The Samuelson Law, Technology, and Public Policy Clinic (the Clinic) at the University of California-Berkeley's Boalt Hall School of Law
Library Best Practices

The Clinic's best practices for RFID are based on the Code of Fair Information Practices[1], and are organized accordingly by data disclosure, collection, retention, security, and notice and permission concerns.[2]

1. **Provide notice to library patrons.**
    a. RFID tags should be clearly labeled. *Patrons have a right to know that the books they carry emit data to nearby readers. Libraries may choose to evaluate this issue in light of concerns that patrons may attempt to tamper with clearly marked tags.*
    b. The library should publicly disclose that it deploys an RFID system and describe its capabilities. *Patrons and the public at large have a right to know about data collected from them and data they carry on their persons. Such disclosure also affords an opportunity to educate the public about the risks and benefits of RFID technology.*

2. **Prevent unauthorized disclosure of the subject of inquiry and other associational data.**
    a. The RFID tag should not contain data describing the article to which it is attached. *Title, author, genre, language, etc. all disclose the subject of inquiry.*
    b. The RFID tag's transmission range should be limited. *The greater the broadcast range, the more susceptible each article is to surreptitious reading.*
    c. The RFID tag's data should be encrypted at best or formatted according to a unique protocol at least, in order to make reading of information by third parties more difficult. *At present, not all tags and readers are interoperable; however, libraries should plan for standards-based scenarios in which all tags can be read by all readers.*
    d. Libraries should maintain secure control over the tag writing process in order to prevent tagging of unauthorized information. *This could include requiring a password before allowing a tag to be written to and transaction logs for writes to tags. Unauthorized writing to RFID tags may pose many threats to the privacy of the patron. For example, location information could be surreptitiously written to tags, allowing tag readers to effectively track a tagged item.*

---

[1] *See infra* note 15.
[2] For other examples of best practices for RFID use in libraries, *see* "Berkeley Public Library, Best Practices for RFID Technology," *available at* http://www.berkeleypubliclibrary.org/BESTPRAC.pdf; Beth Givens, "RFID Technology in Libraries: Some Recommendations for 'Best Practices,'" presentation to ALA Intellectual Freedom Committee, Jan. 10, 2004, San Diego, California, *available at* http://www.privacyrights.org/ar/RFID-ALA.htm

e. The RFID tag should not contain data describing its origin or lending institution. *Library patronage is an associational choice that should be protected. Lender data also provides location information about the patron. Libraries may need to balance competing goals regarding materials management and interlibrary loans with this concern.*
f. The RFID system should not pre-label tags with information that would allow identification of the deploying library. *As described above, this information can invade patron privacy when readable in public.*[3]
g. If the RFID tag contains sorting and reshelving information, this information should consist only of an identifying number that requires an internal look-up in the Library information system to provide shelf location. *Shelving information serves to help identify the item. This recommended practice is part of the larger and more general information-privacy principal—the best way to maintain control over data is to keep it in only one place, the centralized library database, and distribute references to that data instead of the data itself.*
h. The RFID identifying number should not employ standardized labeling protocols such as ISBN or EPC-like labeling systems. *Standardized protocols for labeling disclose the subject of inquiry.*
i. The RFID system should only allow unique identification of holdings within the deploying library. *Consistent identifiers across libraries and/or library systems would make it easier to deduce article identity.* Stated another way, RFID labeling systems should maximize redundancy between identifying numbers *but not the associated articles* at different libraries. Control of this factor may reside with vendors (where they sell pre-programmed tags) or with libraries (where they program their own).
j. The unique identifier assigned to the artifact should not embed information that can be used to infer or derive any of the above.
k. When implementing wireless transmission between readers and the ILS, the RFID systems should use established methods of secure, encrypted transmission. *Remote log-in to library information systems and reader console machines should be deactivated. If active, all transmissions should be encrypted with SSH or similar technology rather than non-encrypted forms of transmission such as Telnet or FTP.*

2. Prevent disclosure of personal identifying information.

a. The RFID tag should not contain or accumulate data about the borrower.
b. The RFID tag should not contain information about the lending transaction. *Date, time, and branch data help track patrons' movements.*
c. Security gates which read information from RFID tags should not log that information, unless a security risk has been detected, such as the book not being cleared for removal from the library. If a security gate does log

[3] To some extent this already takes place with perceivable media such as due date stamps and imprinted dust covers. However, the wireless nature of RFID tag reading poses the possibility that origin and residence information could be read without a patron's knowledge or consent. By contrast, a patron can easily tell when an individual is close enough to read visual labels on the book.

information, it should retain it for only so long as necessary to achieve security goals.

3. **Minimize collection of unnecessary data.**
   a. The RFID system should allow libraries to wholly control what information is written to tags. *In-house programming permits the library to maintain complete control over identifying information.* Libraries must weigh this goal against any potential efficiency from purchasing pre-programmed tags.
   b. Libraries should write minimal information onto tags—only one unique identifying number in non-standardized format (ideally, encrypted).
   c. The RFID tag should probably not contain excess user-programmable memory. *The best-practice label requires only an ID number. Extra memory provides a platform for encoding unnecessary data. However, the library must balance this risk with the benefit of extensibility.*
   d. Libraries should train staff in how to use portable readers in ways protective of patron privacy, and limit portable reader search lists to required items. *Portable readers can invade the privacy of patrons reading in the library by detecting books in their proximity.*
4. **Minimize retention of unnecessary data.**
   a. RFID providers should not retain pre-programmed labeling information following the sale of tags. *All identifier information should stay behind library firewalls. This issue does not arise where libraries program their own tags and all data other than the unique identifier is maintained in a database behind the library firewall.*
   b. RFID check-out consoles and portable readers, when possible, should not cache information. *In cases where the library chooses to activate caching, risks to patron privacy should be made explicit to both library staff and patrons. Moreover, that information should be stored and transmitted securely, based on established information systems security practices.*
5. **Keep data collections secure.**
   a. RFID tags and readers should ideally authenticate each other before data is communicated. *This would prevent tags from responding to data requests from unauthorized readers. Likewise mutual authentication would prevent readers from eliciting responses from third party tags.*
   b. Libraries should institute access control to portable readers—password protection and checkout procedures. *Readers may contain and collect sensitive item-specific information.*
   c. Libraries should adjust ILS security to guard against increased threats from interoperation between the RFID system and the circulation and patron registration database.