Radio Frequency Id and Privacy with Information Goods

Nathan Good[a1]
ngood@sims.berkeley.edu

John Han[a2]
john_han@sims.berkeley.edu

Elizabeth Miles[a3]
emiles@boalthall.berkeley.edu

David Molnar[a6]
dmolnar@eecs.berkeley.edu

Deirdre Mulligan[a4]
dmulligan@law.berkeley.edu

Laura Quilter[a5]
lquilter@law.berkeley.edu

Jennifer M. Urban[a7]
jurban@law.berkeley.edu

David Wagner[a8]
daw@cs.berkeley.edu

Categories and Subject Descriptors
K.5 [**Legal Aspects of Computing**]

General Terms
Security, Legal Aspects.

Keywords
RFID, privacy, information goods, law, policy.

1. NORMS AND LAW

This paper examines the privacy impacts of using radio frequency identification (RFID) to tag information goods such as books, music, and video. Individuals have strong expectations of privacy in their choice of information goods. These expectations are supported by both social norms and law. As a matter of practice, people may generally purchase and browse information goods without identifying themselves or the subject of their inquiry. People may pay in cash and avoid creating records that provide opportunities for third parties to learn of their information habits. Information providers that maintain records, such as libraries and bookstores, have staunchly defended their patrons' privacy, and indeed are often bound legally to demand due process of law before disclosing those records. Data holders can examine subpoenas for authenticity and cause, and challenge them in court before disclosing private information. Bookstores have done so in recent high-profile cases. [6][9] Libraries have developed elaborate policy mechanisms to ensure records are kept private, [1] and lobbied for laws protecting library records.

U.S. law has also been protective of individuals' rights of privacy and free inquiry, grounding those protections in the First and Fourth Amendments of the Constitution. [4][5] Supplementing these constitutional protections, Congress and state legislatures have created a patchwork of industry-specific statutes that shield records of individual inquiry from disclosure to both public and private parties. For example, the Cable Television Privacy Act protects cable television subscribers from unfair data collection and use [3], and the Video Privacy Protection Act protects video rental records from release without a court order. [2] Laws in 48 states protect library records from release with without a court order. [1] These laws and business practices are generally based on Fair Information Practices, which mandate notice to consumers about data collection practices, the opportunity to discover and correct inaccurate records, and limitations on the use of data. [14]

2. RISKS OF USING RFID

Using RFID to tag information goods creates new risks to personal privacy. Put simply, in the RFID-enabled world, 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, neither the individual consumer nor the third-party record-holder, has the opportunity to prevent disclosure of the information on the RFID tag.

All RFID operates through radio, which by its nature, anyone within range can receive. Current generation tags lack access control. Thus anyone, including unintended third parties, can potentially read any information stored on a tag. The static unique identifiers frequently stored on tags thus link the tagged items to the individuals who carry the item. Even stored opaquely—that is, encoded or not patently identifying—static unique identifiers can be linked to the real world object and thus to the object's holder.

Many of these risks are determined by the technical design of RFID readers and tags. While a common technology is used in both retail and library applications, there are some significant differences. Retail 915MHz tags can be read at ten times the distance (20-30 feet) of library 13.57MHz tags (2-4 feet). Additionally, retail users of RFID will use the Electronic Product Code (EPC), a 96-bit number designed to uniquely label individual items. [7] EPC users will have access to the EPC Discovery Service, an aggregate database of tag "sightings" collected from independent readers. Anyone with access EPC Discovery can monitor or track the movement of a particular RFID-tagged item. Commercial information good producers will likely use the EPC format on their RFID tags.

Libraries currently deploying RFID typically tag their holdings with legacy unique identifiers (not EPCs) from their prior barcode systems, which differ from library to library and help mask the

WPES'04, October 28, 2004, Washington, DC, USA.
Copyright 2004 ACM 1-58113-968-3/04/0010…$5.00.

association between tags and specific books. However, tag-to-book and tag-to-library associations can be made by physically examining a particular item or by access to the library database. Since library labels are static and locally unique, point-to-point tracking of individuals carrying library items is also possible. With some tags we examined (ISO 15693 13.56MHz), globally unique collision identifiers provide a static way of tracking tags regardless of the application-level contents of those tags. [13]

Individuals may not know when information goods have RFID tags. Efforts to make tags more unobtrusive, by reducing chip size and concealing antennas, make consumer awareness unlikely absent policies requiring explicit notice. Even if people know an item is tagged, however, they may not know or have a choice whether the tag is read or not. Once captured, tag information may be compiled with other data—for example, a camera positioned near a reader captures data about the individual. [10]

3. TECHNICAL SOLUTIONS

For purchased information goods, "killing" a tag at the point of sale may minimize threats to individual privacy without limiting the inventory benefits of RFID. [8] However, retailers may have little incentive to invest in the technology required to kill tags. [12], or simply be reluctant to kill expensive tags given the opportunity costs relating to potential post-sale applications.

Killing tags is not even an option for libraries and rental businesses with rotating inventories. One approach for such entities may be to rewrite RFID tags with a new random number on each checkout. [11] This is possible for current generation tags and would prevent the unauthorized compilation of bibliographic directories. However, a random number scheme does not address point-to-point tracking. Another approach is to introduce a read password that authenticates the reader before permitting access to a tag's contents. Although no current generation tags support a read password, forthcoming ISO 18000-3 Mode 2 tags have space for one. Unfortunately, passwords may be overheard or collected by spoofing a tag. Password schemes also pose other problems: a single generic password for a set of tags can be easily defeated, but a unique password for each tag could uniquely identify the tag. Other proposals for overcoming the tracking threat have included randomized hash locks and hash chains. [13] Both prevent an adversary from distinguishing two queried tags, but at the cost of reader computation linear to the number of possible passwords. For this reason neither proposal is practical for libraries or retail stores, which may have hundreds of thousands of items. Further, both protocols assume features that are problematic in practice, such as collision-resistant hash functions and the ability to write permanent state at the end of a read.

4. BEST PRACTICES

Until technical solutions are more readily available, retailers should support the option to kill tags at the point of sale and customers should be provided with an unconditional option to do so. Bibliographic and transactional information should never be written to a tag. To the extent necessary, a short unique string may be used to link to a database that is securely protected both by fair information practices and application-appropriate security protocols and practices. Libraries should avoid using standardized label formats (ISBN and EPC) that make it easier to obtain product identifying information. Information should also be obscured through use of a non-standard encoding format. Tag manufacturers should not retain information written to tags. Manufacturers should make clear whether the collision avoidance behavior of tags uniquely identifies them. Suppliers of information goods should not subscribe to the EPC Discovery Service, which compounds the threat of point-to-point tracking. Instead, cooperating companies can use internal information systems that make inventory transparent within and between organizations with less risk of tracking. RFID implementers should employ fair information practices, including notice to consumers, minimal data collection and retention periods, and staff education about privacy.

Policy makers might fruitfully pursue regulation of unfair or deceptive RFID practices, as well as requiring implementation of fair information practices. Ultimately, however, legal requirements will be ineffective without technical solutions that enable compliance with regulations. Privacy-protective implementation of RFID for information and other goods will require collaboration between policy makers and technologists.

5. REFERENCES

[a] University of California, Berkeley. a1: Ph.D. Candidate, School of Information Management and Science (SIMS). a2: Master's Candidate, SIMS. a3: J.D. Candidate, School of Law. a4: Associate Professor, Law. a5: Fellow, Law. a6: Ph.D. Candidate, Computer Science. a7: Visiting Acting Professor, Law. a8: Professor, Computer Science.

[1] American Library Association. Privacy: An Interpretation of the Library Bill of Rights. (2002).

[2] 18 U.S.C. § 2710 (2002).

[3] 47 U.S.C. § 551 (2002).

[4] Denver Area Educ. Telcos. Consortium v. FCC, 518 U.S. 727 (1996).

[5] Lamont v. Postmaster General, 381 U.S. 301, 307 (1965).

[6] Tattered Cover v. City of Thornton, 44 P.3d 1044 (Colo. 2002).

[7] EPC Tag Data Standards Ver. 1.1 Rev.1.24 (2004 April 1).

[8] Class 1, G2, EPC Tags Ready by Q4, *RFID J.* (Dec. 2003).

[9] KramerBooks' 1998 challenge to a subpoena for Monica Lewinsky's book purchase records.

[10] Harris, E. Tesco to Snap Every Shopper. *The Evening Standard* (Aug. 12, 2003).

[11] Ohkubo, M., et al. Non-identifiable anonymous-ID Scheme for RFID Privacy Protection. (2003).

[12] Stapleton-Gray, R. *Would Macy's Scan Gimbels? Competitive Intelligence and RFID.* (2003).

[13] Weis, S., et. al. *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems.* Lecture Notes in Computer Science, V. 2802, p. 201-212, 2003.

[14] U.S. Dept. of Health, Education and Welfare. *Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens*. (1973), viii.