

Security/Privacy Issues

Computer Science and Engineering - University of Notre Dame

What is Privacy?

- * "...the right to be let alone." *Samuel Warren and Louis Brandeis, "The Right to Privacy," Harvard Law Review, 1890*
- * "...the right of the individual to decide for himself, with only extraordinary exceptions in the interest of society, when and on what terms his acts should be revealed to the general public." *Alan Westin Privacy and Freedom, 1967*
- * "Giving consumers control over the collection and use of personal data"

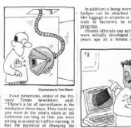
Why is it so important?

- * Privacy empowers people to control information about themselves.
- * Privacy is a utility that protects people against unwanted nuisances, or the right to be left alone.
- * Privacy is a regulating agent in the sense that it can be used to balance and check the power of those capable of collecting data.

Ubicomp and Privacy

* Ubicomp is the potentially inextricable embedding of networked computation into the fabric of society, into the everyday lives of people.

Orwellian Dream Come True: A Badge That Pinpoints You



BY LAWRENCE KLEIN
Illustration by David A. Huxford

Lawmakers Alarmed by RFID Spying

By Rick Bausil | 1 of 2 | by this reporter
10:00 AM Feb. 26, 2008 PT

Lawmakers in several states this week are preparing rules to prevent Wal-Mart radio-frequency identification tags to spy on their customers.

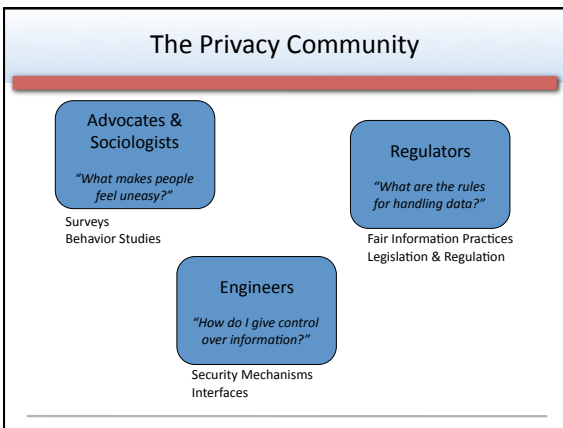
In statehouses in Utah and California, and at the [Federal Reserve Bank of Boston](#), how retailers and government agencies might use the data gathered from RFID tags is a hot topic.

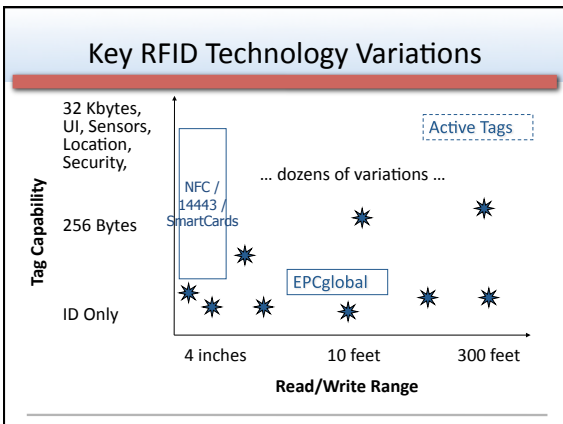
Networking

Commentary: Sprint's GPS technology creates privacy concerns

Last modified November 10, 2008, 3:35 PM PST

[Gather Viewpoint](#)
Special to CHIET News.com





Key Privacy-Sensitive Forms of RFID

- **EPCglobal:** ID number, 20-foot range
 - For supply chain (pallets and cases)
 - What if individual goods are labeled?
 - *REAL ID* (state drivers licenses) is similar to this
- **NFC:** Lots of data, security, 2-inch range
 - Payment cards, cell phones
 - Personal data can be involved
 - *e-Passport* uses NFC, also credit card companies
- **Active RFID:** Idiosyncratic, 300-foot range
 - Person-tracking by employers
 - License plate tracking in UK

Personal Data & Types of “Invasion”

- **Personal Identification**
 - Details about an individual person
 - Primarily in ID documents / badges / cards
 - Privacy violation is “breach”
- **Activity Records**
 - Accumulated based on pseudonym
 - Primarily in consumer goods
 - Privacy violation is “tracking”

PII = Personally Identifiable Information

- Primary category of data protected by “privacy” in US practice
- Many different definitions, here’s one:
 - “any piece of information which can potentially be used to uniquely identify, contact, or locate a single person”
 - Wikipedia says it includes name (if not common), govt. ID #, phone #, street address, email address, vehicle plate #, face / biometric, IP address (sometimes)
 - Fairly loose and squishy definition
 - Different sources have different definitions
- EU “Personal Identification” includes more

RFID Privacy Breaches

- Leak of information through radio
- Collecting information not authorized
- Retaining information not authorized
- Using information in ways not authorized
- Sending information to third parties who are not authorized

- These apply to all IT systems, not just RFID

RFID Radio Security

- Security is to protect data from access by unauthorized parties
- Types of attack:

```
graph TD; AR[Authorized Reader] <--> Tag[Tag]; S[Spoofers] --> AR; E[Eavesdroppers] --> Tag; Sk[Skimmers] --> Tag; T[Tamperers] --> Tag;
```


- Not all systems have adequate security designed in

Tracking


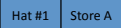
- Activity Records based on pseudonym
- Non-PII Data About Individual
 - New technologies, e.g., RFID, cell phone produce data about things in the world
 - You may leave a “trail of breadcrumbs”
 - Based on pseudonym, not personal ID
 - But the object is yours!
- Actually “trail” ⇒ “mountains”

These data mountains are not considered PII

“Helen Wears a Hat”




- Helen buys a hat at store A.
- The hat contains an RFID tag with a unique ID number.
 - (Even if encrypted it is unique.)
- (The store might record purchase information about Helen, but we will assume they keep it private.)

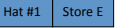
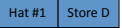
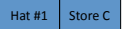
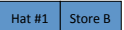


- Helen keeps the RFID tag in the hat because she has a “smart closet”.




“Helen Wears a Hat” – Chapter 2



- Helen visits store B wearing her hat. Store B detects it at the door.



- Helen visits stores C, D, and E, and has lunch with her friend Suzie who has a new sweater.



“Helen Wears a Hat” – Chapter 3

- These stores all sell their data to marketer X, who assembles it and looks for patterns. This information is available to businesses, and is discoverable in legal proceedings.

- ★ Helen’s name and personal data do not appear in the records.
- ★ The usual “privacy policies” and regulations do not apply to this data!

Privacy Breach + Tracking

- Privacy Breach and Tracking have interactions:
 - Breach makes it possible to track
 - Tracking + physical presence can lead to a breach
 - More tracking makes it easier to mine to create a breach
 - Tracking makes the consequences of a breach more serious

Protecting Personal Data

Who does what with your personal data?

- **Sanctioned:**
 - User’s Understanding
 - Authorized Use
 - “Authorization Creep”
 - “Third-Party Freedom”
- **Miscreants:**
 - “Opportunistic”
 - “Professional”
 - “Conspiratorial” (= “Organized”)

↑ Privacy Policy
↓
↑ Privacy & Security
↓

Best Practice Guidelines

- Most experts agree that the primary basis for RFID privacy policy should be Fair Information Practices
 - Many variants, e.g., “Safe Harbor”
 - Notice, Choice, Consent, Security, ...
- This addresses authorized users
- Not always honored by government
 - Identity documents, license plates, etc.
 - Unclear meaning, e.g. what is “consent”?
 - Unclear decision-making process

Privacy Policy for PII: Safe Harbor

- Notice
- Choice & Consent
- Onward Transfer
- Access
- Security
- Data Integrity & Quality
- Enforcement & Remedy

Good reference: *Privacy Best Practices for Deployment of RFID Technology*, Center for Democracy and Technology, 2006.
<http://www.cdt.org/privacy/20060501rfid-best-practices.php>

Security Mechanisms

- **Information Security**
 - Encryption, Authorization, Dynamic IDs, ...
- **Physical Security**
 - On/off switches, Foil covers, Short range, ...
- **Design Security**
 - Opt-in v. opt-out, Default settings, No PII on tags, ...

Resistance to Tracking

- Proposed “privacy” measures:
 - Clipping (IBM): shorten antenna after purchase
 - Killing (EPC): deactivate tag on command
 - Erase the Serial Number: leave the SKU intact
 - Blocker (RSA): device pretends to be every tag
 - Dynamic ID is a new trend in the RFID literature: tag presents apparently random ID
 - Cryptographic techniques for generating a sequence of ID numbers that cannot be inverted
- All of the above have major shortcomings!

Where is the Action Today?

- Guidelines: Industry organizations, standards bodies, privacy advocates
 - Center for Democracy and Technology
- State legislatures in the US
 - CA, IL, WA, NH, AL, ...
- EU, Japan, ...

Common Pitfalls in Proposed RFID Privacy Regulations & Laws

- Overbroad definition of “RFID” includes cell phones, laptops, etc.
 - Example: “RFID means electronic devices that broadcast identification number by radio”
- Regulating technology without limiting data or its use
 - RFID in 2006, what will it be in 2016?
- Ban on technology (reduces innovation)
 - “No RFID until 2010”

Policy Recommendations

- Get good technical guidance!
- Encourage technology development
- Regulate data and its use, not technology
- Foster responsible use
- Codify best practices based on FIP
- Don’t lock in current technologies
- Sensitive applications need careful planning
