Radio Frequency Identification and Privacy with Information Goods

Nathan Good, John Han, Elizabeth Miles, David Molnar, Deirdre Mulligan, Laura Quilter, Jennifer Urban, David Wagner

Abstract

This paper examines the privacy impacts of using RFID to tag information goods such as books, music, and video. Information goods have qualities which make surveillance uniquely invasive. Individuals have strong expectations of personal privacy in their choice of information goods which are reinforced in social norms, public policy, and law. We examine the normative, policy, and legal connection between privacy, the First Amendment, and information goods. We describe 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 discuss the threats to privacy created by the introduction of RFID into these settings. We conclude with best-practice and technical suggestions to make current RFID systems more privacy conscious.

1.0 Introduction

At its current stage of deployment, Radio Frequency Identification is generally used to tag goods at the pallet-level during shipping and warehousing. Already, however, more than 130 libraries in North America have also begun to tag their holdings, including books, music, and video at the item level.[1] There is reason to believe this trend will continue into the retail space for information goods such that proportion of tagged items will increase dramatically in coming years.[2]

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. 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.[3] 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. Proposed legislation based on this model include Utah's Radio Frequency Identification Right to Know Act,[4] which expired in the state senate in the face of protests from industry, and Missouri's bill of the same name,[5] still before the senate in that state. California's proposed S.B. 1834[6] is based on Fair Information Practices[7] and would require

---

[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/)

[3] See http://www.privacyrights.org/ar/RFIDposition.htm

[4] 47-23, introduced by Rep. David Hogue.

[5] S.B. 867, introduced by Sen. Maida Coleman.

[6] Introduced by Sen. Debra Bowen.

[7] 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

retailers to obtain consumers' consent before tracking their purchases with RFID, and to kill RFID tags—render them inoperable—at point of sale.

This paper examines the privacy impacts of using RFID to tag information goods such as books, music, and video. We use the term "information goods" to refer specifically to books, music, and film.[8] Information goods have qualities which make surveillance uniquely invasive. Individuals have strong expectations of personal privacy in their choice of information goods which are reinforced in social norms, public policy, and law. We examine briefly the normative and policy connection 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 conclude with best-practice and technical suggestions to make current RFID systems more privacy conscious.

1.1 Why Businesses are Interested in RFID

In its most basic form, Radio Frequency Identification (RFID) technology consists of a small, wireless RFID tag containing some digital information, and a reading device that is capable of activating the tag and collecting the information it contains. An RFID "tag" consists of two parts: an integrated circuit and an antenna. The circuit is extremely small, and the antenna may be integrated with packaging. RFID tags are passive: they do not have any power source of their own, but are instead powered by a radio signal from an RFID reader. Tags have limited storage, usually on the order of two kilobytes or less, and extremely limited computational power.[9]

RFID has generated interest from those concerned with supply chain management, as well as retailers and libraries. Moreover, RFID for home, security, and ubiquitous computing applications are increasingly active areas of academic research. Major tech industry players, such as, Microsoft, IBM, HP, Sun Microsystems, Philips, and Texas Instruments are aggressively developing RFID for inventory control.[10] Retailers like Wal-Mart hope to use RFID to sell more

---

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.
U.S. Dep't. 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. 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).

[8] We acknowledge scholars who have applied broader definitions Carl Shapiro and Hal R. Varian, Information Rules, Harvard Business School Press, 1999.

[9] In particular, cryptographic primitives such as pseudo-random functions, hash functions, or even pseudo-random bit generators are out of reach for today's low-cost tags. This is unlikely to change in the near future. While the number of transistors per unit silicon doubles every eighteen months, and these could be used to create tags at today's prices with extra security primitives, in practice it seems likely that economics will instead push the industry towards cheaper tags with a similar feature set as today's RFID.

[10] See http://www.infoworld.com/article/04/01/26/HNmsrfid_1.html; http://www.ti.com/tiris/default.htm?DCMP=TIHomeTracking&HQS=Other+OT+home_tirfid; http://www.bizjournals.com/sanjose/stories/2004/05/10/daily9.html; http://wwws.sun.com/software/solutions/rfid/

products by cutting down on when items are out of stock.[11] RFID vendors for retail also claim that the tags can work to reduce product theft.[12] According to vendors of library RFID systems, libraries especially stand to benefit from implementing RFID due to their rotating inventory needs.[13] RFID tagging systems promise to reduce and in some cases eliminate repetitive motions that can cause librarians physical injury. Meanwhile, increased efficiency and time savings may enable libraries to run with leaner staffs.[14]

2.0 Information Goods are Special – Norms 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 policies of institutions that provide information goods, as well as statutory and constitutional protections.

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 this case few means remain beyond the point of sale to discover the buyer's identity or to monitor what use the buyer makes of the work. Without identifying themselves, people can browse information on the Internet or in a library without checking materials out. Although library borrowing requires identification and registration, libraries have historically been staunch defenders of patron privacy, providing elaborate policy mechanisms to ensure records are kept secret from third parties when at all possible.

Traditionally, libraries have championed First Amendment rights to free speech and freedom of inquiry, viewing themselves as determined defenders of due process in the face of threats to free and anonymous inquiry. 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."[15] 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.

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 a range of

---

[11] http://www.informationweek.com/story/showArticle.jhtml?articleID=20600021

[12] See http://tinyurl.com/3brr3

[13] http://www.informationweek.com/story/showArticle.jhtml?articleID=20600021

[14] One major reseller of RFID systems for libraries claims that early adopters of RFID have reduced supply chain costs by three to five percent. http://www.checkpointsystems.com/docs/CKP-EPC_White_Paper.pdf

[15] 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.

settings. 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

The Constitution protects individual rights of free and private inquiry against government intrusion in the First Amendment's prohibition of any law that abrogates freedom of speech[16] and the Fourth Amendment's limits on government surveillance.[17] 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."[18] The Court has found that this right requires protecting the anonymity of speakers. One scholar points out that as new technology to monitor individuals' reading habits further develops, free speech increasingly depends on a right to read with relative anonymity.[19]

Constitutional interests in open, surveillance-free use of information works 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. Rumely*, holding that Congress could not compel a wholesaler of politically controversial books to disclose sales records at a congressional hearing.[20] The Constitution also limits the extent to which the Government can require citizens to disclose their choices in information access. In *Denver Area Educ. Telecommunications Consortium v. FCC*,[21] 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.[22] Further, the Court struck down a statute requiring individuals to identify themselves

---

[16] "Congress shall make no law …abridging the freedom of speech, or of the press." U.S. Const. amend. I.

[17] "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.

[18] 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)).

[19] Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, p*g 29.

[20] 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).

[21] 518 U.S. 727 (1996).

[22] "[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,

in order to receive controversial material, recognizing the burden such rules place on accessing information.[23]

Protection of book sales records received keen public attention recently in the Kramer Books-Monica Lewinsky matter.[24] 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."[25] 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.[26]

2.2 Legislation

Congress and state legislatures have created a patchwork 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.

The heightened sensitivity of expressive materials is reflected in a number of federal laws protecting data collection and use relating to information goods. The statutory protection, while still patchwork and incomplete, are also typically stricter than for other goods. For example, at the federal level, the Cable Television Privacy Act of 1984 protects cable television subscribers

---

(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").

[23] *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)

[24] *Supra* note 25.

[25] 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.*

[26] 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 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

from unfair data collection and use,[27] and the Video Privacy Protection Act protects the video rental records from release without a court order.[28] Similar laws protect library check-out and circulation information from release with without a court order in 48 states.[29] Moreover, the remaining two states have published opinions supporting the privacy of library borrowing records.[30] These laws mirror the express policy of the American Library Association. While legal protections are incomplete and not uniform between different types of information good providers, the practices of those who provide information goods—shaped by norms and law—are overall protective of private inquiry.[31]

3.0 Risks of Using RFID

Whatever the applicable law,[32] 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

---

[27] 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.

[28] 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."

[29] "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).

[30] Id.

[31] *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.

[32] 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.

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, anyone with an RFID reader can potentially discover individuals' informational preferences without their permission. When information goods can be "interrogated" over the radio, revealing the goods' identity (or other information) to the immediate surroundings, no providers, librarians, the individual, sellers of goods**,** nor the law stand between people and those who seek to know what information they consume.[33]

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 have significant distinctions. 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, library RFID tag prices are in the 50-75 cent range.[34] These differences and commonalities must be understood and appreciated before one can make informed decisions about the risks and appropriate responses.

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.

---

[33] 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.

[34] See Boss 2003. 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 in terms of time for libraries to switch implementations.

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.

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 plaintext 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 opaque 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 its 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.[35] The EPC Manager ID is assigned by EPCglobal to a manufacturer, and the manufacturer itself defines type and serial number mappings.

EPCglobal has wide-ranging plans for how information about EPC-tagged items will be used. Two proposals deserve special mention: EPC Object Name Services (ONS) and EPC Discovery Services (EPCDS), both currently being constructed by VeriSign.[36] 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 bar code 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 reverse lookups for barcodes to patrons.

3.3 Tracking

The use of globally unique labels on RFID tags facilitates point-to-point tracking. 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.

---

[35] EPCglobal http://www.epcglobalinc.org/standards_technology/EPCTagDataSpecification11rev124.pdf
[36] http://www.verisign.org/

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 take place. Furthermore, by tracking individual tags, networks of RFID readers can be used to discern relationships between individuals who exchange tagged items, and 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.[37]

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.[38] 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

---

[37] Weis et al. 2003 - *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems.* Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, Security in Pervasive Computing. Lecture Notes in Computer Science, Volume 2802, pages 201-212, 2003.

[38] 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

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 library book that they carry. A similar system was recently used to identify purchasers of Gillette razor blades at shopping centers in England.[39]

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 Solutions

Many of the solutions to existing privacy problems must come through technical choices made early in the design process. For instance, thoughtful policy cannot replace strong data protection techniques like encryption or hashing when protecting raw information contained within a standardized tag. As one scholar noted, "[F]ormal [or policy] conditions of privacy can never fully guarantee protection of privacy when the material [or technical] conditions for invading privacy are at hand."[40] Likewise, the inverse is also true. While many privacy problems may be mitigated by technical redesign, thoughtless use of the technology can always reduce individual privacy. Next we outline several best practices of both the technical and policy type.

4.1 Technical Fixes

4.1.1 Rendering Tags Inoperable – "Killing"

With businesses that sell (rather than rent or lend) products, a kill command, as demonstrated by current models of EPC tags,[41] may support individual privacy, by reducing tracking and associational threats. Killing a tag at the point of sale would minimize subsequent threats to individual privacy without limiting the inventory and distribution management tasks that RFID may be used for in the product supply chain. However, there is incentive for RFID designers and implementers not to kill tags at the point of sale. Retailers lack incentive to invest in the devices used to kill tags at checkout. While these machines may be costly, unless privacy

---

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

[40] Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 Santa Clara Computer & High Tech. L.J. 27, 36

[41] Current generation EPC tags incorporate a special password-protected "kill" command. Sending the kill command causes a tag to become permanently inoperative. http://www.rfidjournal.com/article/articleview/714/1/1/

is taken into consideration, retailers may see no benefit to their implementation, and actual loss in the potential for post-sale applications and re-use.

There are also other reasons for retailers not to kill tags at the point of sale. Information goods maintain their value over relatively longer periods of time—consumers *value* information goods for longer than other goods. Information goods are not subject to the problems of planned obsolescence, simple wearing out, or becoming obsolete through the dictates of fashion. Moreover, information goods are highly differentiated.[42] Information goods, therefore, are quintessentially collectable and maintain strong value to consumers over time. Consumers also use information goods in significantly different ways than other kinds of goods.[43] Consumers have developed many different products to catalog and analyze their personal libraries of books, DVDs, and music [44] taking advantage of standardized identifiers and barcodes. Many personal inventory systems interface with public databases of information about DVDs, CDs, or books,[45] and some even interface with the CueCat™ bar code readers.[46] These different uses and valuations tend to create a very different life cycle for information goods. While libraries are the quintessential lenders of books (and even movies, recorded music, and videogames), personal lending is also commonplace in the information goods sector. Consumers also access information goods through commercial lenders, such as video stores and videogame stores.[47] Additionally, the secondhand market in information goods is much more sophisticated than other second hand markets, and may be increasing in size.[48] Used books, CDs, and DVDs are sold to reselling organizations that would save inventory and labor costs if works they purchased came pre-tagged.

These post sale applications suggest that if anything, the utility of RFID tags to post-sale institutions and individuals will encourage continued RFID use. However, the privacy and expressive values at stake in the information goods sector mean that it is absolutely vital to maximize privacy and security—problems which RFID technology has yet to solve. Consequently, further evaluation is needed of the risks posed in the information goods sector, and the possible solutions and best practices.

---

[42] Recordings by Madonna and Maria Callas are valued very differently by different consumers, even if both are recorded on the same twenty-cent plastic disk. *See* Hal Varian, Markets for Information Goods, IMES Discussion Paper No. 99-E-9 (May 1999), pp. 3-4.

[43] Information goods differ from other kinds of goods in other ways. *See* Hal Varian, Markets for Information Goods, IMES Discussion Paper No. 99-E-9 (May 1999) (discussing some significant ways in which information goods are distinctive, including their experiential nature, the cost to create them, and their nonexcludability and nonrivalrousness, marginal cost of reproducing information).; "Information Goods and Vertical Differentiation" by Hemant K. Bhargava and Vidyanand Choudhary, *Journal of Management Information Systems*, Fall 2001, v. 18, no. 2, pp. 89-106 (showing that information goods are distinctive from other kinds of goods in terms of the effectiveness of price discrimination).

[44] An informal survey of a Windows software archive, VersionTracker.com, for "collection," "catalog," and "inventory," found over 50 programs for managing collections of books, music, or videos. The number of programs available for cataloging information goods dwarfed the number available for general personal home inventories, and only programs for wine collections approached the number of databases for information goods.

[45] Several such products allow interfaces with Amazon.com, the IMDB (Internet Movie Database), and the CDDB (compact disc database).

[46] *See, e.g.*, http://sourceforge.net/projects/jbiblioteca/ .

[47] *See* Hal Varian, "Buying, Sharing and Renting Information Goods," *The Journal of Industrial Economics*, Vol. XLVIII, no. 4, p.473 (Dec. 2000).

[48] *See, e.g.*, "Everything old is new again: while new book sales languish, used titles boost profits," *Publishers Weekly*, 250 (32): 126, Aug. 11, 2003 and Susan and David S. Siegel,"A Portra it of the Used Book Market" (Book Hunter Press, 2004) (growth in used book market);and *Standard and Poor's Industry Surveys*, 2004, "Movies and Home Entertainment Industry Survey" (increase in movie rental expenditures).

4.1.2 Anonymous IDs and other solutions

Libraries and rental businesses that depend on the cyclical use of tags for automated inventory and check-out cannot even depend on killing tags at check-out. Meanwhile, designing tags that can remain "live" while protecting privacy is an open research question. Thus, any library and rental business use of RFID exposes individuals to the associational and tracking privacy threats. One approach for libraries and rental businesses that cannot kill tags may be to rewrite RFID tags with a new random number on each checkout. This is the "anonymous ID scheme" proposed by NTT.[49] The association between number and bar code is kept in a separate database. At check-in, the bar code is re-written to the tag. This change has the advantage of being within the reach of the current generation of tags, and would prevent the compilation of bibliographic directories by third parties.

However, rewriting RFID labels at checkout is not a total solution since it does not alleviate the threat of point-to-point tracking, and in the end still provides a link between a semi-static identifier and bibliographic records. In these respects, privacy for tags that remain live is an open research problem.[50]

4.2 Best Practices

4.2.1 Kill tags when there is an opportunity to do so

Although libraries and rental businesses with circulating inventory don't have a choice whether to remove RFID tags upon check-out, retailers do. Currently there are no technical measures in place to limit serious risks to privacy involved with using RFID technology. At the same time, careful ways of using RFID that mitigate these same threats are not widely practiced. Until a time when technical and best practice precautions are more established, the only certain way to protect individual privacy beyond the point of sale is to kill the tag. At a minimum retailers should support the option to kill tags at the point of sale and customers should be provided with a clear and unconditional option to do so. Hopefully in the future, technical and

---

[49] (Ohkubo et al. 2003)

[50] A different approach to protecting bibliographic information than rewriting the RFID label is to introduce a read password. With read password architectures, a reader and tag share a secret password; the tag refuses to divulge its information to a reader unless it gives the password. No current RFID tag supports a read password. However, the forthcoming ISO 18000-3 Mode 2 tags have space to incorporate a 48-bit read password. Unfortunately, because tags must be read on each exit from the library, an adversary can overhear a password or spoof a tag to a legitimate reader to learn the password. Once the read password is learned, the adversary can post it on the Internet to allow anyone with a reader to read items. The problem is compounded by the fact that it is difficult to give different tags different read passwords. The reader, when presented with a tag, must figure out which password to use, but without knowing the tag's identity. We do not want to build a protocol that would uniquely identify the tag, such as having the tag send an ID that resolves to a read password – this sort of unique ID would defeat the whole purpose of read passwords. Also, any protocol must work during the time an item is passing within the range of the reader. Previous proposals for overcoming the tracking threat include the randomized hash locks of Weis et al. and the hash chains of Ohkubo et al. (See Weis, and Shingo Kinosita, et. al., Non-Identifiable Anonymous-{ID}Scheme for {RFID} Privacy Protection, CSS; Available at http://www.autoidlabs.com/whitepapers/KEI-AUTOID-WH004.pdf). In randomized hash locks, the tag challenges a reader using a pseudo-random function keyed with the shared password. In the hash chain scheme, each time a tag is read, and presents a hash of its real ID and then overwrites itself with the result of a different hash function applied to the ID. Both protocols prevent an adversary from distinguishing two tags if it queries them, but at the cost of reader computation linear to the number of possible passwords. Although both solutions could mitigate the tracking threat, neither is practical for libraries or retail stores, where there may be thousands to millions of items, to use. Further, both protocols assume the use of a collision-resistant hash function and the ability to write permanent state at the end of a read, which are currently problematic features.

best practice protections can be put in place so that post sale applications of RFID can be further explored.

4.2.2 Write minimal information onto tags—only one unique identifier.

For libraries, rental, and non-rental businesses, writing minimal information onto tags means that the organization deploying the RFID system should retain full control governing what information is written to tags. When purchasing tags, blank tags should be preferred over preprogrammed tags. If preprogrammed tags are used, efforts should be made to ensure that the manufacturer of the chips does not retain information about how tags were programmed. Organizations that buy RFID systems should choose systems that do not identify tags uniquely through their collision-avoidance protocols.

Bibliographic and transactional information about a tagged work, its manufacturer, or its owner or borrower should never be directly written to a tag.[51] Often times, a short unique string is all that is need to link a tag to some internal data record which may contain more detailed information.[52] Using tags with excess user programmable memory should be avoided. The benefit for retailers, distributors, publishers, and libraries of purchasing tags with maximum memory, is that future applications may require extra tag memory. However, extra memory can be used as a platform for the encoding of unnecessary and possibly unauthorized data—an unauthorized third party may write information to a tag.

4.2.3 Do not use standardized labeling formats

Using standardized RFID label and data formats (ISBN and EPC) should be avoided in libraries. Standardized labeling facilitates correlation of label identifiers with book identifiers. While some information must be written to tags and to enable the inventory and supply chain practices which justify RFID, that information can be encoded in a way to make access by unintended parties more difficult.

4.2.4 Don't subscribe to the EPC Discovery Service

Retail suppliers using RFID should not subscribe to the EPC Discovery Service. Through positive network externality[53], the EPC Discovery Service makes RFID-based tracking an eminent and ubiquitous possibility. Where data collected by every reader is combined with data collect by each other reader, and open access to this information is promoted, point-to-point tracking of individual items become a simple task. By enabling tracking without a court order, EPC Discovery Service create an easy source for data on individuals that will likely be accessible to the government without the limits of the 4th Amendment, and to private parties without the tracked individual receiving notice or having the opportunity to object. More importantly, leveraging the supply-chain management benefits of RFID does not require use of this global service. Use of internal information systems can make inventory and shipping transparent within and between cooperating companies, with less of a tracking risk.

---

[51] Any information necessary for record-keeping or to conduct subsequent transactions can be stored in a separate database which is protected from unauthorized access using established information system practices. A unique identifier can be used to link the tagged artifacts with these protected data records. However, care should be taken that the identifier assigned to the artifact does not contain information which can be used to infer any of the information discussed above.

[52] In such circumstances, where deploying institutions have a choice concerning what protocol to use, those label formats that require less data storage are more supportive of privacy than those that require more.

[53] The more data is dumped into the network, the more valuable the network is, and the more incentive individuals have to join.

4.2.5 Fair Information Practices

Foremost, individuals working with RFID should be informed that RFID is in use, what the technology does, what the potential risks to privacy are, and ways to mitigate those risks. Notice should include clear labels wherever tags are. In some circumstances this must be balanced with the use of RFID for theft detection. Users ought to have the option of retaining services provided by an organization without using RFID. The transmission range of RFID tags and the sensitivity of RFID readers should be limited to short ranges. The greater the read range, the more susceptible articles are to surreptitious reading. Security gates that read RFID tags should not log that information by default. If a security gate must log information for a functional purpose, the gate should retain that information for only as long as necessary to achieve that purpose. RFID reader consoles and portable readers, when possible, should also be configured not to cache collected information. RFID deploying institutions should provide staff with special training in how to use portable readers in order to minimize unnecessary data collection.

When implementing wireless transmission between readers and other information systems, established methods of encrypted transmission should be used. Organizations should reexamine information system security to guard against new threats from interoperation with RFID systems. RFID readers should have access control lists which are modified only according to strict policy and procedures. Tag writers should also have access control lists which are changed only through a standard and monitored procedure.

5.0 New Laws

Current proposals for legal reform are useful to consider but fail to address RFID implementations that cannot use killable tags, such as tags on credit, debit, club, and identification cards; driver's licenses; airline tickets; and circulating goods (all of which have been proposed). State regulations cannot address implications of nationwide RFID implementations. Additionally, they create the possibility that a patchwork of regulation over RFID data will make it difficult for consumers to understand their rights, RFID implementers to fulfill their obligations, and technologists to freely develop better solutions. More fundamentally, legal requirements will be ineffective without technical and best practice guidelines that fix current RFID security flaws so implementers can comply with any privacy regulations passed.

Among the legal avenues that policy makers might fruitfully pursue are Federal Trade Commission guidelines that define what RFID implementation practices will constitute unfair or deceptive conduct by RFID deployers and collectors of RFID data, and laws such as the proposed California bill that require Fair Information Practices by implementers of RFID. Discussion of these initiatives must recognize that protecting privacy is not as simple as killing RFID tags, but that various technical measures may be available or developed in the near future to make implementation of FIP-based regulations possible. Policy makers should work in tandem with the technologists to realize the most privacy-protective framework for broad deployment of RFID.

6.0 Conclusion

RFID technology has not been designed with privacy in mind. At the same time, its new application in many industries lack practices which promote privacy. Books, music, and video are especially sensitive to surveillance, and although existing customs, laws, and expectations support relative anonymity in access to information, RFID presents individuals with the ability to side-step these protections and harvest data without individuals' permission. Although many technical solutions have been proposed to alleviate these privacy problems, none are effective with current technology unless tags are killed. More technical solutions must be proposed. Concurrently, best practices, education, and training should take place to educate the public about privacy conscious use of RFID.