Privacy Issues in RFID Applications

Information Security Privacy Advisory Board (ISPAB)

30 March 2005

By:
Anna Slomovic

SRA INTERNATIONAL, INC.

Privacy issues arise when RFID leads to *collection* or *connection* of information about individuals

- **Supply management: a tagged item is bought, carried or worn by an individual**
  - Information about single purchases, behavior profiling, location tracking
- **Libraries: patron checks out tagged material**
  - Information about intellectual interests, tracking associations via "hotlisting"
- **Access credentials: individual accesses resources**
  - Location tracking, information about resources of interest
- **Transportation: individual uses token to pay transportation or driving fee**
  - Location tracking, profiling associations
- **Documents: individual accepts document or token with contactless IC**
  - Personal information about the individual, profiling associations, location tracking

RFID devices involve data privacy and location privacy

- Data privacy
  - Data on the tag or IC
  - Data in database associated with the tag or IC
  - Profiling based on multiple tags associated with the individual
  - Profiling based on characteristics of a tag, e.g, tags distributed in one part of the world
  - New databases created using tag number as "anchor"
- Location privacy
  - Location and time of tag read
  - Association between individuals based on tags

Page 3

Understanding privacy issues begins with understanding the application

- What RFID characteristics are needed by the application?
  - Supply chain: data on tag; location of tag; non-line-of-site readability; readability through obscuring materials
  - Libraries: data on tag; tag entry/exit logging; tag location (in facility only)
  - Documents: data on IC only
- How wide is the interoperability?
  - Passports: many unrelated (and sovereign) parties reading data
  - Company access credential: use in a single company's facilities
- How varied is the lifecycle of tag/IC within application?
  - Supply chain: different uses by manufacturer, retailer, post-sale service
  - Transportation: single type of use for lifetime of tag

Page 4

Understanding the application, continued

- What value-added applications are complementary?
  - Consumer applications: profiling for marketing
  - Access credentials: employment actions; traffic congestion analysis
- What other technologies are involved in the system?
  - Access credentials and documents: biometrics
  - Supply chain: GPS; sensors
- What rights does an individual have with respect to tag/IC?
  - Consumer applications: few restrictions on accepting or altering tag on consumer-owned item
  - Documents: individual must accept document or token and may not make alterations

RFID privacy protection: general proposals

- Fair Information Practices
  - Information about the presence of tags and readers, content of tags, purposes of information collection and use
  - Ability to refuse tagged item in consumer product applications
  - Ability to disable or destroy tags in consumer product applications
- Security measures
  - Encryption on tag
  - Secure communication protocols
  - Secure back-end databases
  - Authentication of tags and readers
  - Number randomization or non-identifier based numbering algorithm in some applications
  - Physical shielding of tags

Generic measures vary in usefulness and effectiveness in different applications

- Application determines whether specific privacy-protection measures work without inhibiting the application
  - "Killing" the tag works for bookstores but not for libraries
  - Metallic sleeves work for passports but not for ID that must be displayed as it is worn
  - Encryption works for tags within a delimited system but not in a system where many unrelated parties must read data (until/unless universal encryption standards are accepted)
- Fair Information Principles are applied in different ways for different applications
  - Records of access to resources are at a level of detail individuals do not track and whose accuracy they may not be able to assess
  - To whom do inferential records (e.g., profiles) belong?

Privacy impact evaluation must be specific to the application and deployment

- Determine what aspects of RFID technology matter
  - Credible use case scenarios
  - Comparison with privacy characteristics of other technologies that might accomplish the same goal (e.g., 2D barcode on documents)
  - History of deployments and data collection efforts in similar applications
  - Understanding risks presented by "extra" capabilities of the technology
- Examine policies in conjunction with technical controls—if technical controls cannot support policy, policy is more likely to fail
  - Limitations on data collection
  - Limitations on data use and analysis
  - Limitations on data retention
  - Mitigation of risks associated with capabilities not needed in the application or deployment

Privacy impact evaluation, continued

- **Examine the whole system to identify privacy risks**
  - System architecture
  - Component technologies
  - Organizational structure
  - Physical infrastructure
- **Determine which security technologies can support privacy protection—and which create their own privacy issues**
  - Audit logs for policy enforcement create records of individual actions
  - Centralized authentication allows inferences about resources used

A note of caution...

The consistent experience with data protection suggests that, over time, there is always pressure to use data collected for one purpose for other purposes.

Report of the Technology and Privacy Advisory Committee, 2004