EVALUATION FRAMEWORK

A. Efficiency Requirements

The vendor proposals focus on meeting the Library's efficiency needs. This section summarizes these proposals in order to frame the subsequent review of privacy implications.

i. Any RFID System adopted should allow unique identification of holdings within a given library.

As a basic requirement, any inventory system should allow the library to identify each holding and distinguish it from other holdings.

ii. Any RFID System adopted should reduce repetitive physical labor.

Library administration and maintenance require certain physically repetitive tasks which, over time, tend to cause physical injury. For example, checking-in and checking-out library holdings involve repetitive wrist motions which can result in carpal-tunnel syndrome. RFID tagging systems promise to reduce and in some cases eliminate the extent to which some of these types of tasks are required. Accordingly, any prospective RFID system should meet this goal.

iii. Any RFID system adopted should promote overall efficiency gains.

Central among the evaluative criteria for RFID proposals are efficiency gains in managing materials flow. An investment in RFID should pay off in significant reductions in labor hours spent checking materials in and out, reshelving, as well as monitoring and processing inventory.

B. Privacy Requirements

i. Any RFID system adopted should accord with current American Library Association (ALA) and Public Library Association (PLA) policy recommendations as well as state and federal law concerning patron privacy and confidentiality.

The ALA has articulated clear principles and policy goals for the role libraries should play in promoting freedom of inquiry and protecting the privacy of all patrons. These principles require safeguarding not only personal identifying information, but also the subject of each patron's inquiry. In an Interpretation of the Library Bill of Rights, the ALA instructs that "[i]n a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others."[1] To this end, "[r]egardless of the technology used, *everyone* who collects or

[1] Privacy: An Interpretation of the *Library Bill of Rights*, ALA, *available at* http://www.ala.org/ala/oif/challengesupport/dealing/privacyinterpretation.pdf. This document also states,

accesses personally identifiable information in any format has a legal and ethical obligation to protect confidentiality." In the traditional library this burden rested with a library's administration. In the RFID-enabled library, the "everyone" in question expands to potentially encompass anyone in the outside world, as well.

State law also governs how libraries must manage information. California Government Code Section 6267 forbids public libraries from disclosing registration or circulation information.[2] Deploying RFID tags could potentially disclose information to any individual, group, or government agency with an RFID reader.

To promote libraries' essential mission, comply with the law, and continue libraries' role as gatekeepers between readers and those who seek information about reading habits, librarians should examine each proposed RFID system with detailed attention to privacy concerns and how they are affected by this technology.

Primary privacy threats can be categorized into:

(1) Threats to stored data (RFID tags and data collections).

- Surreptitious tag reading by third parties in public or within the library. *Many privacy threats associated with RFID arise essentially from the distribution of labeling information with books that accompany library patrons from the library and out into everyday life. These risks include, for instance, tracking patrons as they carry RFID tagged materials and associating patron with particular library*

"All users have a right to be free from any unreasonable intrusion into or surveillance of their lawful library use …. Users have the right to use a library without any abridgement of privacy that may result from equating the subject of their inquiry with behavior." Similarly, an ALA policy asserts that "[t]he First Amendment's guarantee of freedom of speech and of the press requires that the corresponding rights to hear what is spoken and read what is written be preserved, free from fear of government intrusion, intimidation, or reprisal." ALA Policy Concerning Confidentiality of Personally Identifiable Information about Library Users, *available at* http://www.ala.org/ala/oif/statementspols/otherpolicies/policypersonallyidentifiable.pdf.

[2] Cal. Gov. Code § 6267 (West 2004). The provision reads in full:

> All registration and circulation records of any library which is in whole or in part supported by public funds shall remain confidential and shall not be disclosed to any person, local agency, or state agency except as follows:
>
> (a) By a person acting within the scope of his or her duties within the administration of the library.
> (b) By a person authorized, in writing, by the individual to whom the records pertain, to inspect the records.
> (c) By order of the appropriate superior court.
>
> As used in this section, the term "registration records" includes any information which a library requires a patron to provide in order to become eligible to borrow books and other materials, and the term "circulation records" includes any information which identifies the patrons borrowing particular books and other material.
>
> This section shall not apply to statistical reports of registration and circulation nor to records of fines collected by the library.

There is no case law on § 6267.

materials. Surreptitious reading of RFID tags by third parties is therefore a significant threat.

- Intra-library tag reading of patron materials by staff members using readers for searches, inventory, and other material flow management tasks (inadvertent or by unauthorized or untrained staff). *Similarly, some of the same threats to privacy manifest from reading information contained within RFID tags by unauthorized library staff or by authorized library staff for unauthorized purposes.*
- Caching of ILS record information at portable RFID check-in / out stations. *Some RFID vendors advertise that their check-out stations are capable of operating even while disconnected from the ILS. This is accomplished by caching some patron and library inventory information locally. While this feature adds potential convenience during ILS system outage, it also provides another information repository which must maintain library standards for protecting information.*
- Caching of ILS record information at portable RFID hand-held readers. *By their functional nature portable RFID readers must be capable of storing some library record information. As with portable checkout stations, library administrators should take caution to ensure that the data contained within these devices meets minimum standards of ILS security.*

(2) Threats to data during transmission.

- Eavesdropping on reader / tag correspondence
Data is at risk of unauthorized access while in transmission between reader stations and tags. RFID is by definition a wireless technology. As such, all transmissions are broadcast in nature. Listening device placed within proximity of such transmission may be able to eavesdrop on those transmissions without detection by either reader or tag.
- Eavesdropping on reader / ILS correspondence
Likewise, some vendors may offer wireless enabled check - out stations and portable readers. Although the WEP cryptographic techniques used by 802.11b wireless protocol to protect transmissions are sufficient for many purposes (such as keeping out accidental eavesdroppers with no intent to eavesdrop), they have been proven to be insecure against determined eavesdroppers. Because wireless communication involves broadcasting communications, eavesdroppers may potentially access information transmitted between readers and the ILS. Stronger protection than WEP, such as VPN, is preferred. These risks exist with wired transmission in addition to wireless transmissions and they are already present for other library systems. Nonetheless RFID systems adds another set of vulnerabilities and are thus worthy of mention.

(3) Threats concerning transparent data labeling practices.

- Standardization threat
If labeling formats for RFID are standardized, private information embedded on these tags may be read by many readers other than library authorized ones.
- Reverse-lookup books by bar code.

Using local data formats protects privacy only to the extent that those formats prevent linking with ILS data records. Providing reverse-lookup features for library holdings would negate any privacy protection afforded by in-house labeling format. For example, the use of bar codes on RFID tags creates the following possible scenario for a library that allows patrons to use the bar code to look up books: a third party reads the RFID tags in a patron's backpack, goes to the kiosk, and looks up the bar codes. The patron's right to read anonymously is compromised.

- Vendor identity
  Some RFID tag vendors may be identifiable by labeling formats used within their tags. This is a threat to privacy. Once data seekers identify an RFID vendor, they can research the vendor's customers to identify the deploying library, thus creating an association between the individual carrying the book and the lending library.
- Compiling directories of RFID labeling information.

i. Mapping bar codes directly to RFID
Mapping bar codes directly to RFID threatens privacy because there has been and continues to be ample opportunity for a data seeker to compile tables documenting the correspondence between visually discernible bar code labels and book identity. With such a table, permanent unique ids on RFID tags could easily be translated into book identity. (See also above comment under reverse lookup.)

ii. Inter-Library Lending
Inter-library loans (ILL) present an interesting problem when evaluating the pros and cons of standardization of RFID tagging systems. On one hand, standardized labeling would allow borrowing libraries to read and categorize books with partner libraries without redundancy. However, standardizing intra library labeling also poses the severe privacy risk that understanding the labeling system for one library could enable understanding the labeling system for all libraries.

ii. Requirements. In order to protect patron privacy, an RFID system should:

1. Prevent 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 transmission range while writing to tags and checking materials in and out should be limited. *Shorter transmissions reduce the risk of eavesdropping on data exchange.*

d. The RFID tag's data should be encrypted at best or locally formatted 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 a standards-base scenarios in which all tags can be read by all readers.*

e. Libraries should maintain secure control over the tag writing process in order to prevent programming of inappropriate information. *This could include password protection, user authentication by encoding equipment, and transaction logs. Unauthorized writing to RFID tags may cause many threats to the privacy of the patron. In one example, location information could be written to tags such that those tags could contain information concerning where they've been.*

f. The RFID tag should not contain data describing its origin or residence (lending institution). *Library patronage is an associational choice that should be protected. Lender data also provides localizing information about the patron. Libraries may need to balance competing goals regarding materials management and interlibrary loans.*

g. The RFID system should not pre-label tags with information which would allow identification of the deploying library. *As described above, this information an invade patron privacy when readable in public. To some extent this already takes place with perceivable media such as due date stamps and imprinted dust covers. However, the inherently concealed nature of RFID tag reading poses the possibility that origin and residence information could be read without a patron's knowledge or consent.*

h. 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 Internal Library System (ILS) 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— to maintain control over data, keeping it in one place the database and distribute references to that data instead of the data itself.*

i. The RFID identifying number should not employ standardized labeling protocols such as ISBN or EPC-like labeling systems. *Standardized protocols for labeling facilitate universal correlation of RFID tagging information to book and patron identifiers as well as other private information.*

j. 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).

k. Libraries should consider purchasing an RFID system with rewritable tags in order to allow the library to change identifier information as necessary to keep the article it references confidential; but should be careful to maintain control over the rewriting process. *On one hand, the longer a given article bears the same identifier, the more likely are third parties to* *be able to identify the item by surreptitious reading of the tag. On the other hand, rewritable tags may threaten inventory management if tags can be rewritten by anyone, not only library agent. This could also seriously threaten patron privacy. See Requirement e, above.*

i. The RFID system should give libraries the capability to quickly and efficiently rewrite tags as materials are returned, using a locally designated labeling format for identification.

l. The unique identifier assigned to the artifact should not embed information that can be used to infer or derive any of the above.

m. When implementing wireless transmission between readers and the ILS, the RFID systems should use established methods of secure, encrypted transmission. *Remote log-in to ILS 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 patron's 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 clear for removal from the library. If a security gate does log information, it should retain it only for as 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.

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 danger with the benefit of forward compatibility for future applications which require additional memory.*

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 manufacturers 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 in ways secure according to established information systems practices. Access to the information should be limited to authorized persons.*

5. Keep data collections secure.

a. RFID tags should employ technology to protect data from being overwritten by third parties.

b. 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 tags they were not supposed to.*

c. Libraries should institute access control to portable readers—password protection and checkout procedures. *Readers may contain and collect sensitive item-specific information.*

d. Libraries should adjust ILS security to guard against increased threats from constant interface between the RFID system and the circulation and patron registration database.

6. Be transparent 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 what its capabilities are. *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 on the risks and benefits of RFID technology.*