RFID Workshop - Comment, P049106
The Samuelson Law, Technology, and Public Policy Clinic (the Clinic) at the University of California-Berkeley's Boalt Hall School of Law

Federal Trade Commission Public Workshop
Radio Frequency Identification: Applications and Implications for Consumers

We file this comment to emphasize the privacy issues related to tagging of information goods such as books, CDs, and DVDs. The potential for surveillance inherent to RFID technologies is uniquely invasive in the information goods context. Individuals have strong expectations of personal privacy in their choice of information goods, which are reinforced by social norms, public policy, and law. While the privacy issues in information goods are particularly keen, large-scale item level tagging has already begun. More than 130 libraries in North America have tagged their holdings, including books, music, and video, at the item level.[1] Libraries thus provide a useful case study to examine the actual risks to privacy posed by RFID in one context. There is reason to believe that item level tagging of information goods will expand into the retail space and will increase dramatically in coming years.[2] For these reasons it is important to assess these privacy threats and to take appropriate technical and policy measures.

In this comment, we examine briefly the normative, legal, and policy connections between privacy, the First Amendment, and information goods. We distinguish the treatment of information goods in the retail and library settings and describe the technical differences between tags and readers used in each setting. Next we describe the threats to privacy created by the introduction of RFID into these settings. We describe our work with the Berkeley Public Library as a case study. In conclusion we recommend that the FTC (1) conduct a special workshop for the use of RFID with information goods to more carefully assess the implications in this unique environment, and (2) develop a guideline for RFID use that clarifies which practices may be deceptive or unfair.

2.0 Information Goods, Institutional Norms, Individual Expectations, and Law

Individuals have strong expectations of privacy in their choice of information content for reading, listening, and viewing. These norms are reflected in the culture and policies of institutions that provide information goods, as well as statutory and constitutional protections.

[1] As of mid-2003, approximately 200 libraries had installed RFID systems. Large-scale implementations include the University of Connecticut, the University of Nevada, and the Las Vegas Library in the U.S., along with the Vienna Public Library, the Catholic University of Leuven in Belgium, the National University of Singapore, and the Netherlands Library Service. Richard W. Boss, RFID Technology for Libraries; Radio Frequency Identification Systems, 39 Library Technology Reports (Vol. 6) 1 (2003); *see also* RFID in Libraries, *at* http://libraryrfid.typepad.com/libraryrfid/ (a weblog tracking current library RFID implementations).

[2] Some grocery outlets have begun to adopt the technology in Germany (see http://www.topix.net/tech/rfid), and in England (http://www.rfidjournal.com/article/articleview/658/1/1/); Industry analysts predict widespread adoption of item level retail RFID tagging by 2005 – 2008 (see http://www.ftc.gov/bcp/workshops/rfid/boone.pdf)

Individuals' expectations of privacy when buying or borrowing books, music, and film stem from traditional ways to access those media with relative anonymity. Currently, individuals can purchase each of these goods with cash. In cash transactions, the point of sale terminates most opportunities to discover the buyer's identity or to monitor what use the buyer makes of the work. In other settings, people can browse information on the Internet or in a library with relative anonymity.

Established public policy aligns with and reinforces these normative customs of relatively anonymous or confidential access to information. A patchwork of existing law protects the unique privacy interests in information goods from a number of would-be intrusions in various settings.[3] While the privacy protections surrounding information goods are neither complete nor uniform, taken as a whole they reflect a core policy principle: that our democratic society guarantees the right to freely speak and listen without the potential chilling effect of personal identification with the subject at hand.

2.1 The Constitution – Association with Purchase and Borrowing Records

The Constitution protects individual rights of free and private inquiry against government intrusion, through both the First Amendment's prohibition of any law that abrogates freedom of speech[4] and the Fourth Amendment's limits on government surveillance.[5] The Supreme Court has pronounced that the First Amendment protects the right to inquire freely as the logical corollary to freedom of speech: "The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read . . . and freedom of inquiry."[6] The Court has found that this right requires protecting the anonymity of speakers. As new technology capable of monitoring access to speech further develops, surveillance shifts to cover *access* to speech as well as its expression. In other words, as surveillance technology spreads in use, free speech depends increasingly on a right to read with relative anonymity.[7]

Constitutional interests in open, surveillance-free use of information limits the Government's power to discover the nature of its citizens' intellectual consumption. The Supreme Court provided a compelling example of this boundary in *United States v.*

[3] See, e.g., the Video Privacy Protection Act, 18 U.S.C. § 2710 (2002).
[4] "Congress shall make no law …abridging the freedom of speech, or of the press." U.S. Const. Amend. I.
[5] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. Amend. IV.
[6] Griswold v. Connecticut, 381 U.S. 479, 482. *See also* Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas."); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 64-65 n.6 (1963) ("The constitutional guarantee of freedom of the press embraces the circulation of books as well as their publication."); *Smith v. California*, 361 U.S. 147, 150 (1959) (stating that "the free publication and dissemination of books and other forms of the printed word furnish very familiar applications" of the First Amendment); *Martin v. City of Struthers*, 319 U.S. 141, 143 (1943) ("The right of freedom of speech and press has broad scope. . . . This freedom embraces the right to distribute literature . . . and necessarily protects the right to receive it."); *Lovell v. City of Griffin*, 303 U.S. 444, 452 (1938) (circulation of expressive material is constitutionally protected) (cited in *Tattered Cover v. City of Thornton*, 44 P.3d 1044, 1051 n.11 (Colo. 2002)).
[7] Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace,* 28 Conn. L. Rev. 981, 1010 (1996).

Rumely, holding that Congress could not compel a wholesaler of politically controversial books to disclose sales records at a congressional hearing.[8] In *Denver Area Educ. Telecommunications Consortium v. FCC*,[9] the Supreme Court struck down a statutory provision requiring subscribers of indecent cable television programming to first register in order to receive those programs. The Court found that the requirement abridged the broadcaster's speech rights and represented an unconstitutional restriction on individuals' right to view privately.[10] Further, the Court struck down a statute requiring individuals to identify themselves in order to receive controversial material, recognizing the burden such rules place on accessing information.[11]

Protection of book sales records received keen public attention in the Kramer Books-Monica Lewinsky matter.[12] In 1998, Kramer sued to stop subpoenas from Independent Counsel Kenneth Starr for Monica Lewinksi's book purchase records. The store's owner stated that it is their company policy to "not turn over any information about [their] customers' purchases."[13] Kramer was successful in blocking Starr's subpoenas. Many organizations, including the Association of American Publishers, the American Library Association, the Publishers Marketing Association, and the Recording Industry Association of America, lauded the action and announced formal support for bookstore defense of consumer privacy as a matter of policy.[14]

[8] 345 U.S. 41 (1953). Though the Court declined to rule explicitly on First Amendment grounds because the committee in question was only empowered to investigate lobbying activities and bookselling could be considered outside its scope, Justice Frankfurter noted that the statute at issue carried "the seeds of constitutional controversy" and the Court was required to construe laws to preserve their constitutionality. *Id.* at 43-45. Explaining the privacy interest at stake, Justice Douglas wrote, "When the light of publicity may reach any student, any teacher, inquiry will be discouraged." *Id.* at 57 (Douglas, J. concurring).

[9] 518 U.S. 727 (1996).

[10] "[T]he "written notice" requirement will further restrict viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the "patently offensive" channel. Id. at 754. *See also Lamont* v. *Postmaster General*, 381 U.S. 301, 307, (1965) (finding unconstitutional a requirement that recipients of Communist literature notify the Post Office that they wish to receive it); *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803 (2000) (striking down a statutory provision requiring scrambling or hours restrictions on the broadcast of adult programming and citing "the First Amendment interests of speakers and willing listeners—listeners for whom, if the speech is unpopular or indecent, the privacy of their homes may be the optimal place of receipt").

[11] *Lamont, DBA Basic Pamphlets v. Postmaster General*, 38 U.S. 301 (striking down a statute requiring the post office to ask intended recipients to confirm desire to receive Communist mail).

[12] *Supra* note 13.

[13] http://internet.ggu.edu/university_library/if/bookstore.html#challenge; The American Booksellers Association and the American Booksellers Foundation for Free Expression supported Kramer's move with an amicus brief. *Id.*

[14] Other supporters included the Freedom to Read Foundation, PEN American Center, the International Periodical Distributors Association, the Periodical Wholesalers of North America, the National Association of College Stores, the Periodical and Book Association of America, the Media Coalition, the American Civil Liberties Union, and the National Association of Recording Merchandisers. http://internet.ggu.edu/university_library/if/bookstore.html#challenge. In the Tattered Cover case, the government sought to identify the purchaser of a how-to book on making methylene through the records of a local bookstore. The bookstore won a challenge to the warrant on First Amendment grounds, the judge in the case noting that such a disclosure would implicate the expressive rights not just of the purchaser but of the entire book-buying public. *Tattered Cover v. City of Thornton*, 44 P.3d 1044 (Colo. 2002). The Colorado Supreme Court described the constitutional interest in information goods thus: "Bookstores are

2.2 Legislation – Association with Purchase and Borrowing Records

Congress and state legislatures have created a variety of industry-specific statutes that shield records of individual inquiry from disclosure to public and private parties alike. These laws are generally based on Fair Information Practices and limit the collection, retention, and disclosure of data.[15]

Overall, the statutory protections for information about individual use of information goods are both stricter and more specific than other statutory privacy protections. This reflects the heightened sensitivity to the expressive interest in information goods. For example, at the federal level, the Cable Television Privacy Act of 1984 protects cable television subscribers from unfair data collection and use,[16] and the Video Privacy Protection Act protects video rental records from release without a court order.[17] Similar laws at the state level protect library check-out and circulation information from release with without a court order in 48 states.[18] The remaining two states have published legal opinions supporting the privacy of library borrowing

places where a citizen can explore ideas, receive information, and discover myriad perspectives on every topic imaginable. When a person buys a book at a bookstore, he engages in activity protected by the First Amendment because he is exercising his right to read and receive ideas and information." *Id.* at 1052. Colorado's constitutional protection of free speech is stricter than the federal floor, so it is not clear how the analysis might result in another jurisdiction.

[15] U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii (1973), *available at* http://www.epic.org/privacy/consumer/code_fair_info.html.

[16] 47 U.S.C. § 551 (2002).: (a) Cable providers must provide notice to subscribers regarding what personal data they collect, how they disclose and use it, and how subscribers may access their own data; (b) providers may not use the cable system to collect personal information other than as required to provide service; (c) providers may not disclose personal information without consent except as needed to provide service; even if served with a court order, providers must give subscribers notice and may not divulge individual programming choices; (d) providers must give subscribers access to their own personal data; and (e) providers must destroy personal data when it is no longer needed.

[17] 18 U.S.C. § 2710 (2002). Passed in 1998 in response to the disclosure of Supreme Court nominee Robert Bork's video rental records by a newspaper. Also grounded in FIP principles, the VPPA limits the parties to which video rental stores may disclose rental records to law enforcement with a warrant and civil litigants with a "compelling need," and requires stores to destroy rental records "as soon as practicable."

[18] "Eleven state constitutions guarantee a right of privacy or bar unreasonable intrusions into citizens' privacy. Forty-eight states protect the confidentiality of library users' records by law, and the attorneys general in the remaining two states have issued opinions recognizing the privacy of users' library records." See http://www.ala.org/Template.cfm?Section=stateifcinaction&Template=/ContentManagement/ContentDisplay.cfm&ContentID=14773. For instance, California state law provides: "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." Cal. Gov. Code § 6267 (West 2004). *See also, e.g.*, Code of Ala. § 41-8-10 (Alabama); 75 ILCS 70/1 (Illinois); NY CLS CPLR § 4509 (2004) (New York).

records.[19] These state laws mirror the express policy of the American Library Association, mandating respect for the expressive interests embodied in patron and circulation records.

2.3 Institutional and Professional Norms

While legal protections are incomplete and not uniform across different types of information good providers, business and professional practices of information goods providers reflect the legal and professional norms of protecting privacy. [20]

In libraries, the professional norms established by librarians reinforce individual privacy expectations. In an Interpretation of the Library Bill of Rights, the American Library Association 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."[21] To this end, "[r]egardless of the technology used, *everyone* who collects or accesses personally identifiable information in any format has a legal and ethical obligation to protect confidentiality." In addition to this broad policy statement, libraries' privacy policies typically implement Fair Information Practices—they hold patrons' information for the shortest time possible, keep minimal patron records, and restrict access to patron borrowing records, even where not required by law to do so. While actually borrowing materials from a library requires identification and registration, libraries have historically championed First Amendment rights to free speech and freedom of inquiry, positioning themselves as staunch defenders of due process when anonymity is threatened. Similarly, while not subject to the same legislative data protection requirements applied to libraries, bookstores along with related trade associations, have often been at the forefront of privacy actions.[22]

[19] *Id.*

[20] *See infra*. Bookstores are not subject to the same legislative data protection requirements that libraries are in states that enforce library privacy laws. However, bookstores and other information good providers are "presumptively under the protection of the First Amendment" and hence subject also to the Fourth Amendment requirement that state actors seeking their records show reasonable cause and obtain a subpoena. *Roaden v. Kentucky*, 413 U.S. 496, 504 (1973). Nonetheless, it is important to note that much of the information good supply chain, including, publishers, warehousers, and distributors, remains largely unregulated, particularly concerning non-governmental invasions of privacy.

[21] 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, "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.

[22] *See, e.g.*, *Ashcroft v. ACLU*, 542 U.S. ___ (2004) (plaintiffs included Salon.com, an online literary journal; A Different Light Bookstores; Powell's Bookstore; and the American Booksellers Foundation for Free Expression, among many others); *Tattered Cover supra.* (a Colorado bookseller resisted a subpoena); the Kramer Books matter *infra* (a Washington, D.C., bookseller resisted a subpoena). In these and many other litigations, the American Booksellers Association have participated, demonstrating broad industry support for private, anonymous access to information.

3.0 Risks of Using RFID

Whatever the applicable law,[23] the policy goal of protecting private inquiry may become much more difficult as RFID is implemented. In the pre-RFID world, individuals can pay in cash leaving no records and can hide the fact of the purchase to limit third party knowledge of their reading habits. Moreover, before widespread retail and library use of RFID, providers of information goods, from wholesalers to retailers to renters and lenders, have control over their own records, and are often bound legally to demand due process of law before disclosing private records. Data holders can examine subpoenas for authenticity and cause, and challenge them in court before disclosing private information. In the RFID-enabled world, however, it is possible that anyone with an RFID reader could discover individuals' informational preferences without their permission. Whether this possibility becomes reality depends in large part on whether RFID system designers and deployers are attentive to privacy norms. When information goods can be "interrogated" over radio waves, revealing whatever is on the tag (the goods' identity or other information), most likely in unencrypted form, to the immediate surroundings, no providers, librarians, the individual, sellers of goods or existing law will be sufficient to protect the privacy of purchasers and borrowers from those who seek to know what information they consume.[24]

Using RFID to tag information goods introduces a number of risks to personal privacy. Many of these risks are determined by the technical design of RFID readers and tags. RFID tags used for retail applications and tags used for libraries are significantly distinctive from each other. Retail tags are driven by technology developed for supply chain management. Tags are applied at manufacture and stay with the product during its life cycle. Retail tags may cost as little as 20 cents, with 5 cent tags envisioned within five years. Library tags, in contrast, are today applied individually by each library, remain with library holdings as they leave the library, and use a different set of technologies and tag labeling practices. While vendors have not publicly disclosed exact tag costs, an industry analyst reveals that library RFID tag prices are in the 50-75 cent

[23] Internationally, global commerce and supply chains may also subject entities implementing RFID to foreign data protection laws. The European Union is particularly protective of data privacy, and its laws are much more stringent than in the United States. *See, e.g.*, EC Data Protection Directive 95/46/EC.

[24] RFID technology also raises the unanswered question of what will constitute intentional interception of radio transmissions or unlawful access to information stored on RFID tags for purposes of the Wiretap Act as amended by ECPA. Violation of these laws requires a reasonable expectation of privacy on the part of the speaker, and such expectation may not be reasonable when an individual broadcasts information by radio frequency. 18 U.S.C.S. § 2510(2) (2000). Indeed, from 1986 to 1994 the law specifically exempted the radio portion of cordless phone conversations of phone conversations from protection because such transmissions were so easily intercepted. S. Rep. No. 541, 99th Cong., 2d Sess. 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566, cited in *McKamey v. Roach*, 55 F.3d 1236, 1239 (6th Cir. 1995). Though a subsequent amendment deleted the exception, courts have said that "broadcasting communications into the air by radio waves is more analogous to carrying on an oral communication in a loud voice or with a megaphone than it is to the privacy afforded by a wire." *United States v. Hall*, 488 F.2d 193, 196 (9th Cir. 1973), cited in *United States v. Smith*, 978 F.2d 171 (5th Cir. 1992) (noting that cordless phone conversations over radio frequencies are not subject to Fourth Amendment protection). To realize its purpose, ECPA may require further amendment or interpretation by courts that extends its protections to the radio transmissions of RFID.

range.[25] These differences and commonalities must be understood and appreciated before one can make informed decisions about the risks and appropriate responses.

Below, the Clinic has identified five areas in which tagged information goods pose risks to privacy in the stream of commerce.

3.1 Broadcasting and Lack of Access Control

All RFID technology, as the name suggests, operates through use of radio, which by its nature, anyone within range can hear. Because today's tags do not implement any access control on who can read the data stored on the tag, nothing prevents an illicit reader from learning RFID tag contents. Thus, third parties who are able to surreptitiously read tag data can identify the objects to which they are affixed. Moreover, even if tags respond only to authorized readers, the radio nature of RFID makes eavesdropping a likely possibility. Compounding these risks, different tags and readers have varying read ranges which cannot be discerned through physical appearance—some tags can be read at great distances while others require close proximity.

Retail tags operate at a radio frequency of 915MHz, which enables read ranges of up to roughly 20-30 feet. Most currently deployed retail tags are based on specifications created by EPCglobal, Inc., a joint venture between the Uniform Code Council (UCC) and EAN International, two agencies responsible for the administration of current retail bar codes. Recently the International Organization for Standardization (ISO) developed a new standard, ISO 18000-6, which proposes an alternative protocol for 915MHz tags. Library deployments, on the other hand, use RFID tags operating at a frequency of 13.56MHz. At least three major tag types exist. Tags based on the ISO 15693 standard are manufactured by companies such as Texas Instruments and Phillips, and deployed in a library setting by vendors including 3M and Libramation. The French company TAGSYS sells proprietary FOLIO C220 tags, which are used by VTLS and TechLogic in libraries. Finally, Checkpoint manufactures tags which are used only by the library systems division of Checkpoint. Recently standardized, but not yet available in libraries, is a new type of tag that follows the ISO 18000-3 Mode 2 standard. Library tag types are summarized in Table 1.

[25] See Boss 2003, *supra* note 1. The high cost relative to retail tags is often explained by noting that libraries are a smaller market than retail, and that library tags must have lifetime durability measured in years rather than weeks or months as with retail tags. Library RFID applications must tag every single book, and many libraries have hundreds of thousands or even millions of books, so even small differences in the cost of a single tag can have a large impact on the total cost of implementation. Because of this cost, after a library invests in a particular tagging system it is very hard financially and logistically to switch implementations.

Tag Type	Manufacturers	Library Vendors	Example Library
ISO 15693	TI, Phillips	3M, Bibliotheca	Natl' U, Singapore
TAGSYS C220	TAGSYS	VTLS, TechLogic	Eugene, Oregon
Checkpoint	Checkpoint	Checkpoint	Santa Clara, CA
ISO 18000-3 Mode 2	Coming soon	Coming soon	N/A

Table 1: Library RFID Tag Types and Vendors

13.56MHz library tags have significantly different characteristics than retail 915MHz tags, in part because they use slightly different physics. In particular, read range in 13.56MHz tags depends more on the size of the reader antenna than on the reader power. Long-range reading and tracking is difficult with 13.56MHz tags. Vendors claim roughly 8 inches for hand-held reading units, while free-standing exit sensors may read 2-4 feet.

In contrast, 915MHz tags have a larger read range: the "forward direction" of 915MHz units may carry for extremely long distances, and the "backward" direction of communication from tag to reader may propagate 20-30 feet. To read a 13.56MHz library tag, on the other hand, adversarial readers would need larger antennas to extend the read range of the tags, making the unauthorized reader harder to conceal. For these reasons, retail tags are more susceptible to surreptitious reading and eavesdropping than library tags.

3.2 Labeling

The digital contents of all RFID tags can be anything within the constraints of tag memory. It is the implementer's choice what information to include, and how to encode or represent that information digitally. Including bibliographic information, information about the individual carrying the tag, or information about past transactions with the tag onto an RFID label in plain text threatens to associate individuals with the books, music, and movies they carry. Encoding RFID labels using openly readable technical standards may further facilitate this associational privacy violation. However, use of opaque or encrypted labeling in not sufficient to prevent this threat. Even when encrypted labels are used in place of transparent ones, unauthorized third party readers can build databases linking identifying codes to actual objects. These associations can be created by reading a tag and physically examining the object to which it is attached, or more automatically using database reverse look-up features if they are available.

In the retail and supply chain settings, the Electronic Product Code (EPC) has emerged as the identifier of choice. An EPC is a 96-bit number that will uniquely identify each instance of a product; it can be thought of as a bar code augmented with a serial number so no two items have the same EPC. As prices of 915MHz tags drop, it will be feasible for every item to have a tag with a unique EPC identifier. The EPC namespace is administered by EPCglobal, which has far-reaching plans for the processing of RFID data. An EPC consists of three main fields: a "EPC Manager ID," which identifies the manufacturer of the item; an "Object Class" field that identifies the type of item; and finally a unique serial number.[26] The EPC Manager ID is assigned by EPCglobal to a manufacturer, and the manufacturer itself defines type and serial number mappings.

EPCglobal has equally wide-ranging plans for uses of the information about EPC-tagged items. Two proposals deserve special mention: EPC Object Name Services (ONS) and EPC Discovery Services (EPCDS), both currently being constructed by VeriSign.[27] ONS is a directory service used to link a manufacturer provided tag identifier to a website which contains more information about the RFID tag identified. Use of ONS may provide information about the manufacturer of a tagged product, the class of product tagged, and the tracking history of each unique tagged good. EPC Discovery Service does not hold any product information, but is simply a database of RFID "sightings" by all readers registered with EPC Discovery Service. EPCDS relies on individuals with readers to populate its database. Anyone with access to this database can in effect leverage all connected readers to monitor or track the movement of a particular EPC RFID label. Using ONS and EPCDS, one may discover the unique identity of books, down to the publisher, type of book, and bibliographic facts.

Libraries, however, have not used the standardized EPC labeling system. Library tags could contain a wide range of information, but libraries often use a unique id only (a barcode). These bar codes are assigned by each individual library to books as the books enter the collection. Typically, bar codes are a sequence of digits with a prefix unique to the particular library, and the rest of the sequence assigned arbitrarily by the library. Some libraries keep bibliographic databases (listing the barcode to book association) secret, but others do not. Most libraries do not coordinate when deciding which barcode maps to which book.

These localized practices create non-uniformity in identifier usage that help to mask the association between tags and books. Even so, adversaries can discover barcode to book associations by examining them physically. Moreover, the labeling string used may be used to identify which library a tag comes from. This puts adversaries closer to identifying a book by bibliography and is undesirable if we are to protect individual choice in reading. Finally, some (though by no means all) libraries provide the public with reverse lookups for barcodes, allowing a user to enter the barcode and find out the title and other bibliographic data about the book. Table 2 below summarizes differences between retail and library uses of RFID.

[26] EPCglobal http://www.epcglobalinc.org/standards_technology/EPCTagDataSpecification11rev124.pdf

[27] http://www.verisign.org/

Usage Setting	Retail	Library
[redacted]	[redacted]	[redacted]
Radio Frequency	915 MHz	13.56 MHz
Read Range	20-30 ft	1 - 4 ft. depending on the size of the antenna
Cost	$0.20 ($0.05 within five years)	$0.50-0.70
Existing Standards	ISO 18000-6	No Standard
Labeling Protocols	EPC: 96–bit globally unique ID	No Standard
Other Differences	Single Pass Inventory	Revolving inventory

Table 2 Retail and Library Uses of RFID Compared.

3.3 Tracking

The use of globally unique labels on RFID tags facilitates point-to-point and individual-to-individual tracking of goods shipped. A uniquely identified object that passes in front of several readers may reveal the movements of the individual who carries it. If these readers are networked to each other, the entity that owns that network may have access to more robust data about the location of an individual over time. By mapping that data onto contextual knowledge, information can be harvested about what types of establishments a person frequents.

With retail tags, the EPC Discovery Service poses special dangers of tracking by allowing individuals to make use of a global network of independently owned and operated RFID readers. Local readers upload read logs to the centralized EPC database, where records containing the same EPC label can be aggregated and displayed by any user of EPCDS. Libraries, which do not use standardized labeling protocols or globally unique ids, are, again, at less of a risk for tracking than retail businesses. Yet because all library labels are locally unique within the deploying library, with some knowledge concerning which library an RFID tag belongs to, point-to-point tracking can still to occur. Furthermore, by tracking individual tags, networks of RFID readers can be used to discern relationships between individuals who exchange tagged items, and can also be used to derive more sophisticated information about social networks.

Reducing RFID information to static labels which are globally or locally unique is not sufficient to protect privacy because these identifiers can be correlated with individuals and then used to track those people. Further, while RFID users are able to control what is written to labels at the application level, with some tags we studied, globally unique collision identifiers provide a static way of tracking tags, irrespective of what the application-level contents of those tags are. Because RFID tags use a shared radio medium, they need some method to avoid stepping on each others' communication.

Procedures for achieving this are called “collision avoidance” protocols. If privacy is a goal, care must be taken that these protocols are “private”—that is, the behavior of a tag during collision avoidance does not uniquely identify that tag.

Presently, however, the collision avoidance protocol for a popular standard of library 13.56MHz tags uniquely identifies each tag. The ISO 15693 standard for 13.56MHz tags specifies the use of a unique 64-bit MFR Tag ID, and the collision avoidance protocol reveals this ID; therefore ISO 15693 tags are uniquely identifiable even if the data on them is protected. While some attention has been given to private collision avoidance in retail 915MHz EPC tags, the collision avoidance protocols in 13.56MHz tags are different and cannot re-use this work.[28]

3.4 Invisibility

Both library and retail tags are very small and easily concealed, which means that individuals may not receive notice that goods are tagged. A great deal of research has gone into making tags unobtrusive to the consumer while preserving their read range. The trend for RFID has been to make tags smaller by reducing chip size and concealing antennas.[29] In library, rental, and retail applications, RFID may be used as an anti-theft device, which makes it imperative that tags are hidden. Moreover, even with knowledge that an object is tagged, holders of tags are unlikely to realize when those tags are remotely read. Consequently, RFID tags are unlikely to provide adequate notice to affected parties, a violation of Fair Information Practices.

RFID readers threaten privacy even when they are short-range and fully visible. For instance, readers can be set up at check points that enforce close proximity. Anti-theft gates in retail and rental stores currently do this. Moreover, some security gates in RFID equipped libraries look similar to traditional anti-theft gates but are in fact RFID readers which not only monitor permission for books to be removed, but also look up internal records containing bibliographic and check-out information as tags pass through them. Some gates record the ids of passing books in a cache. In either case, these security gates offer a source of sensitive data, which adversaries may have incentive to seek.

3.5 Joining Data

Although the information contained on a tag may be sensitive (such as the book title or ISBN), it may also seem innocuous on its face (such as a randomly generated unique number). However, innocuous information may be joined with data from other sources to produce more troubling effects. For example, an RFID reader working in tandem with a camera could link the appearance of an individual with the unique id of a

[28] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems.* 2003, available at http://theory.lcs.mit.edu/~sweis/spc-rfid.pdf. Weis, et. al., *Security in Pervasive Computing*. Lecture Notes in Computer Science, Volume 2802, pages 201-212, 2003.

[29] One firm is even researching use of magnetic ink as an antenna, in which case most of the space taken up by a tag would literally be printed on, and difficult if not impossible distinguish from ink that is not serving as an RFID antenna. http://www.rfidjournal.com/article/view/548.

library book that they carry. A similar system was recently used to identify purchasers of Gillette razor blades at shopping centers in England.[30]

Moreover, a reader could collect information from more than one tag an individual carries. If one is able to associate additional information (such as individual identity) with any one of these tags, each other tag carried may become linked with that information. For example, consider an individual who has been careful to select a book store that values patron privacy. He carries an RFID tagged book. His jeans are also tagged with an EPC label applied at the point of manufacture. When crossing the path of an RFID reader, both tags activate and identify themselves to the reader. Information about his identity linked only with the tagged clothing (which he paid for by credit card) is joined with the digital information provided by the book, and his anonymity at the book store is retroactively threatened. If the RFID reader that activated the tags with his jeans and book is a subscriber to EPC Discovery, his identity may be joined with that book title (or at least the connection made more readily derivable) in a database openly accessible to many people.

4.0 A Case Study of RFID in Libraries

We studied libraries as an early example of RFID adoption for use with information goods. As early implementers with direct contact with end users, libraries have grappled with privacy concerns, served as flashpoints of public opinion, and developed best practices to use RFID in a way consistent with constitutional rights and library patron expectations.

We studied the way that the Berkeley Public Library (BPL) manages its inventory processing and services tasks without RFID. We then reviewed their stated goal in adopting an RFID system. Using this information and technical knowledge of information system privacy and security best practices, we performed a threat analysis of BPL's planned RFID system. We discuss these threats below.

4.1 Threats to Privacy in a Library Setting

Use of RFID in libraries raises all of the threats to privacy applicable to other non-library settings. However, libraries as institutions create additional unique threats not present in retail stores.

- *Revolving Inventory and Directories for RFID Labeling Information*

  The unique RFID labels can be correlated with the items they tag through:

  i. Vendor Databases

     Vendors may retain databases of RFID identifiers after tags are sold to libraries.

  ii. Reverse-Lookup by Barcode Systems

      Some libraries provide public, or web accessible, computer terminals with these reverse-lookup features.

  iii. Physical Mapping

[30] Ed Harris, "Tesco to snap every shopper," The Evening Standard, 12 August 2003, available at http://www.thisislondon.com/news/articles/6181085?source=Evening%20Standard.

If barcode are mapped directly onto RFID, individuals can associate identifiers to bibliographic information by physically reading the barcode label. Alternatively, but equally insidious, individuals could read the RFID tag and record the identifier.

- Eavesdropping on Reader - Library System correspondence
  Wireless transmissions between RFID Readers and library information systems pose a particularly insidious threat to privacy due to the large volumes of data that are transmitted when scan logs are uploaded and downloaded.

  WEP and 802.11b encryption are not used in many of the wireless readers and checkout stations sold to libraries. Even with these protections, however, the systems are not secure. WEP and 802.11b have both consistently been broken by eavesdroppers with relatively little effort and are relatively insecure.

- RFID systems create additional data streams and caches that can by accessed surreptitiously or with authorization (as with a subpoena).
  i. Caching at Portable RFID Check-In / Out Stations.
  While caching library records at portable check-out stations allows books to be taken out during library system outages, doing this is risky for patron privacy because an additional repository that links patron and book information is created.
  ii. Caching at Portable RFID Readers.
  By their functional nature portable RFID readers must be capable of storing some library record information.
  iii. Caching at Security Gate.
  Some RFID systems cache data from items scanned by security gates. In some cases, the gates themselves may look-up and cache information. In others, information about book RFID labels read by the gates will be stored in a different part of the Library Information System.
  iv. Publisher Tagging.
  Some trade press suggests that publishers are considering use of RFID for supply chain management. If labels are applied at the point of manufacture, protecting the label information on book become increasingly difficult. It makes sense for the parties engaged in business as parts of these supply chains to adopt a common standard for labeling and tracking books. The number of companies involved and the likely open nature of such a labeling standard (such as an extension of ISBN) make the privacy of those labels difficult if not impossible to imagine.

4.2 Best Practices for Libraries; Models for Other Deployments

We next developed guidelines for mitigating some of these threats, which we have refined into a set of best practices. However, these best practices are not specific to BPL and can be used by any library. The best practices we have developed require foremost that the libraries provide patrons with notice that RFID is in use and of the potential risks to individual privacy. The best practices suggest use of a variety of methods to prevent unauthorized disclosure of a patron's subject of inquiry and personally identifying information. According to established Fair Information Practices, we recommend minimization of data collection and retention.[31] Most importantly we suggested that any data collected must be kept secure from both surreptitious and unauthorized access. For the complete best practices see Appendix I.

5.0 Recommendations

RFID technology has not been designed with privacy in mind. Books, music, and video are especially sensitive to surveillance, and although existing customs, laws, and expectations support relative anonymity in access to information, the introduction of RFID, if not attentive to privacy, may thwart these protections. Although several technical solutions have been proposed to alleviate privacy problems in RFID, none are effective in settings with revolving inventory and the most useful in the purchase setting, killing tags, prevents consumers from reaping any benefit from post-sale uses of RFID technology. Additional technical solutions must be found.

Survey research tells us that many consumers are not aware of what RFID technology is, how it is used, and what costs it raises to their privacy.[32] Even with information, near ubiquitous retail adoption of RFID may reduce consumer choice between RFID and non-RFID tagged products hindering self-policing within the marketplace. It is clear that RFID may make many efficiency gains possible. At the same time, there are also ways to implement RFID which, in our opinion, ought to be "unfair" or "deceptive" according to established FTC guidelines.

The Federal Trade Commission should conduct a formal technical and policy assessment of RFID. The Commission should also hold a workshop focused on the use of RFID technology to manage information goods. While libraries and book sellers are keenly aware of the privacy interests of their patrons, it is uncertain whether other distributors of information goods are as aware or sensitive to these issues.

Based on the outcome of this work, the FTC should develop guidelines for RFID deployment and data use that defines particular encoding, tagging, and data collection practices with RFID that the FTC considers to be deceptive and / or unfair.

When considering these guidelines, the Clinic believes that:

- **Entities using RFID must provide adequate notice explaining the technology, as well as how and why it is being used in the current context.**

[31] See *supra.* Note 15.

[32] RFID and Consumers: Understanding their Mindset, A U.S. Study Examining Consumer Awareness and Perceptions of Radio Frequency Identification Technology, CapGemini, available at http://www.us.capgemini.com/DownloadLibrary/files/CPRD_RFID_mindset_ES.pdf

- **Even with notice, encoding certain types of information onto RFID tags is presumptively unfair[33] because it undermines individuals' expectations of privacy.**
- **In the information goods context, databases that link RFID identifiers to particular items thereby allowing the content of inquiry to be associated with an individual should be tightly controlled to prevent the revelation of intellectual consumption.**

5.0 Conclusion

The threat to individual privacy stemming from item-level tagging of goods has generated criticism from a number of consumer advocacy organizations. At the same time, retailers and libraries that have tested item-level implementations of RFID have come under fire from privacy advocates.[34] Privacy concerns are generating policy action. Internationally, the European Union's Data Protection Directives may already apply to use of RFID with personal information, as well as use of location information.[35] Canadian officials produced a report documenting the privacy threats of RFID in

[33] Encoding certain information onto RFID tags in certain contexts would meet the relevant *Sperry & Hutchinson* criteria for unfairness: 1) substantial, unjustified, and avoidable injury to the consumer, and 2) violation of public policy. *See* FTC Policy Statement on Unfairness, *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[34] A group called the Privacy Rights Clearinghouse has called for a legislative moratorium on item-level RFID tagging until a formal government assessment of the technology takes place. See http://www.privacyrights.org/ar/RFIDposition.htm; The advocacy group Consumers Against Privacy Invasion and Numbering has drafted model legislation that would require the Federal Trade Commission to establish RFID privacy standards and educate the public, while also calling for disclosure labels on all items bearing RFID tags.

[35] Berwin Leighton Paisner LLP thinks that tracking individuals using RFID is subject to Europe's data protection laws. Under the data protection conditions, organizations that link personal information with RFID labels must first acquire permission from the data subject.

With respect to location data, Directive 2002/58/EC provides a definition for "location data" of "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service." According to this Ustaran argues that "the use of RFID tags to monitor customers will be subject to the specific obligations affecting location data under the e-privacy directive." *Id.* That directive requires that location data be anonymized unless consent is obtained from the subject. Individuals must have the option of withdrawing consent at anytime. Moreover, individuals must be able to prevent the processing of their location information, if they choose to do so, at any time. Obsolete data must be destroyed.

Telecommunications provider NTT Do Ko Mo also outlined EU law governing location data in a report. The 2002 Directive on Privacy and Electronic Communications established technology-neutral legal standards for privacy in electronic communications. Under the directive, data collected for billing must be erased or made anonymous at the end of each billing cycle. However, after the September 11th terrorist attacks, terms were included in the Directive to allow, but not require, member states to legislate the retention of both location and subscription data for law enforcement. The UK, France, Belgium, and Spain have all adopted laws for the retention of location information. Moreover, it seems likely that most remaining EU states (excluding Germany and Austria) will adopt similar provisions.

If the EU applies existing legal data protections to RFID, this will reflect their recognition that many threats posed to current generation technologies map to the RFID space. However, even in that case, the legally enforced retention of location records in many EU nations poses a threat to RFID users who may be tracked by readers at different locations over time.

February 2004.[36] Later in June 2004, the government of Ontario published guidelines to help libraries interested in using the technology adhere to existing Canadian Data Protection law.[37] In the United States, proposed legislation based on the Data Protection

[36] The Information and Privacy Commissioner of Ontario published a report this February 2004 dealing with the privacy implications of RFID. In it, she discussed the problem of linking personally information with the unique identifier on an RFID tag. Basis for this concern lay within the Canadian principle of informational self-determination – that is "that information about an individual belongs to that person, and is to be communicated or not, as the individual determines." (Ontario Information and Privacy Commissioner, Tag You're It: Privacy Implications of Radio Frequency Identification Technology, 2004, at 16, available at http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=15007&N_ID=1&PT_ID=11351&U_ID=0).

One primary fear has been that the ubiquity of tagging will increase to the level where consumers may have no alternative but to purchase and use tagged goods. In addition, data mining projects like the United States' Total Information Awareness program make the linking of disparate data sources highly probable. The Commissioner was particularly troubled by the Ontario Provincial Police's recent inquiry into constructing a reader capable of "interrogat[ing] any and all tags that might be attached to virtually anything." Id.

The Commissioner concluded that the Pillars of Privacy are notice and consent, in addition to an easily accessible option to kill tags at the point of sale. As Fair Information Practices for RFID, the Commissioner described that RFID users should not:

(1) tie future actions, such as product return, to maintaining an active RFID tag;
(2) prevent individuals from detecting the presence of tags and readers, or disabling tags affixed to their possessions;
(3) use RFID to tracking individuals without written consent from the data subject; and
(4) use RFID in a way that directly eliminates or reduces anonymity, such as by labeling currency.

[37] In June of 2004, the Information and Privacy Commissioner of Ontario published a set of implementation guidelines for the use of RFID in libraries. Those guidelines included:

(1) All libraries should have a privacy policy.
(2) Education and training should be provided to teach employees about the policy.
(3) Notice that RFID is in use is a basic expectation.
(4) Libraries should use open standards with RFID technology for interoperation with other libraries.
(5) Security procedures and technologies used with RFID should be audited regularly.
(6) Use of RFID should be reviewed periodically to evaluated continuing necessity.

For the purposes of the guideline, personal information is defined as "any recorded data, or other records of an identifiable individual." (Act at 5.)

The Act goes on to declare that "no person shall collect personal information on behalf of an institution unless the collection is *expressly authorized by statue*, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity." (emphasis added) (Id.) This statement points out a fundamental difference in how data collection is regulation in America, where some forms of data collection are forbidden but by default most are permitted, versus Canada, where there inverse is true—some forms of data collection are permitted explicitly and all other forms disallowed.

The first best practice that the Commissioner listed was the construction of a policy for operation and administration of any RFID system. Such a policy should include:

- The rationale for the system
- The location of readers, and a list of personnel authorized to operate them
- The name of a senior staff member responsible for adherence to the stated policy.
- Contractual obligations between the library and all RFID vendors / service providers that data records collected will remain in the control of the library and subject to Canada's Data Protection Act.
- A procedure to follow in case personal information is accidentally disclosed.

Some of the remaining best practices are as follows:

- Pamphlets with full information describing the use of RFID should be made available.
- Any personal information linked to a borrowed work through RFID should be de-linked when that item is returned.

model include Utah's Radio Frequency Identification Right to Know Act,[38] which expired in the state senate in the face of protests from industry, and Missouri's bill of the same name,[39] still before the senate in that state. California's proposed S.B. 1834[40] is based on Fair Information Practices[41] and would require retailers to obtain consumers' consent before tracking their purchases with RFID, and to kill RFID tags—render them inoperable—at point of sale.

We believe that the Commission should provide guidance to industry designing and implementing RFID technology to assure that the technology is deployed in a manner consistent with privacy norms and expectations. We appreciate the opportunity to participate in the RFID Workshop and hope that this effort will lead to greater public awareness of the privacy issues with RFID, heighten vendor sensitivity to such concerns, new technological responses to current privacy challenges, and the development of appropriate policy.

Respectfully submitted,

Deirdre Mulligan
Jennifer Urban
Laura Quilter
Nathan Good
John Han
Elizabeth Miles
Samuelson Law, Technology and Public Policy Clinic
University of California, Berkeley
School of Law (Boalt Hall)
392 Simon Hall
Berkeley, CA 94720
(510) 848-1501

- Personal information should never be stored directly onto an RFID label.

[38] Utah, 47-23, introduced by Rep. David Hogue (2003).

[39] Missouri, S.B. 867, introduced by Sen. Maida Coleman (2003) (available at http://www.senate.mo.gov/04info/billtext/intro/sb867.htm).

[40] California, Introduced by Sen. Debra Bowen. (2004).

[41] A set of privacy protective principles promulgated by the U.S. Department of Health, Education and Welfare in response to the revolutionary change computer technology enacted on the ability to collect, compile, store, and use personal electronic data. The five principles guiding the Fair Information Practices require (1) notice to consumers when data is collected; (2) a mechanism for individuals to discover what data is collected about them and how it is used; (3) a limitation on data use to its original purpose unless the consumer consents to other uses; (4) a procedure for correcting inaccurate personal information; and (5) the requirement that all who create, maintain, use, or disseminate personally identifying information assure its accuracy and prevent its misuse. *See supra* Note 15. The year after the government put forth the Fair Information Practices, Congress passed The Privacy Act which reinforced similar principles. "to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes." 93 P.L. 579 (1974), codified at 5 U.S.C. 552(a) (2000).

APPENDIX I
Library Best Practices

The Clinic's best practices for RFID are based on the Code of Fair Information Practices[42], and are organized accordingly by data disclosure, collection, retention, security, and notice and permission concerns.[43]

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.*
   e. The RFID tag should not contain data describing its origin or lending institution. *Library patronage is an associational choice that should be*

[42] *See infra* note 15.

[43] 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

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.*[44]

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

3. **Minimize collection of unnecessary data.**

[44] 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.

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.

APPENDIX II
RFID Vendor Assessment Tool

In addition to best practices, we have created a privacy assessment tool for libraries to gauge the privacy protection capabilities of particular RFID systems. This question set helps a library evaluate particular systems they may be considering. Guidelines for RFID vendors could call for automatic disclosure of such information.

- Do RFID writers used by the system write any information to tags by default? *The behavior of tag writers should be transparent, so that deploying entities can control the data contents of RFID tags they deploy.*
- Does the system use labeling formats that obscure data to unauthorized readers? *When possible, labeling formats should obscure data. This may conflict with needs to standardize formats for interoperability.*
- Who can rewrite the tags and how is this controlled technically? *Tag writers should maintain some type of access control, such as password protection, to prevent unauthorized and potentially malicious use.*
- What are the read ranges on each piece of RFID equipment? *Longer read ranges can cause problems with packet collision avoidance. More importantly, from a privacy standpoint, long read ranges increase the threat of surreptitious reading and eavesdropping.*
- Is there a wireless interface option between circulation stations and the library database? If so, what measures does the system provide to protect those transmissions? *Systems are most secure when they do not engage in wireless transmission, which due to the broadcast nature of radio, can easily be intercepted. If wireless components are used, efforts should be taken to protect transmission with standard cryptographic techniques. However, even in such situations, it is important to bear in mind that standard wireless protocols that incorporate encryption are often trivial to break.*
- How long does the server retain the cached information? How is cached data accessed? How is cached data protected from unauthorized access? *When components of the RFID system cache information, periodic deletions of records should be performed to prevent the accrual of massive databases which may be subject to unauthorized access at a later time. Data that is being stored should be protected with adequate access controls to limit unauthorized access.*
- Do the security gates generate item logs? Do the security gates log only items that have not been checked out or all materials passing through? *Security gates that cache information about which tags have passed within proximity present a large store of information which if accessed by an unauthorized party could lead to large scale privacy violations. Systems which use security gates capable of logging all books should be configured to log only those with permissions violations. Second, if at all possible, security gates should not access and cache internal library records. Most security purposes should require only verification of*

deactivation of the so-called 'security bit'—a bit which is toggled at check-in and check-out.

- Are pre-programmed tags rewriteable? If so, who is able to rewrite them, and how is this enforced technically? *Tag writers with access control mechanisms should be selected over those without access controls.*
- What is the nature of and purpose of the factory programmed serial number on the tag? How many series does the factory use? *When purchasing preprogrammed tags from an RFID vendor, it is important to discover whether it uses a serial number management system which can easily be reverse engineered, such as labeling tags uniquely in increasing sequence. Privacy is promoted when systems are chosen that provide for redundancy between labels sold to different customers, and that employ a thoughtful process of allocating those numbers in order to avoid easy discovery by unauthorized third parties.*
- What is the nature of the extra memory? *Some systems provide two regions of memory: one which can be rewritten, 'extra memory', and another portion which is read only. Other systems provide only one rewritable section. If your system is the first, your RFID vendor may retain information about your tag labels which you are unaware of. Moreover, without full information about tag contents, assessment of privacy risks may be inaccurate.*
- What is the tag encryption scheme? *None of the tag systems we examined use an encryption scheme. Indeed researchers have noted that strong encryption is not possible in current generation tags due to a lack of computational power. However, systems capable of encrypting tag contents are more desirable from a privacy standpoint than other systems.*
- Can the library lock all or part of the tag's memory? How is this accomplished technically? *When purchasing systems with so-called 'memory locks' libraries should take caution to discover how these locks work. Libraries should not rely on their efficacy until there is independent confirmation of their functionality in controlling all writers, and not just writers from the tags' manufacturer. Some systems claim to use 'memory locks' on tags in order to prevent data from being encoded onto RFID memory without authorization. However, with the systems we examined this is a red herring. Chips contain a 'write bit' which may be toggled. RFID writers from the same manufacture then scan the setting of this bit before allowing or disallowing writing to the chip. A writer from a different manufacturer could simply ignore this bit, or be unaware of it, and write to the contents of the tag in spite of its setting.*