



Today's Menu

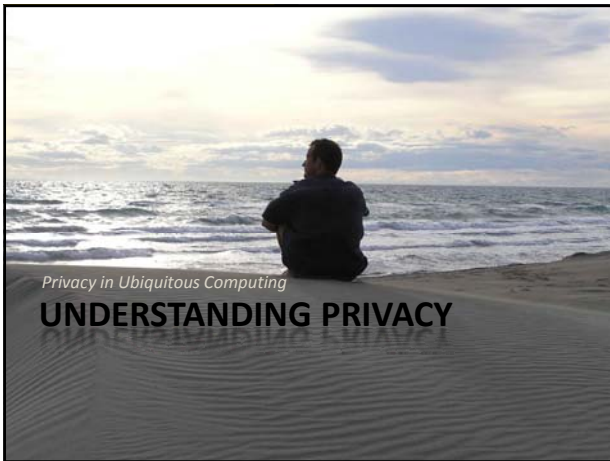


- Understanding Privacy
 - Definitions
 - 1. History and legal aspects
 - 2. Motivating privacy




- Technical Approaches
 - Challenges
 - 1. Location privacy
 - 2. RFID privacy



14



A Privacy Definition

- “The right to be let alone.”
 - Warren and Brandeis, 1890 (Harvard Law Review)
- “Numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the housetops’”



Louis D. Brandeis, no date Samuel D. Warren, c. 1900

Image source: <http://historyofprivacy.net/RPIIntro3-2009.htm>

Technological Revolution, 1888

THE KODAK CAMERA

100 Instantaneous Pictures!

Anybody can use it. No knowledge of photography is necessary.

The latest and best outfit for amateurs.


Send for descriptive circulars.

Price \$35.00.

The Eastman Dry Plate & Film Co.

ROCHESTER, N. Y.

1888




George Eastman
1854-1932

Image Source: Wikipedia; [Encyclopedia Britannica \(Student Edition\)](#)

Information Privacy

- “The desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others.”
 - Alan Westin, 1967
Privacy And Freedom, Atheneum



Dr. Alan F. Westin

18


Privacy Facets

- Bodily Privacy
 - Strip Searches, Drug Testing, ...
- Territorial Privacy
 - Privacy Of Your Home, Office, ...
- Communication Privacy
 - Phone Calls, (E-)mail, ...
- Informational Privacy
 - Personal Data (Address, Hobbies, ...)



Privacy Invasions

- When Do We Feel that Our Privacy Has Been Violated?
 - Perceived privacy violations due to crossing of “privacy borders”
- Privacy Boundaries
 1. Natural
 2. Social
 3. Spatial / temporal
 4. Transitory



Gary T. Marx
MIT

Privacy Borders (Marx)

- Natural
 - Physical limitations (doors, sealed letters)
- Social
 - Group confidentiality (doctors, colleagues)
- Spatial / Temporal
 - Family vs. work, adolescence vs. midlife
- Transitory
 - Fleeting moments, unreflected utterances




Privacy in Ubiquitous Computing


1. HISTORY AND LEGAL ISSUES

Privacy Law History

- Justices Of The Peace Act (England, 1361)
 - Sentences for Eavesdropping and Peeping Toms
- „The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail; its roof may shake; ... – but the king of England cannot enter; all his forces dare not cross the threshold of the ruined tenement“
 - William Pitt the Elder (1708-1778)
- First Modern Privacy Law in the German State Hesse, 1970



Fair Information Principles (FIP)



- Drawn up by the OECD, 1980
 - “Organisation for economic cooperation & development”
 - Voluntary guidelines for member states
 - Goal: Ease transborder flow of goods (and information!)
- Eight Principles
 1. Collection Limitation
 2. Data Quality
 3. Purpose Specification
 4. Use Limitation
 5. Security Safeguards
 6. Openness
 7. Individual Participation
 8. Accountability
- Core principles of modern privacy laws world-wide

Source: Robert Gellman „Fair Information Practices: A Basic History“, <http://hobellman.com/rg-docs/rg-FIPsHistory.pdf>
See also http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1_00.html

Laws and Regulations

- Privacy laws and regulations vary widely throughout the world
- US has mostly **sector-specific laws**, with relatively minimal protections
 - Self-Regulation favored over comprehensive privacy laws
 - Fear that regulation hinders e-commerce
- Europe has long favored strong, **omnibus** privacy laws
 - Often single framework for both public & private sector
 - Privacy commissions in each country (some countries have national and state commissions)

25

US Public Sector Privacy Laws

- Federal Communications Act, 1934, 1997 (Wireless)
- Omnibus Crime Control and Safe Street Act, 1968
- Bank Secrecy Act, 1970
- **Privacy Act, 1974**
- Right to Financial Privacy Act, 1978
- Privacy Protection Act, 1980
- Computer Security Act, 1987
- Family Educational Right to Privacy Act, 1993
- Electronic Communications Privacy Act, 1994
- Freedom of Information Act, 1966, 1991, 1996
- Driver's Privacy Protection Act, 1994, 2000

26

US Private Sector Laws

- Fair Credit Reporting Act, 1971, 1997
- Cable TV Privacy Act, 1984
- Video Privacy Protection Act, 1988
- Health Insurance Portability and Accountability Act, 1996
- Children's Online Privacy Protection Act, 1998
- Gramm-Leach-Bliley-Act (Financial Institutions), 1999
- Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM), 2003

27

EU Privacy Law

- EU Data Protection Directive **1995/46/EC**
 - Sets a **benchmark for national law** for processing personal information in electronic and manual files
 - Expands on OECD Fair Information Practices:
 - no automated adverse decisions
 - minimality principle
 - retention limitation
 - special provisions for "sensitive data"
 - compliance checks
 - Facilitates data-flow between Member States and restricts export of personal data to „unsafe“ non-eu countries

28

National Implementation

- Directive(s) **Transcribed** Into National Law(s)
 - Fines for countries that fail to meet deadline
- National Laws Can Be **Stricter** Than Directive
 - Directive only sets **baseline** privacy level
 - Still **27+3** national regimes (EU+EEA)!
- Data Protection Commissioner **Oversight**
 - Significantly **different powers** in each country: some only „advise“, others can block legislation

EEA: *European Economic Area* (Norway, Lichtenstein, Iceland)
 EFTA: *European Free Trade Association* (EEA+Switzerland)

29

EU Privacy Law

- EU Data Protection Directive **1995/46/EC**
 - Sets a benchmark for national law for processing personal information in electronic and manual files
 - Expands on OECD Fair Information Practices:
 - no automated adverse decisions
 - minimality principle
 - retention limitation
 - special provisions for "sensitive data"
 - compliance checks
 - Facilitates data-flow between Member States and **restricts export of personal data to „unsafe“ non-EU countries**

30

Related EU Directives



- Telecommunications Directive **97/66/EC**
 - Added specific rules for telecommunications systems
- Privacy & Electronic Comm. Directive **2002/58/EC**
 - Updates 97/66 to cover „electronic communications“
- Data Retention Directive **2006/24/EC**
 - Adds provisions for retaining (call, email, Web)-logs
 - Data must be stored for **6-24 months**
 - Member states can go beyond what 2006/24 mandates

See, e.g., <https://wiki.vorratsdatenspeicherung.de/Transposition> for current status of transposition





Privacy in Ubiquitous Computing

2. MOTIVATING PRIVACY


Why Privacy?

- “A free and **democratic society** requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy... privacy is a **key value** which underpins **human dignity** and other key values such as freedom of association and freedom of speech...”
 - Preamble To Australian Privacy Charter, 1994
- “All this secrecy is making life **harder**, more expensive, **dangerous** and less serendipitous”
 - Peter Cochrane, Former Head Of BT Research
- “You have no privacy anyway, **get over it**”
 - Scott McNealy, CEO Sun Microsystems, 1995

36

The NTHNTF-Argument



- „If you’ve got nothing to hide, you’ve got nothing to fear”
 - UK Gov’t Campaign Slogan for CCTV (1994)
- Assumption
 - Privacy is (mostly) about hiding (evil/bad/unethical) **secrets**
- Implications
 - Privacy protects **wrongdoers** (terrorists, child molesters, ...)
 - No danger for **law-abiding** citizens
 - **Society overall better off without it!**

37



Dec. 2009



“If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.” - Google CEO Eric Schmidt



“But I’ve Got Nothing to Hide!”

Do you?

- Arson Near Youth House Niederwangen, CH
 - At scene of crime: Tools from supermarket chain
 - Court ordered disclosure of all 133 consumers who bought items on their supermarket loyalty card (8/2004)
 - (Arsonist not yet found)
- “Give me six lines written by the most honorable of men, and I will find an excuse in them to hang him”
 - Armand Jean du Plessis, 1585-1642 (a.k.a. Cardinal de Richelieu)

Armand Jean du Plessis, 1585-1642 (a.k.a. Cardinal de Richelieu)

Issue: Profiles

- Allow **Inferences** About You
 - May or may not be true (re. AOLStalker!)
- May **Categorize** You
 - High spender, music aficionado, credit risk
- May Offer Or Deny **Services**
 - Rebates, different prices, privileged access
- „**Social Sorting**“ (Lyons, 2003)
 - Opaque decisions „channel“ life choices








Image Sources: http://www.dmmjaneays.com/sketchblog/paperdollmask_large.jpg and <http://www.queensjournal.ca/story/2008-03-14/supplement/kenzie-zaks-personal-data/>

Why Privacy Law?

- As Empowerment
 - “Ownership” of personal data
- As Utility
 - Protection from nuisances (e.g., spam)
- As Dignity
 - Balance of power (“nakedness”)
- As Constraint Of Power
 - Limits enforcement capabilities of ruling elite
- As By-Product
 - Residue of inefficient collection mechanisms




Prof. Lawrence Lessig
Stanford Law School



Source: Lawrence Lessig, Code and Other Laws Of Cyberspace.

Example: Search And Seizures


- 4th Amendment Of US Constitution
 - “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
- Privacy As Utility? Privacy As Dignity?



Source: Lawrence Lessig, Code and Other Laws Of Cyberspace.

Search & Seizures 21st Century

- All Home Software Configured By Law To Monitor For Illegal Activities
 - Fridges detect stored explosives, PCs scan hard disks for illegal data, knives report stabbings
- Non-illegal Activities NOT Communicated
 - Private conversations, actions, remain private
 - Only illegal events reported to police
- No Nuisance Of Unjustified Searches
 - Compatible with 4th amendment?



Source: Lawrence Lessig, Code and Other Laws Of Cyberspace.

Not Orwell, But Kafka!

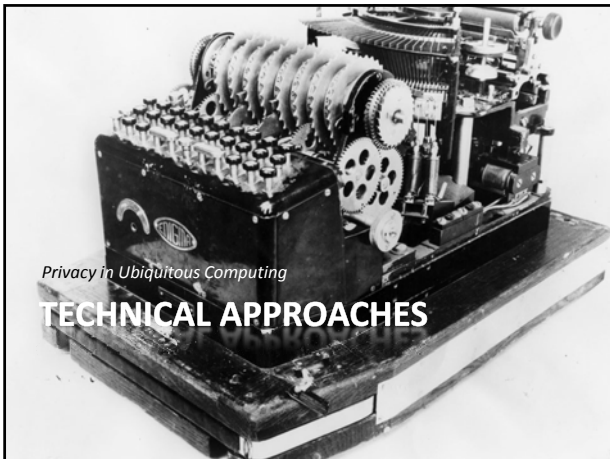


47


Today’s Menu

- Understanding Privacy
 - Definitions
 - 1. History and legal aspects
 - 2. Motivating privacy
- Technical Approaches
 - Challenges
 - 1. Location privacy
 - 2. RFID privacy

48



The Information Society



Paul Sieghart
Portrait by Paul Benny


- **More transactions** will tend to be recorded
- The records will tend to be **kept longer**
- Information will tend to be given to **more people**
- More data will tend to be transmitted over **public** communication channels
- **Fewer** people will know what is happening to the data
- The data will tend to be **more easily accessible**
- Data can be **manipulated**, combined, **correlated**, associated and **analysed** to yield information which could **not** have been obtained without the use of computers"

Paul Sieghart: *Privacy and Computers*. London, Latimer, 1976, pp. 75-76

50

UbiComp Privacy Implications


- Data Collection ("more transactions")
 - Scale (everywhere, anytime)
 - Manner (inconspicuous, invisible)
 - Motivation (context!)
- Data Types ("not without computers")
 - Observational instead of factual data
- Data Access ("more easily accessible")
 - "The Internet of Things"




51

Changing the Playing Field

- UbiComp: The Reversal of Defaults
 - What was once hard to copy is now trivial to duplicate
 - What was once forgotten is now stored forever
 - What was once private is now public
- Challenges for Society
 - New ways of public/private life?
 - New balance between the individual and society?
 - Who is in charge?




Ron Rivest
MIT



52

FIP Challenges in UbiComp


- How to inform subjects about data collections?
 - Unintrusive but noticeable
- How to provide access to stored data?
 - Who has it? How much of this is "my data"?
- How to ensure confidentiality, and authenticity?
 - Without alienating user (think „usability“)!)
- How to minimize data collection?
 - What part of the "context" do we really need?
- How to obtain consent from data subjects?
 - Missing UIs? Do people understand implications?



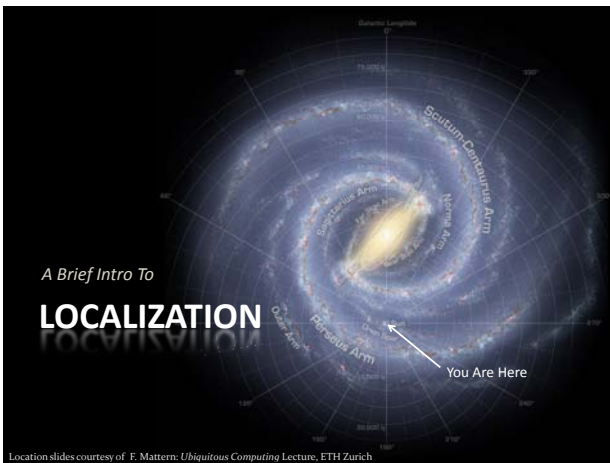
53

Border Crossings in UbiComp

- Smart appliances (natural borders)
 - "Spy" on you in your own home
- Family intercom (social borders)
 - Grandma knows when you're home
- Consumer profiles (temporal borders)
 - Span time & space
- "Memory amplifier" (transitory borders)
 - Records careless utterances



54



Why Location Information?

- Positioning
 - e.g., emergencies
- Navigation and Routing
 - for mobile devices
- Logistics
 - tracking moving objects, monitoring,...
- Resource optimization, energy savings
 - turn down the heating when I am far away
- Location-based services

F.Ma. 56

Location Models

- Geometric („physical“)
 - based on a reference coordinate system (“grid based“)
 - locations and located objects: points, areas, volumes - sets of coordinate-tuples
- Symbolic
 - topology (contained, adjacent,...),
 - typically hierarchically organized (e.g., postal address)
 - human-friendly, but
 - needs to be maintained
 - names depend on the application domain
 - reverse mapping (symbolic to physical) may be not unique
 - limited spatial resolution

F.Ma. 57

Location Technologies

- Various location technologies
- No technology is right for every situation, different considerations
 - cost
 - accuracy
 - scalability
 - indoor / outdoor
 - private / public

F.Ma. 58

Loc. Technology Characterization

- Absolute Positioning
 - w.r.t. Some reference system
- Relative Positioning
 - e.g., measure movement of object
- Tagged
 - locate a marker
- Untagged
 - e.g., vision
- Self-positioning
 - object knows its position
- Remote positioning
 - system is aware of object position

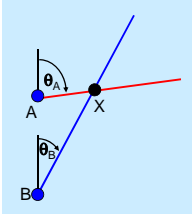
F.Ma. 59

Absolute Positioning: Geometry

- Triangulation (AOA)
 - by taking the bearings of an object from fixed points
- Trilateration (TOA)
 - also called „spherical positioning“
 - by measuring the distance
- Multilateration (TDOA)
 - also called „hyperbolic positioning“
 - by comparing relative distances

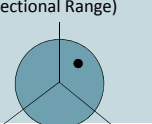
F.Ma./M.La. 60

Angle of Arrival (AOA)



- Angle between sender and receiver
- Needs only 2 transmitters for 2-D positioning!
- Highly range dependent
 - Small measurement errors can lead to big inaccuracies at large distances

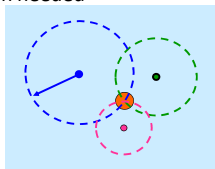
- VOR (VHF Omnidirectional Range) used in aviation
- GSM sector



F.Ma. 61

Time of Arrival (TOA)

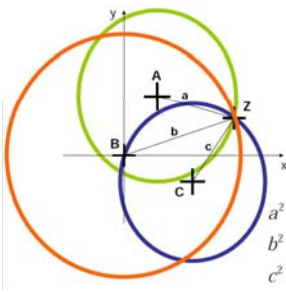
- Delay between sender and receiver
 - propagation time (3 stations for 2-D positioning)
- One-way time: time synchronization needed
 - accurate, stable clocks
 - or 2 signals having different velocity
 - or additional time reference
- Round-trip time
 - no synchronization



■ GPS, Radar

F.Ma. 62

Trilateration



$$a^2 = (y_A - y_Z)^2 + (x_Z - x_A)^2$$

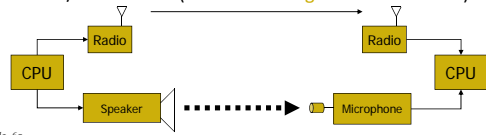
$$b^2 = (y_B - y_Z)^2 + (x_Z - x_B)^2$$

$$c^2 = (y_C - y_Z)^2 + (x_Z - x_C)^2$$

Source: FU Berlin F.Ma. 63

Measuring Time-of-Flight with Two Different Velocities

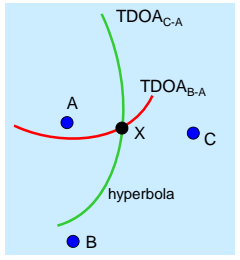
- Radio channel is used to **synchronize** the sender and receiver (over short distances)
- Time-of-flight of **acoustic** signal is determined by comparing arrival of RF and acoustic signals
 - 3ns/m for electromagnetic (i.e., RF) signals
 - 3ms/m for sound (6 orders of magnitude difference!)



F.Ma. 65

Time Difference of Arrival (TDOA)

- Receivers compare **time difference of signal arrival**
 - sent by unknown location X
- In 2D: at least 2 **hyperbolae** required
 - needs 3 receivers A, B, C
- **Synchronization** between reference stations required



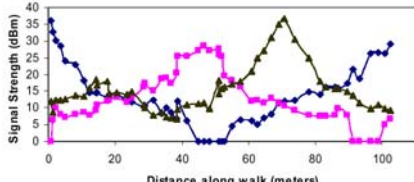
■ mobile phones

F.Ma./M.La. 66

Signal Strength As Distance Measure?

Received Signal Strength Indicator

- In **theory** signal strength (RSSI) **correlates** with distance
- But: Various sources of **errors** (multipath, fading etc.)
 - → not a **monotonic** function!

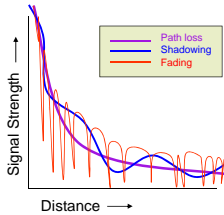


Source: Victor Bahl, Microsoft Research

F.Ma. 67

Practical Difficulties with RSSI


- **Path loss** characteristics depend on environment ($1/r^n$)
- **Shadowing** depends on environment
- Short-scale **fading** due to **multipath**
 - adds random high frequency component with huge amplitude (30-60dB)
 - mobile nodes might average out fading, but static nodes can be stuck in a deep fade



F.Ma. 68

Fingerprinting

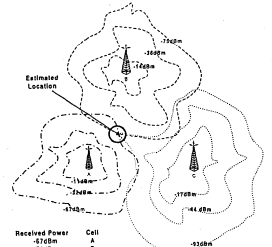
- **Have I seen this before?**
 - correlation with past observations
 - need to keep track of environmental properties
 - works with: vision, radio signals, etc.
- Requires **learning phase**
 - connect true locations with observations in database
 - e.g., tabulate <location, signal strength> information
- **Recognition phase**
 - make observations (e.g., signal strength from base stations)
 - find entry that "best" matches the observation



M.La. 69

Signal Strength Fingerprinting

- **Map of signal distribution**
 - measured
 - model, calculated
- **Errors**
 - obstacle
 - multipath



Received Power
 Cell A: 37dBm
 Cell B: 35dBm
 Cell C: 33dBm

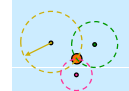
Estimated Location

- Must be periodically retrained, as environment changes (base stations)

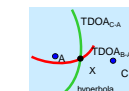
F.Ma. 70

Summary: Absolute Positioning

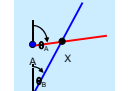
TOA - time of arrival



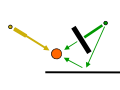
TDOA - time difference of arrival



AOA - angle of arrival



Signal strength



Absolute positioning methods do not rely on knowledge of previous positions

F.Ma. 75

Relative Positioning

Distance

- **distance** itself (odometer)
- **velocity** (speedometer)
- **acceleration**


$$x = \iint a(t) dt dt$$

- **height** (e.g., barometer)

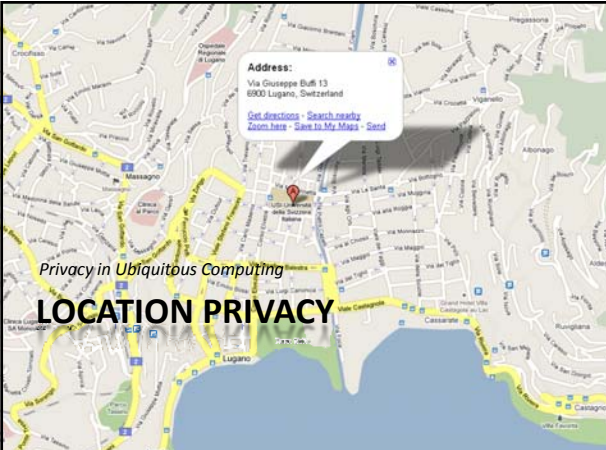
- **Inertial Navigation System (INS)** used in aviation
- **Car navigation** (also uses compass)

Orientation in space

- **gyroscope** (rigid in space)



F.Ma./M.La. 76



Address:
Via Giuseppe Buffi 13
6900 Lugano, Switzerland

Get directions · Search nearby
Zoom here · Save to My Maps · Share

Privacy in Ubiquitous Computing

LOCATION PRIVACY


Location Privacy

- “... the ability to prevent other parties from learning one’s current or past location.”
(Beresford and Stajano, 2003)
- „It’s not about where you are... It’s where you have been!”
 - Gary Gale, Head of UK Engineering for Yahoo! Geo Technologies




Motivating Disclosure

- Why Share Your Location?
 - By-product of positioning technology (e.g., cell towers, WiFi, ...)
 - Required to use service (local search, automated payment for toll roads, ...)
 - Social benefits (let friends and family know where I am, finding new friends, ...)
- Why NOT to Share Your Location?
 - Location profiles **reveal/imply** activities, interests, identity




Location Implications

- Places I Go
 - Where I Live / Work
 - Who I Am (Name)
 - Hobbies/Interests/Memberships
- People I Meet
 - My Social Network
- Profiling, e.g.,
 - ZIP-Code: implies income, ethnicity, family size



Location Privacy Technology


- Many Proposals
 - Laws/regulations and audits (enterprise privacy)
 - Anonymization (“k-anonymity”)
 - Obfuscation
 - Rule-based access control
- Privacy Model?
 - Assumption: Less location disclosure means more privacy
- (Krumm, 2008) Provides Overview of State-of-the-Art



Location Anonymity

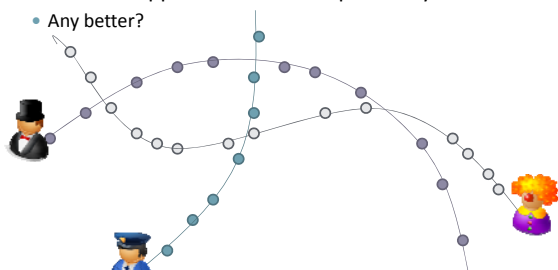
[Naïve Approach]

- Use random IDs that change periodically
 - Trivial to trace




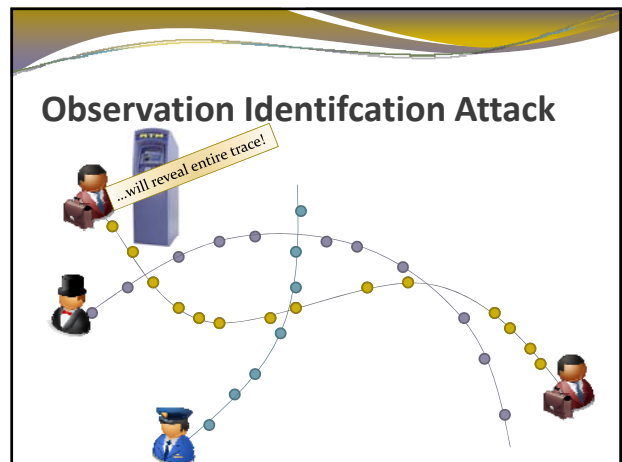
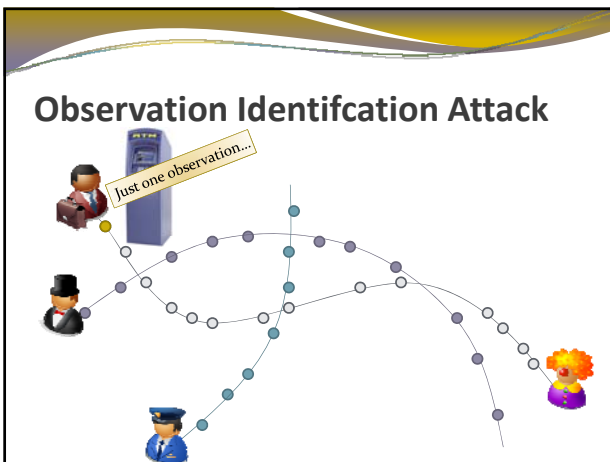
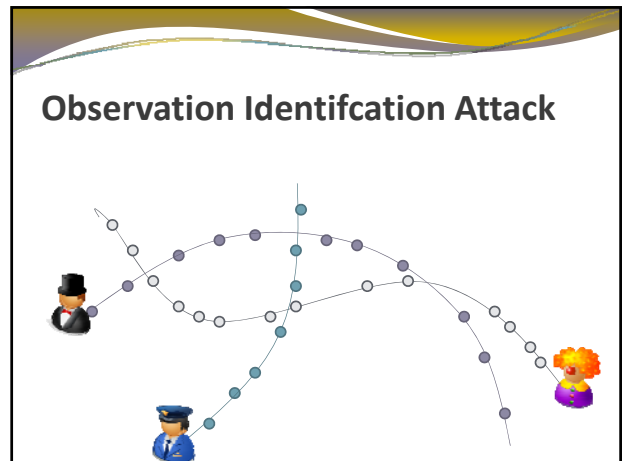
Might As Well Use Pseudonyms

- Since naïve approach is trivial to pseudonymize
 - Any better?




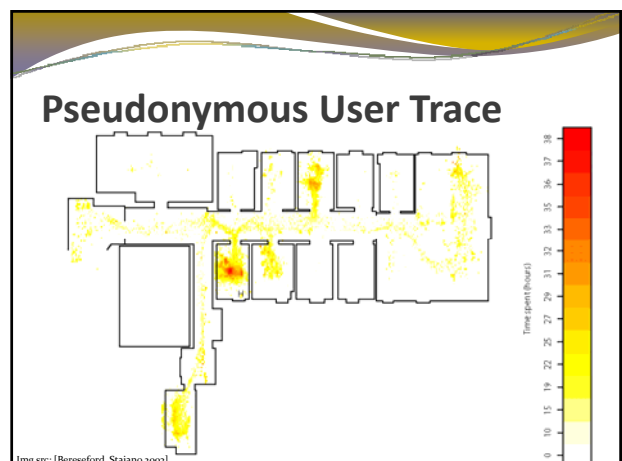
Why Pseudonyms Don't Work

- Observation Identification (OI) Attack
 - Correlate **single identifiable observation** with location pseudonym
 - ATM use @ location -> Name for pseudonym

Why Pseudonyms Don't Work

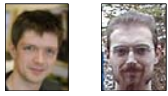
- Observation Identification (OI) Attack
 - Correlate **single identifiable observation** with location pseudonym
 - ATM use @ location -> Name for pseudonym
- Restricted Space Identification (RSI) Attack
 - Works without direct observations
 - Uses **known mapping** from place to name
 - Home location -> Home address -> Name (Phonebook)

Challenge: Where to setup such Mix Zones? And what if no one's there (late night)?

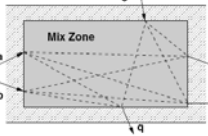
Location Mix Zones

- Address Restricted Space Identification Attacks
 - How to change pseudonyms?
- Idea: Designate "Mix Zones" With No Tracking / LBS Active
 - Change pseudonyms only within mix zone
 - (Beresford and Stajano, 2003) offer probabilistic model for unlinkability in mix zones




Alastair Beresford
Cambridge Univ.

Frank Stajano
Cambridge Univ.




Location Obfuscation



- Adding noise, perturbation, **dummy traffic** to location data
 - Protects against attackers, but **degrades service use**
 - (Krumm, 2007) showed that **LOTS** of obfuscation is needed
 - Typically combined with rules to selectively adjust accuracy

Image Source: Krumm, J., Inference Attacks on Location Tracks, in Fifth International Conference on Pervasive Computing (Pervasive 2007), 2007, Toronto, Ontario Canada, p. 127-143.

Track Obfuscation




Speed Histogram From Highway to Ramp

Speed (meters/second)	Normalized Frequency
2.5	0.00
7.5	0.05
12.5	0.10
17.5	0.35
22.5	0.25
27.5	0.25
32.5	0.05

- Location *tracks* more difficult to fake! Requires
 - Believable **speeds** (existing speed limits)
 - Realistic start/end-points, **trip times** (duration, days)
 - Suboptimal **routes** (human driver vs. route planner)
 - Expected GPS noise (higher in urban environments)

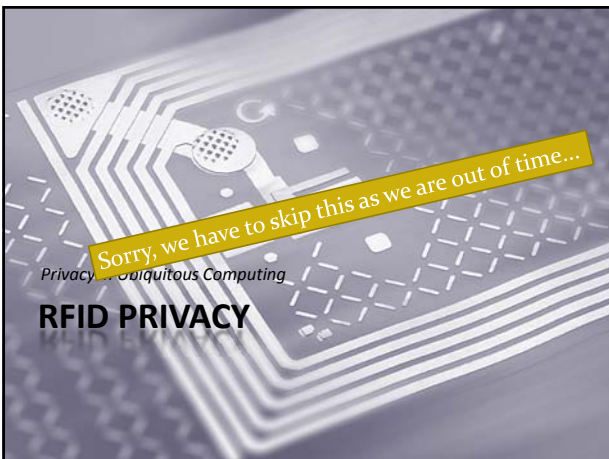
Krumm, J., Realistic Driving Tracks for Location Privacy, in 7th International Conference on Pervasive Computing (Pervasive 2009), Nara, Japan, Springer.

Summary: Location Privacy



- Location popular information to share
 - Location-based Web search
 - Friend finder, local recommendations
- Location traces as source for profiling
 - Imply activities, interests, friends, \$\$, ...
- Simple anonymization does not work
 - Observation Identification Attack
 - Restricted Space Identification Attack
- Solutions? Mix Zones, Obfuscation, Dummy Traffic, ...

93



Sorry, we have to skip this as we are out of time...

Privacy in Ubiquitous Computing

RFID PRIVACY




Summary and Outlook


Img src: www.flickr.com/photos/11896427@N00/431005441/

Beware the Techno Fallacies!

- “if some is good, more is better”
- “only the computer sees it”
- “that has never happened”
- “facts speak for themselves”
- “if we have the technology, why not use it?”
- “technology is neutral”



Gary T. Marx
MIT



Melvin C. Kranzberg
Georgia Tech (1917-1995)

Technology Is Neither Good Nor Bad. Nor Is It Neutral
Melvin C. Kranzberg

Source: G. Marx, “Some Information Age Techno-Fallacies,” Contingencies and Crisis Management, 1(1), March 2003, pp. 25-31. See also <http://www.digital-privacy.org/essential/techno-fallacies.html>

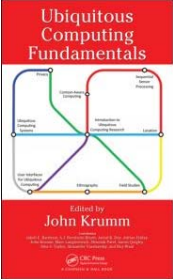
Take Home Message

- Privacy is Not Just Secrecy and Seclusion!
 - Privacy is a process, not a state
 - Solution requires good understanding of social, legal, and policy issues involved
- Ubiquitous Computing Offers New Challenges
 - Invisible, comprehensive, sensor-based, ...
- Ubicomp (Privacy) Challenges
 - User interface (notice, choice, consent)
 - Protocols (anonymity, security, access)
 - Social compatibility (privacy boundaries)








Ubiquitous Computing



- John Krumm (ed): Ubiquitous Computing Fundamentals. Taylor & Francis, 2009
- With Contributions From:
 - Roy Want
 - Jakob Bardram and Adrian Friday
 - Marc Langheinrich
 - A.J. Bernheim Brush
 - Alex S. Taylor
 - Aaron Quigley
 - Alexander Varshavsky and Shwetak Patel
 - Anind K. Dey
 - John Krumm




General Privacy Reading

- David Brin: The Transparent Society. Perseus Publishing, 1999
- Simson Garfinkel: Database Nation – The Death of Privacy in the 21st Century. O’Reilly, 2001
- Lawrence Lessig: Code and Other Laws of Cyberspace. Basic Books, 2006 <http://codev2.cc/>

Privacy Law

- Rotenberg: The Privacy Law Sourcebook 2004. EPIC, 2004
- Privacy & Human Rights 2006. EPIC
- Solove, Schwartz: Information Privacy Law. 3rd edition, Aspen, 2009

Privacy and Technology

- Deborah Estrin (ed.): Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers. National Academies Press, 2001. <http://www.nap.edu/openbook.php?isbn=0309075688>
- Waldo, Lin, Millett (eds.): Engaging Privacy and Information Technology in a Digital Age. National Academies Press, 2007.
- Wright, Gutwirth, Friedewald, et al.: Safeguards in a World of Ambient Intelligence. Springer, 2008

