

Ethics and Policy Issues in Computing

Jim Herbsleb

1-26-09

Today

- Privacy: intuitions and new technologies
- Planning a paper

- Next time: Lorrie Cranor

Technology and Search

- U.S. Constitution, 4th Amendment:
- "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."
- In general, a warrant is required (many exceptions)
 - Warrantless searches of homes are usually unconstitutional
- Must show a judge "probable cause"
- Question: what is a "search"?

Bugged Phone Booth – Search?

- *Katz v. United States*, 389 U. S. 347 (1967)
 - Using telephone booth to transmit gambling data across state lines
 - “The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment.”
 - Harlan’s concurrence: “that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable.””

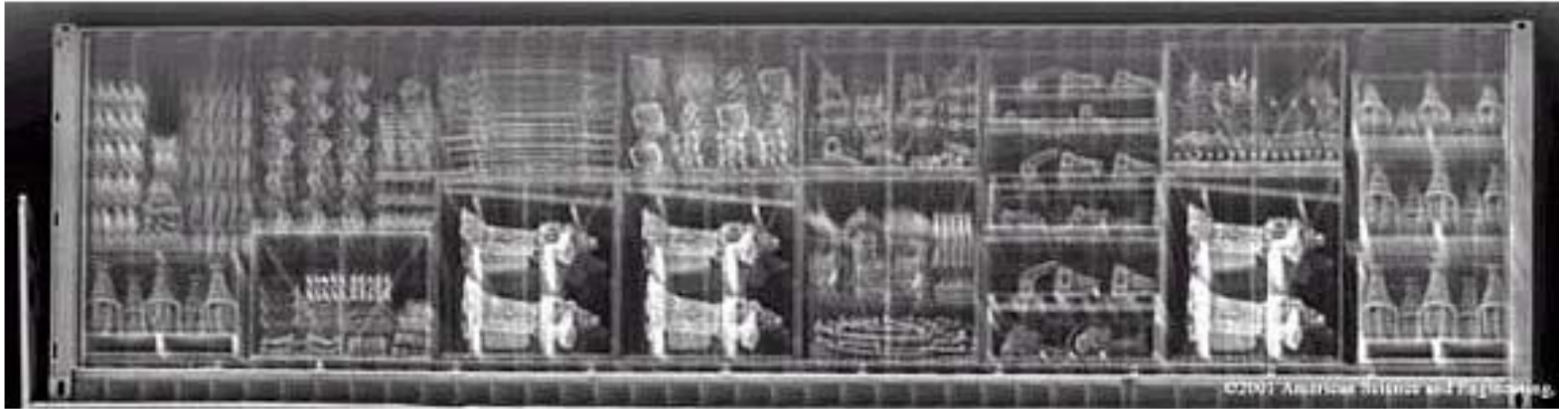
Aerial Photography – Search?

- *California v. Ciraolo*, 476 U.S. 207 (1986)
 - Police suspected marijuana growing in tightly fenced back yard, took aerial photos from 1,000 feet
 - "[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."

Infrared Pictures – Search?

- *Kyllo v. United States*, 533 U.S. 27 (2001)
 - DEA agent suspected that marijuana was being grown in a house using high intensity lamps. Used infrared camera to discover that roof over garage and one wall unusually hot
 - “obtaining by sense-enhancing technology any information regarding the home's interior that could not otherwise have been obtained without physical “intrusion into a constitutionally protected area,” . . . constitutes a search--**at least where (as here) the technology in question is not in general public use.**”
 - “in the sanctity of the home, *all* details are intimate details”

Expectation of Privacy? Decade-old Technologies

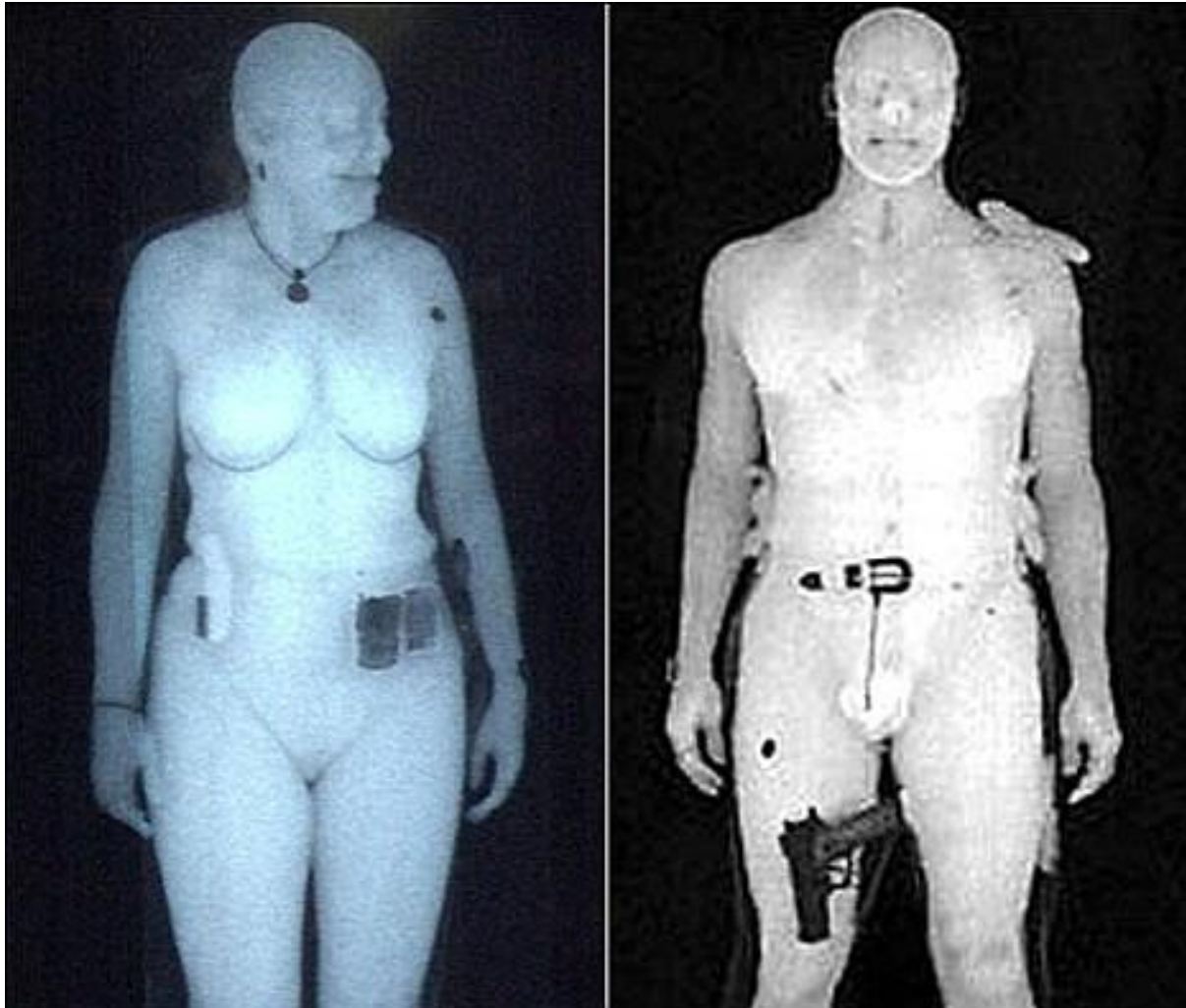


RADAR Flashlight

Georgia Tech RADAR flashlight

<http://gtresearchnews.gatech.edu/newsrelease/RADARFLASH.html>

Airport Surveillance X-rays



The Global Positioning System (GPS)

- Radio-navigation system operated by US DoD
- Comprised of 24 satellites and 5 ground stations
- Uses satellites to triangulate and calculate 3D position from 4 satellite signals
- Receivers listen for radio beacons and triangulate their position
- Typical accuracy in meters, cm accuracy possible
 - DoD intentionally degraded accuracy until May 2000
- One-way system
 - Use other system to report location back
- Does not work indoors

New GPS Application

- Mobile Millennium
- Developed at UC Berkeley
- Traffic reports on cell
- Uses GPS coordinates of all users
- Detects and predicts unusual congestion



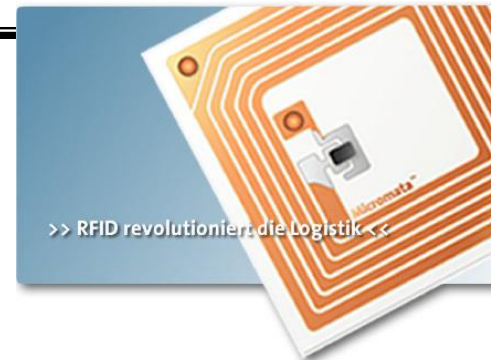
Radio-frequency identification (RFID)

- Tags

- Antenna bonded to small silicon chip encapsulated in glass or plastic (as small as grain of rice)
- Unpowered (passive) tags and powered (active) tags

- Readers

- Broadcast energy to tags, causing tags to broadcast data
- Energy from readers can also power onboard sensors or cause tag to write new data to memory
- Read ranges currently a few centimeters up to a few meters



Source: Sixwise



Current and near term uses of RFID

- Automobile immobilizers
- Animal tracking
- Building proximity cards
- Payment systems
- Automatic toll collection
- Inventory management (mostly at pallet level)
 - Prevent drug counterfeiting
- Passports

Electronic Product Code

- Standard managed by EPCglobal
- Relatively small tags
 - Inexpensive
 - No encryption, limited security
 - Kill feature
 - Password feature
- Designed to replace UPC bar codes
- 96-bit+ serial number
- Object Name Service (ONS) database operated by EPCglobal

Post-sale uses

- Read product labels to blind people
- Sort packaging for recycling
- Provide laundry instructions to washer, dryer, dry cleaner
- Allow smart refrigerator to automatically generate shopping lists and warn about expired items and recalls
- Allow smart closet to suggest outfits
- Simplify product returns

Privacy concerns with EPCs?

- What are the privacy risks?
- What are possible solutions?
- What are the limitations of these solutions?

Credit cards

- Can obtain the following credit card data easily*
 - **Cardholder Name**
 - **Complete credit card number**
 - **Credit card expiration date**
 - **Credit card type**
- Requires only cheap off-the-shelf hardware and software*
- Modest technical skills*
- Solutions involve adding crypto to cards

*Heydt-Benjamin, T.S., Bailey, D.V., Fu, K., Juels, A., & O'Hare, T. (2006). RFID Payment Card Vulnerabilities Technical Report.

http://www.nytimes.com/packages/pdf/business/20061023_CARD/techreport.pdf?scp=6&sq=proximity%20cards&st=cse

Engineering privacy

- Privacy by policy
- Privacy by architecture

Privacy stages	identifiability	Approach to privacy protection	Linkability of data to personal identifiers	System Characteristics
0	identified	privacy by policy (notice and choice)	linked	<ul style="list-style-type: none"> ■ unique identifiers across databases ■ contact information stored with profile information
1	pseudonymous		linkable with reasonable & automatable effort	<ul style="list-style-type: none"> ■ no unique identifies across databases ■ common attributes across databases ■ contact information stored separately from profile or transaction information
2		privacy by architecture	not linkable with reasonable effort	<ul style="list-style-type: none"> ■ no unique identifiers across databases ■ no common attributes across databases ■ random identifiers ■ contact information stored separately from profile or transaction information ■ collection of long term person characteristics on a low level of granularity ■ technically enforced deletion of profile details at regular intervals
3	anonymous		unlinkable	<ul style="list-style-type: none"> ■ no collection of contact information ■ no collection of long term person characteristics ■ <i>k</i>-anonymity with large value of <i>k</i>

Source: Rahul Tongia

Discussion / Q&A
