Privacy: It’s All in the Use Case

Susan Landau
Visiting Scholar, Computer Science
Harvard University

A Brief History of Privacy

A Brief History of Privacy

- Brandeis and Warren (1890).

A Brief History of Privacy

- Brandeis and Warren (1890).
- Olmstead v. United States (1928):

A Brief History of Privacy

- Brandeis and Warren (1890).
- Olmstead v. United States (1928).
- (NAACP v. Alabama (1958), Griswold v. Connecticut (1965)).

A Brief History of Privacy

- Brandeis and Warren (1890).
- Olmstead v. United States (1928).
- Alan Westin, *Privacy and Freedom* (1967).

A Brief History of Privacy

- Brandeis and Warren (1890).
- Olmstead v. United States (1928).
- Alan Westin, *Privacy and Freedom* (1967).
- HEW study, *Records, Computers, and the Rights of Citizens* (1973).

A Brief History of Privacy

- Brandeis and Warren (1890).
- Olmstead v. United States (1928).
- Alan Westin, *Privacy and Freedom* (1967).
- HEW study, *Records, Computers, and the Rights of Citizens* (1973); Fair Information Practices.

Fair Information Practices

- Notice: what information is being collected, by whom, for what purpose, for which recipients, and whether the data is being provided voluntarily.

Fair Information Practices

- Notice.
- Choice/Consent: the ability of the individual to control secondary uses of the data.

Fair Information Practices

- Notice.
- Choice/Consent.
- Access/Participation: ability of the individual to access data about themselves and to correct errors.

Fair Information Practices

- Notice.
- Choice/Consent.
- Access/Participation.
- Integrity/Security: that data collector ensures accurate collection, that the data is protected against unauthorized access, destruction, or disclosure.

Fair Information Practices

- Notice.
- Choice/Consent.
- Access/Participation.
- Integrity/Security.
- Enforcement/Redress: that there is a mechanism in place to permit enforcement and redress if these principles are not followed.

In 2011 ...

facebook

+1

OnStar®

foursquare

CHECK-IN HERE

Check in to unlock specials, meet up with friends and explore what's nearby.

foursquare.com
@foursquare

E-ZPass

Real Privacy Threat Categories

Real Privacy Threat Categories

- Linkability.

Real Privacy Threat Categories

- Linkability: of entity across disparate sets.

Real Privacy Threat Categories

- Linkability.
- Identifiability of a subject.

Real Privacy Threat Categories

- Linkability.
- Identifiability.
- Non-repudiation.

Real Privacy Threat Categories

- Linkability.
- Identifiability.
- Non-repudiation: allows the attacker to demonstrate something about the user.

Real Privacy Threat Categories

- Linkability.
- Identifiability.
- Non-repudiation.
- Detectability: determining that an item exists.

Real Privacy Threat Categories

- Linkability.
- Identifiability.
- Non-repudiation.
- Detectability.
- Information Disclosure: making information available to those who should not have access.

Real Privacy Threat Categories

- Linkability.
- Identifiability.
- Non-repudiation.
- Detectability.
- Information Disclosure.
- Content Unawareness: content available without the user's knowledge.

Real Privacy Threat Categories

- Linkability.
- Identifiability.
- Non-repudiation.
- Detectability.
- Information Disclosure.
- Content Unawareness.
- Non-compliance: site not complying with advertised policies.

Real Privacy Threat Categories

- **L**inkability.
- **I**dentifiability.
- **N**on-repudiation.
- **D**etectability.
- Information **D**isclosure.
- Content **U**nawareness.
- **N**on-compliance.

“A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements,” Deng, Wuyts, Scandariato, Preneel, Joosen.

Federated Identity Management

Federated Identity Management

- Liberty Alliance (2001).
- Microsoft Passport (2001).
- Proliferation of standards: WS, SAML, …
- Identity management for the “open” Internet (2005).
- NIST's Levels of Assurance.
- FICAM (Federal Identity, Credential, Access, and Management).

Federated Identity Management: Use Cases

Federated Identity Management: Liberty Alliance Use Case

- Outsourcing

Federated Identity Management: Liberty Alliance Use Case

- Outsourcing

Federated Identity Management: Liberty Alliance Use Case

- Outsourcing: HR

  travel

  suppliers

Federated Identity Management: Liberty Alliance Privacy Threat

- Linkability.

Federated Identity Management: Liberty Alliance Privacy Threat

- Linkability.

  Pseudonymity

Federated Identity Management: Use Case

- Shibboleth: library access across different research institutions.

Federated Identity Management: Privacy Threat

- Shibboleth: library access across different research institutions.
- Threat: identifiability.

Federated Identity Management: Privacy Threat

- Shibboleth: library access across different research institutions.
- Threat: identifiability.
- Solution: give only “needed” identity.

Federated Identity Management: (Not Our) Use Case

- Privacy issue: link --- but don't identify.

Federated Identity Management: (Not Our) Use Case

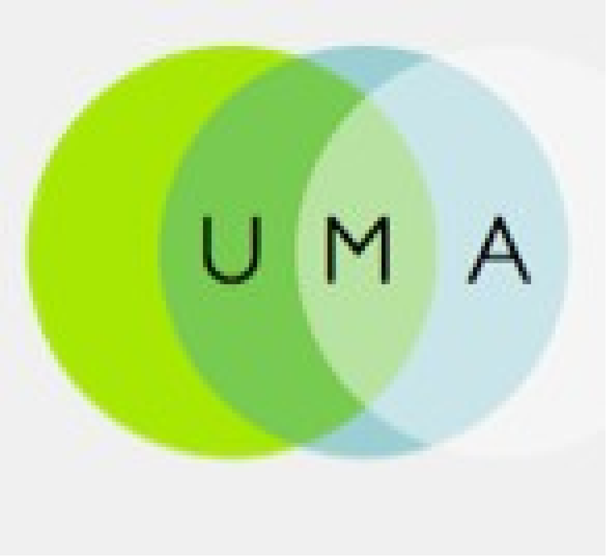
- Privacy issue: link --- but don't identify:

Federated Identity Management: (Not Our) Use Case

- Privacy issue: user control of private data.

Federated Identity Management: (Not Our) Use Case

- Privacy issue: user control of private data:



Federated Identity Management:
What Did We Miss?

Federated Identity Management: What Did We Miss?

- Need for light-weight identity (e.g., comments to blog posts).

Federated Identity Management: What Did We Miss?

- Need for light-weight identity (e.g., comments to blog posts).
- Users outside the enterprise as anything but “consumers.”

Federated Identity Management: What Did We Miss?

- Need for light-weight identity (e.g., comments to blog posts).
- Users outside the enterprise as anything but “consumers.”
- The “open” Internet.

RFID Tags

RFID Tags

- Technology not new.

RFID Tags

- Technology not new.

- Had been used for IFF, animal tracking, car key fobs, inventory management, toll collection.

RFID Tags

- Technology not new.
- Had been used for IFF, animal tracking, car key fobs, inventory management, toll collection.
- **Now was being proposed for inventory management at the consumer level: individual goods.**

RFID Tag Problems

- Remarkably rich source of information:

  data on tag

  data in database

  time of reading

  location of reading

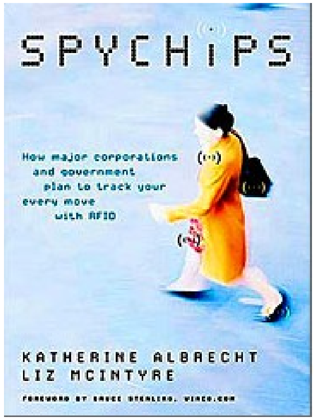
  association between individuals.

RFID Tags

HIGHLY, HIGHLY CONTROVERSIAL

RFID Tags

HIGHLY, HIGHLY CONTROVERSIAL


SPYCHiPS
How major corporations and government plan to track your every move with RFID
KATHERINE ALBRECHT
LIZ MCINTYRE

RFID Tag Problems

- Remarkably rich source of information:

  data on tag
  data in database
  time of reading
  location of reading
  association of individuals.

RFID Tag Problems

- Remarkably rich source of information:

  data on tag

  data in database

  time of reading

  location of reading

  association of individuals.
- LINDDUN (**l**inkability, **i**dentifiability, **n**on-repudiation,**d**etectabilty, information **d**isclosure, content **u**nawareness, **n**oncompliance).

RFID Tag Threats

- Creates ability to profile an individual.

RFID Tag Threats

- Creates ability to profile an individual --- including about many aspects that were previously private.

RFID Tag Threats

- Creates ability to profile an individual --- including about many aspects that were previously private.
- Creates ability to track an individual.

RFID Tag Threats

- Creates ability to profile an individual --- including about many aspects that were previously private.
- Creates ability to track an individual.
- Simplifies remote corporate espionage through tracking.

RFID Tag Solutions: What's the Use Case?

-

RFID Tag Solutions: What's the Use Case?

- Libraries: track where the books are.

RFID Tag Solutions: What's the Use Case?

- Libraries.

The right to read anonymously is extremely important.

RFID Tag Solutions: What's the Use Case?

- Need the data: on exit/entry to library,
  within library for tracking.

RFID Tag Solutions: What's the Use Case?

- Need the data: on exit/entry to library,
  within library for tracking,

  but nowhere else.

RFID Tag Solutions: Libraries
What's the Use Case?

- Need the data: on exit/entry to library,
  within library for tracking.

Track books (not users).

RFID Tag Solutions: Libraries (policy side)

RFID Tag Solutions: Libraries (policy side)

- Have an effective privacy policy in place.

RFID Tag Solutions: Libraries (policy side)

- Have an effective privacy policy in place.
- All data collected goes to the library **and nowhere else.**

RFID Tag Solutions: Libraries (policy side)

- Have an effective privacy policy in place.
- All data collected goes to the library and nowhere else.
- **Supply appropriate training and education.**

RFID Tag Solutions: Libraries (policy side)

- Have an effective privacy policy in place.
- All data collected goes to the library and nowhere else.
- Supply appropriate training and education.
- **Post policy (e.g., “This library uses RFID technology. It does not collect personal information.”).**

RFID Tag Solutions: Libraries (policy side)

- Have an effective privacy policy in place.
- All data collected goes to the library and nowhere else.
- Supply appropriate training and education.
- Post policy (e.g., “This library uses RFID technology. It does not collect personal information.”).
- **Strive for openness and standardization.**

RFID Tag Solutions: Libraries (policy side)

- Have an effective privacy policy in place.
- All data collected goes to the library and nowhere else.
- Supply appropriate training and education.
- Post policy (e.g., “This library uses RFID technology. It does not collect personal information.”).
- Strive for openness and standardization.
- **Audit regularly and often.**

RFID Tag Solutions: Libraries (technical side)

- Address privacy during design stage.

RFID Tag Solutions: Libraries (technical side)

- Address privacy during design stage.
- RFID use is about book tag, **not** smart cards.

RFID Tag Solutions: Libraries (technical side)

- Address privacy during design stage.
- RFID use is about book tag, not smart cards.
- **Ensure that patron information databases are not linked with tag information databases or tag chips.**

RFID Tag Solutions: Libraries (technical side)

- Address privacy during design stage.
- RFID use is about book tag, not smart cards.
- Ensure that patron information databases are not linked with tag information databases or tag chips.
- **Patron information should only be linked on checkout of media.**

RFID Tag Solutions: Libraries (technical side)

- Address privacy during design stage.
- RFID use is about book tag, not smart cards.
- Ensure that patron information databases are not linked with tag information databases or tag chips.
- Patron information should only be linked on checkout of media.
- **Personal information should not be stored on the RFID tag's chip.**

Guidelines for Using RFID Tags in Ontario Public Libraries

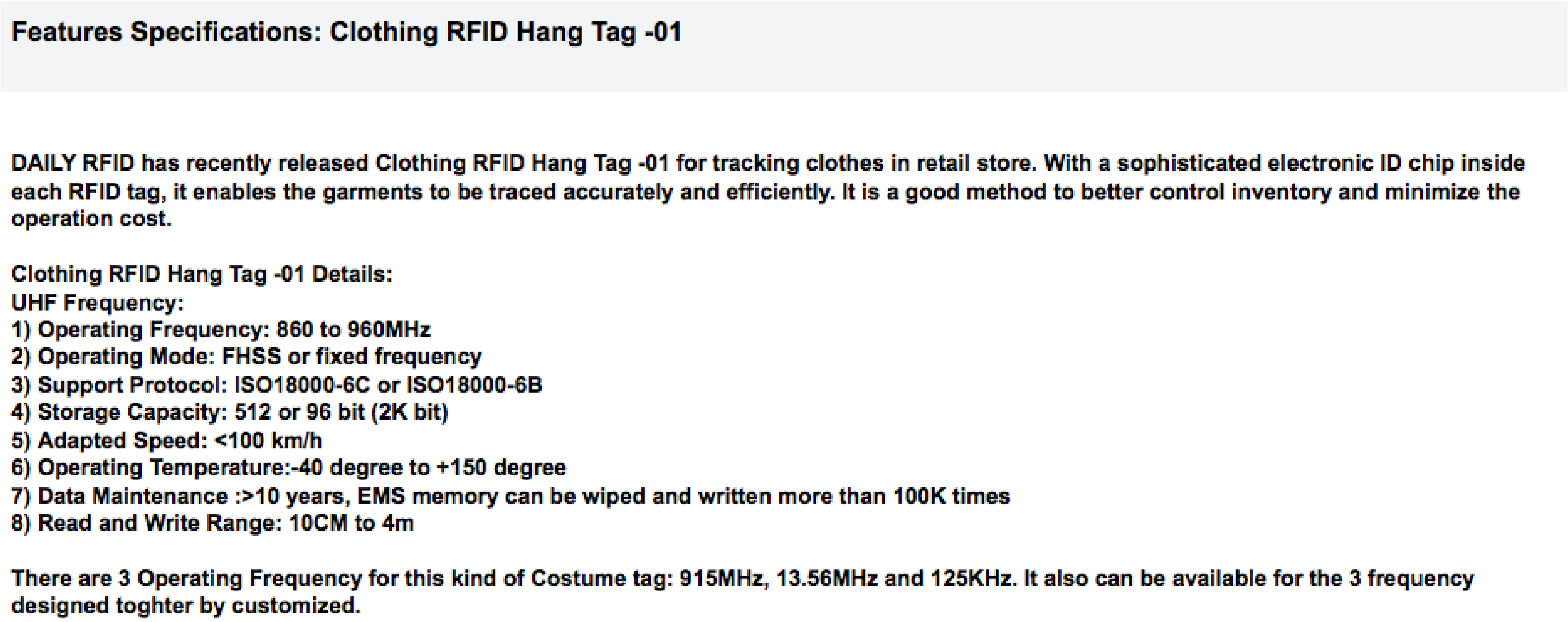
RFID Tags: What's the Technology?

RFID Tags: What's the Technology?

- Passive, active, read only, read-write.
- Encryption on tag.
- Secure communication protocols.
- Authentication of tags and readers.
- Randomized numbering of tags.

RFID Tags Solutions: Consumers

RFID Tags Solutions: Consumers



Features Specifications: Clothing RFID Hang Tag -01

DAILY RFID has recently released Clothing RFID Hang Tag -01 for tracking clothes in retail store. With a sophisticated electronic ID chip inside each RFID tag, it enables the garments to be traced accurately and efficiently. It is a good method to better control inventory and minimize the operation cost.

Clothing RFID Hang Tag -01 Details:
UHF Frequency:
1) Operating Frequency: 860 to 960MHz
2) Operating Mode: FHSS or fixed frequency
3) Support Protocol: ISO18000-6C or ISO18000-6B
4) Storage Capacity: 512 or 96 bit (2K bit)
5) Adapted Speed: <100 km/h
6) Operating Temperature:-40 degree to +150 degree
7) Data Maintenance :>10 years, EMS memory can be wiped and written more than 100K times
8) Read and Write Range: 10CM to 4m

There are 3 Operating Frequency for this kind of Costume tag: 915MHz, 13.56MHz and 125KHz. It also can be available for the 3 frequency designed toghter by customized.

RFID Tags Solutions: Consumers

- Full LINDDUN (**L**inkability, **I**dentifiability, **N**on-repudiation,**D**etectability, Information **D**isclosure, Content **U**nawareness, **N**on-compliance).

RFID Tags Solutions: Consumers

- Full LINDDUN (**L**inkability, **I**dentifiability, **N**on-repudiation,**D**etectability, Information **D**isclosure, Content **U**nawareness, **N**on-compliance).
- Response: De-activate RFID on purchase (European Commission, 2009).

RFID Tags Solutions: Supply Chain

- Partial LINDDUN (**L**inkability, **I**dentifiability, **N**on-repudiation,**D**etectability).

RFID Tags Solutions: Supply Chain

- Partial LINDDUN (**L**inkability, **I**dentifiability, **N**on-repudiation,**D**etectability).
- Tags contain unique identifier.

RFID Tags Solutions: Supply Chain

- Partial LINDDUN (**L**inkability, **I**dentifiability, **N**on-repudiation,**D**etectability).
- Tags contain unique identifier.
- Cloning easy, tracking easy.

RFID Tags Solutions: Supply Chain

- Partial LINDDUN (**L**inkability, **I**dentifiability, **N**on-repudiation,**D**etectability).
- Who's the threat?
- What's the risk?
- Does it make things better than before?

RFID Tags: Privacy Depends on the Use Case

- Library: passive tags, no personal information on tags.
- Consumer: deactivation or removal at point of sale unless opt in (European Commission, 2009).
- Supply chain: currently problematic --- **in theory.**

The Privacy Lessons

- Privacy protections are customized per use case.

The Privacy Lessons

- Privacy protections are customized per use case.
- When use case changes, so do privacy protections.

The Privacy Lessons

- Privacy protections are customized per use case.
- When use case changes, so do privacy protections.
- Privacy tradeoffs are not just about cost.

The Privacy Lessons

- Privacy protections are customized per use case.
- When use case changes, so do privacy protections.
- Privacy tradeoffs are not just about cost.
- Policy role critical.

The Privacy Lessons

- Privacy protections are customized per use case.
- When use case changes, so do privacy protections.
- Privacy tradeoffs are not just about cost.
- Policy role critical.
- In privacy, there are no spherical chickens.