RFID and personal privacy

California Research Bureau

Sacramento, October 2007

Lee Tien
tien@eff.org

Electronic Frontier Foundation

Empirical verification needed

- "Trustworthiness demands not only that technology providers create hardware and software that embody integrity and provide fundamental security, reliability and privacy protections, *but that all of these elements be demonstrated to the public conclusively*."
  - Microsoft RFID comments to FTC, 2004

Electronic Frontier Foundation

Basic RFID concerns

- Confidentiality
  - Unauthorized* reading/copying?
- Integrity/availability
  - Modification, spoofing, replay attacks?
  - Deletion of tag data?
- Liability for abuse/misuse of tag data?
- *authorized by who?

Electronic Frontier Foundation

Security concerns. . . .

- *"Basic RFID technology does not have necessary technological protections to eliminate the risk of terrorists, criminals, or illegal aliens… spoofing or counterfeiting PASS cards to enter the United States undetected."*

  – Smart Card Alliance

Electronic Frontier Foundation

Fundamental RFID privacy issues

- RF transmissions hard to secure
- RFID tags can hold much information
  - unique static identifier allows *tracking*
- RFID tags often *promiscuous*
  - respond to any compatible reader
- RFID systems are *stealthy*
  - how do ordinary people exert control?*

Electronic Frontier Foundation

RFID: two basic privacy threats

- Exposure/leakage of data on chip
  - skimming or eavesdropping
  - personal data or inventorying
- Tracking
  - static/persistent unique ID
  - distinctive *combination* of type IDs*
- Exacerbated because you don't know if you've been read. . . .

Electronic Frontier Foundation

. . . Enhanced by inference-making

- E.g., associating chip data with other data
  - Corporate, government databases
  - Gov’t has huge appetite for data
- Tracking need not be in real time:
  - if system logs “xy101zzy” now, can get “true name” later

Electronic Frontier Foundation

Special case —information goods

- Books, CDs, DVDs more sensitive
  - Political, religious, cultural beliefs?
- Ex.: Vienna, Austria Main Library
  - RFID tags placed on more than 240,000 books and 60,000 CDs/DVDs
  - Contains ISBN, author, title, location in library, last person who checked it out

Electronic Frontier Foundation

Summary of privacy risks

- Personal data stored on RFID tag
- Inventorying of goods, especially information goods that reveal beliefs
- Cloning: pretending to be you
  - Security risk if used for access control
- Tracking if static unique identifier or constellation of type IDs

Electronic Frontier Foundation

Are the threats real?

- “Read ranges are too short”?
- Many tags (WHTI/EPC) have long read range
- More important: not the right question
  - RSA: attackers don’t need high reliability; “Reading 1% of cards passing by a busy street corner could be good enough for an attacker.”
  - chokepoints (doorways) mean 1-2 feet enough

Electronic Frontier Foundation

EFF in good company

- GAO: *"Key privacy concerns include tracking an individual's movements and profiling an individual's habits, among others"*
- DHS Privacy and Integrity Committee: *"widespread surveillance of individuals…without their knowledge or consent."*
- AeA: *"Perversely maximize the possibility… of an illicit actor 'tracking' a person at very long ranges… would potentially threaten individual U.S. citizen privacy."*

Electronic Frontier Foundation

RSA on tracking (Bailey, Juels 2006)

- *"EPC tags per se . . . are poorly endowed as security devices."*
- *"EPC tags emit static, unique identifiers . . . . Thanks to their identifiers, EPC tags are subject to clandestine tracking; with a network of readers, an entity can correlate sightings of an individual tag —and thus potentially track its bearer."*

Electronic Frontier Foundation

RSA on cloning

- *"EPC tags . . . release their identifiers and product information in a promiscuous manner. Any reader may scan any EPC tag; no access control exists on EPC codes."*
- *"Even without blank tags . . . it is an elementary matter to create wireless devices that . . . perfectly simulate their output."*

Electronic Frontier Foundation

Microsoft: *"new potential for infringements of consumer privacy"*

- Unobtrusiveness
- Uniqueness of ID "*raises the possibility that individual objects might be tracked over time through the accumulated record of their sightings by RFID readers.*"
- Interoperability
- Proliferation: "*risks . . . will increase*"

Electronic Frontier Foundation

Microsoft: “Helen wears a hat”

- Helen wears her hat to Fourth Coffee, which doesn’t bother to read the tags
- But Southridge Video in Blue Yonder Mall has tag readers and poorly trained staff
- Blue Yonder Mall records Helen’s movements in and out of stores
- The data is sold to Tailspin Toys for marketing purposes
- All this data is discoverable (legal sense)
- Is Helen aware of all this?

Electronic Frontier Foundation

Microsoft's key threat scenario

- Person acquires "live" tagged item
- At time of acquisition, "*RFID tag ID can be associated with other personal information*"
- "*The threats are greatest when the item is carried into a public venue in which its tag may be exposed to RFID readers operated by other parties.*"
- = GOVERNMENT ID CARD PROBLEM

Electronic Frontier Foundation

MS privacy vulnerability summary

Enablers

- Item tagging
- Interoperability
- Broadcast range
- Unique ID
- After-purchase use
- Take into public venues

Threats

- Radio snooping
- Network snooping
- Database cracking
- Database selling

RFID Exacerbations

- Intimacy of data
- Accumulation of data
- Distribution of data
- Data handling by untrained people

Electronic Frontier Foundation

Critical case: government applications

- Transport systems, ID cards
  - No choice when government mandates
  - Concern for accountability*
- Likely designed, intended to be:
  - Promiscuous: readable by many sensors
  - Persistent: can't kill tags
  - Pervasive: tags *and* sensors/readers will proliferate in public places (malls, airports, campuses)

Electronic Frontier Foundation

Vermont “enhanced” driver’s license?

- “*At a briefing on Capitol Hill in July, Tres Wiley of Texas Instruments demonstrated for lawmakers and staffers how easy it is to clone a UHF tag*”
- Smart Card Alliance: “*readers can be rendered useless by a commercially available RFID transceiver that is pointed at the CBP antennas*”

Electronic Frontier Foundation

What's the accountability problem?

- GAO noted lack of privacy discussion in federal RFID decision-making
  - as if deciding to use RFID = deciding to buy new chairs
  - burden should be on government
- Industry seems to have strong ex parte channels into gov't decisions, with no privacy advocates or even neutral security researchers involved
- We need good public data

Electronic Frontier Foundation

Again, Microsoft

- "Trustworthiness demands not only that technology providers create hardware and software that embody integrity and provide fundamental security, reliability and privacy protections, *but that all of these elements be demonstrated to the public conclusively*."
  - Microsoft RFID comments to FTC, 2004

Electronic Frontier Foundation

Classic case: RFID and US-VISIT

- Process? Public notice very weak on details
- Alternative technologies?
  - key criterion: "no direct action on the part of the traveler" — excludes many techs
  - anti-privacy — where'd that come from?
- Failure after 15-month trial – GAO
  - "performance and reliability problems"
  - At one site RFID readers correctly ID'd 14% of cars but target read rate 70%
  - Cross-read problem hard to fix

Electronic Frontier Foundation

Claimed benefits must be proven

- We need accurate, reliable data
- Who's got the burden of proof?
  - trust industry?
  - or verify?
- Normally in the law, burden of proof is on those with superior access to information

Electronic Frontier Foundation

Government *and* business

- Not either/or – we're seeing alliance of gov't and commerce
- DoD, transport sector adopting RFID
- Govt not just using but *subsidizing* RFID
  - Scale economies = lower cost
  - Legitimizes RFID use
  - More RFID sensors in everyday life

Electronic Frontier Foundation

RFID as privacy pollution

- Classic “social cost” problem -- RFIDs leak
  - personal information
  - persistent ID # for association, tracking
- But *worse* than ordinary pollution
  - don’t know if your data was captured*
  - “pollution” has value to business, govt**
- So who has incentive to protect privacy?

Electronic Frontier Foundation

Bigger picture around Sutter incident

- *"The envisioned system should … enable the identification, location, and tracking of individuals on school grounds; ideally, visitors and intruders, as well as staff and students. Cooperative identification and tracking is acceptable; <u>however, non-cooperative identification and tracking is desired</u>."*
  - U.S. Department of Justice, "Solicitation for Concept Papers" re new school ID and tracking systems, 10/5/05

Electronic Frontier Foundation

Media gets big picture …

- *"[Some parents in Sutter] realize that unless they protest loudly, other districts and companies will just assume that people think it's no big deal to have their movements monitored and privacy invaded. They're standing up for everyone's rights by refusing to have the wool pulled over their eyes."*
  - Editors, San Jose Mercury News (2/11/05)

Electronic Frontier Foundation

Privacy is dead — get over it?

- RFID presents every concern we already have about the ocean of personal information in today's information society
  - And then adds its own
- Paradigm shift in tracking:
  - Once, tracking required work
  - Now we carry trackable devices, only issue is whether data is being captured

Electronic Frontier Foundation

Can’t look at RFID alone

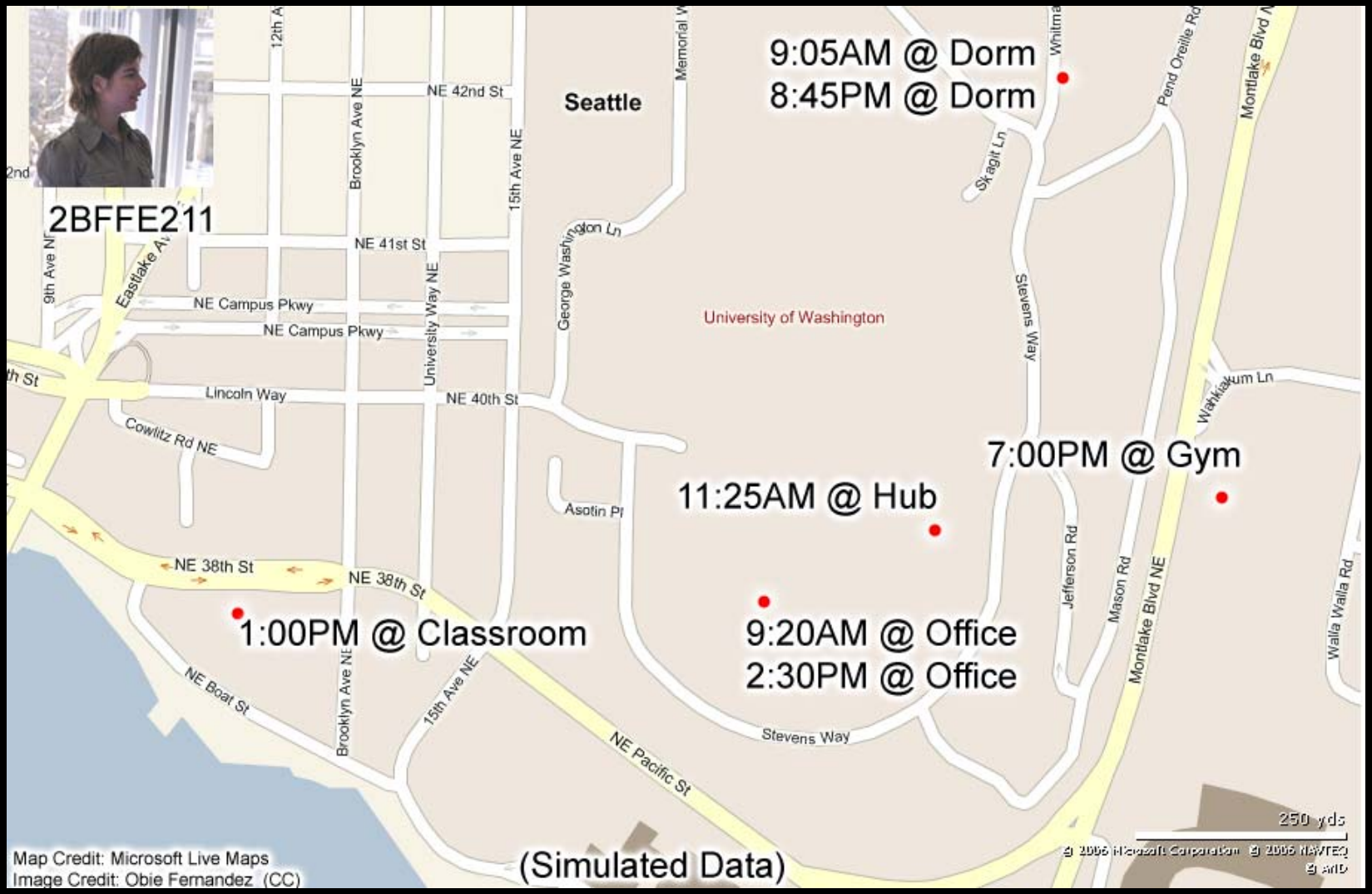
- True that RFID merely one of many privacy threats, but that’s cold comfort
- Technologies *combine* in the real world
- Identification: biometrics as well as RFID
- Location: GPS, videocameras, cellphones
- Data storage: computer databases
- Analysis, profiling: data-mining

Electronic Frontier Foundation

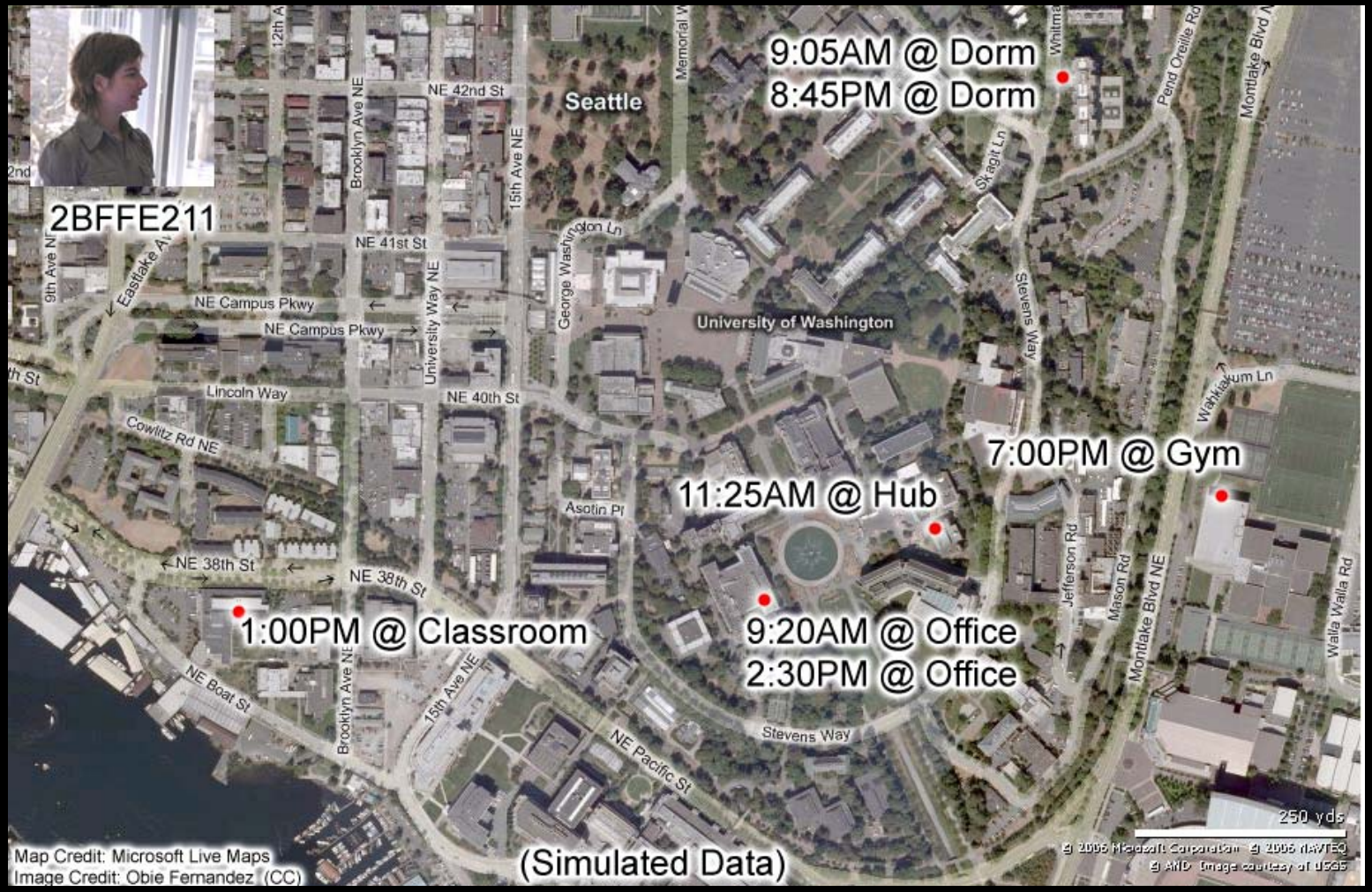
"Devices that Tell on You: the Nike+iPod Sport Kit”

- Kit: shoe chip (size of dinner mint) + receiver (iPod Nano plug-in), records data
- Researchers connected receiver to laptop serial port, wrote app that displayed each device in range (60 feet)
- http://www.cs.washington.edu/research/systems/track.html

Electronic Frontier Foundation



Electronic Frontier Foundation



Electronic Frontier Foundation

AIM Global told Congress

- Consumers should have the rights
- *To know whether products contain RFID*
- *To have RFID removed or deactivated*
- *To opt out of RFID-enabled services*
- *To access RFID tag stored data*
- *To know when, where and why RFID is being used*

Electronic Frontier Foundation

Summary

- Many agree with EFF that RFID poses new privacy and security risks
- Don’t need a genius to build a cloner
- Whatever today’s threat level, it will get worse
- Why wait?

Electronic Frontier Foundation