2007).
29. National Information Standards Organization, RFID in U.S. Libraries, NISO RP-6-2008, Dec. 2008, www.niso.org/apps/group_public/download.php/116/RP-6-2008.pdf (accessed Sept. 14, 2010).
30. Chachra and McPherson, "Personal Privacy and Use of RFID Technology;" NISO, RFID in U.S. Libraries, 37.
31. NISO, *RFID in U.S. Libraries*, viii, 37-40.
32. *Intellectual Freedom Manual*, 288-292.
33. Michael E. Levine and Jennifer Forrence, "Regulatory Capture, Public Interest, and the Public Agenda: A Synthesis," *Journal of Law, Economics, and Organization*, 6, special issue 1990, 167–198.
34. Thirteen states have adopted laws regulating RFID use in drivers' licenses and other identity documents and human implantation. Four states criminalize the unauthorized skimming of RFID-enabled identity cards if done for a criminal purpose. (See National Conference of State Legislatures, State Statutes Relating to Radio Frequency Identification (RFID) and Privacy, Sept. 2010, www.ncsl.org/default.aspx?tabid=13442n [accessed Sept.19, 2010].)
35. Gordon Flagg, "Should Libraries Play Tag with RFIDs?" (2003) *American Libraries*, December, 69–71.