The Case For Ubicomp Privacy

Marc Langheinrich
ETH Zurich

RESEARCH GROUP FOR
Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

What's Up?

- Privacy Definitions
  - What Is Privacy, Anyway?
- Privacy Motivation
  - Why Should We (Not) Want Privacy?
- Privacy Evolution
  - How Is Privacy Changing?
- Privacy Threats
  - Why Should We Care?
- Privacy Solutions
  - How Can We Achieve Privacy?

1. Privacy Definition

What is Privacy, Anyway?

RESEARCH GROUP FOR

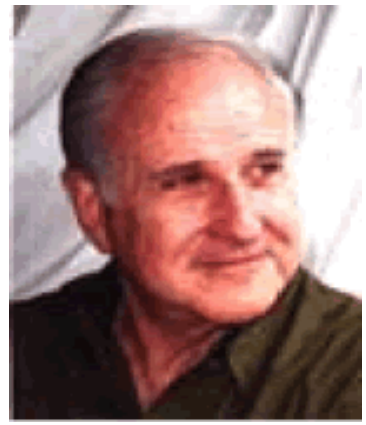
Distributed Systems

What Is Privacy?

- „The right to be left alone.“
  - Louis 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, 1856 - 1941

What Is 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“)

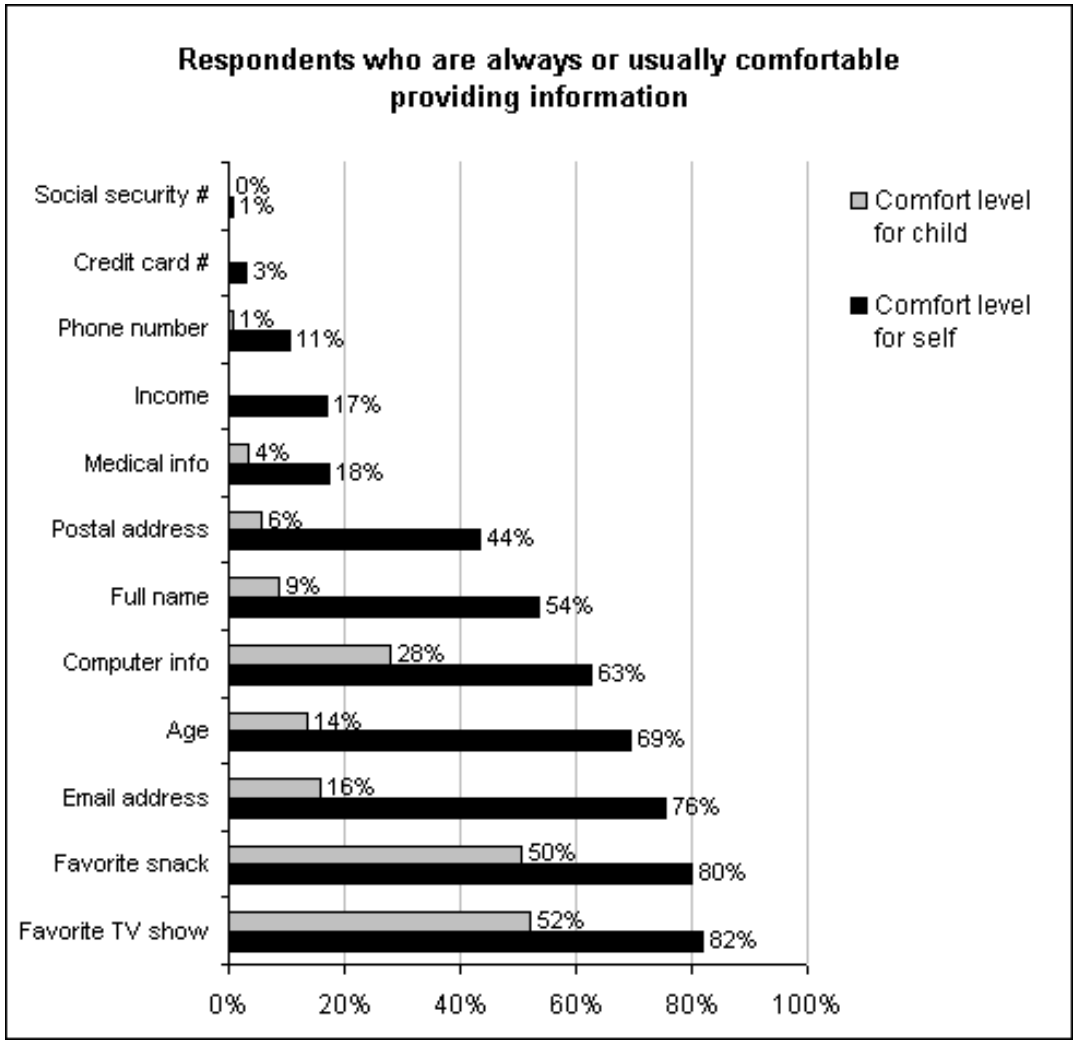
Facets

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

Informational Privacy

- Preferences Vary
  - Willingness to Disclose Personal Data is Highly Context-Specific
- April 1999 Study „Beyond Concern“
  - Internet users more likely to provide information when they are not identified
  - Acceptance of persistent identifiers (e.g. cookies) varies according to purpose
  - Some types of data more sensitive than others

What Data Is Private?



Source: Cranor, Reagle, Ackerman „Beyond Concern: Understanding Net Users' Attitudes About Online Privacy"

Do People Care?

- Harris-Westin US Survey (1995,1996)
  - 24% Have Personally Experienced A Privacy Invasion
  - 80% Feel That Consumers Have Lost All Control Over How Personal Information About Them Is Circulated And Used By Companies
- Japan's Ministry Of Postal & Telecomm. Survey (1999, Interview With 968 Adults)
  - 70% Have Interest In Privacy Protection
  - 92% Fear That Personal Information Is Used Unknowingly

Regional Differences

- IBM-Harris Multinational Survey
  - Phone Interviews With 1000+ Adults In Each Of Three Countries: US, UK And Germany (10/1999)
  - US:
    - Greatest Trust In Companies, But
    - Most Likely To Actively Protect Privacy
  - Germany:
    - Most Comfortable With Governmental Privacy Protection

Loyalty Card Programs

- Free Customer Card
  - Purchases Accumulate “Points”
- Often Sweeping Privacy Statements
  - Consumers Agree To Usage Of Data For Marketing Purposes And Transmission To Undisclosed Recipients
- Emnid Survey, March 2002 (Germany)
  - 50% Got At Least 1 Loyalty Card
  - 72% Think Positively About Such Programs

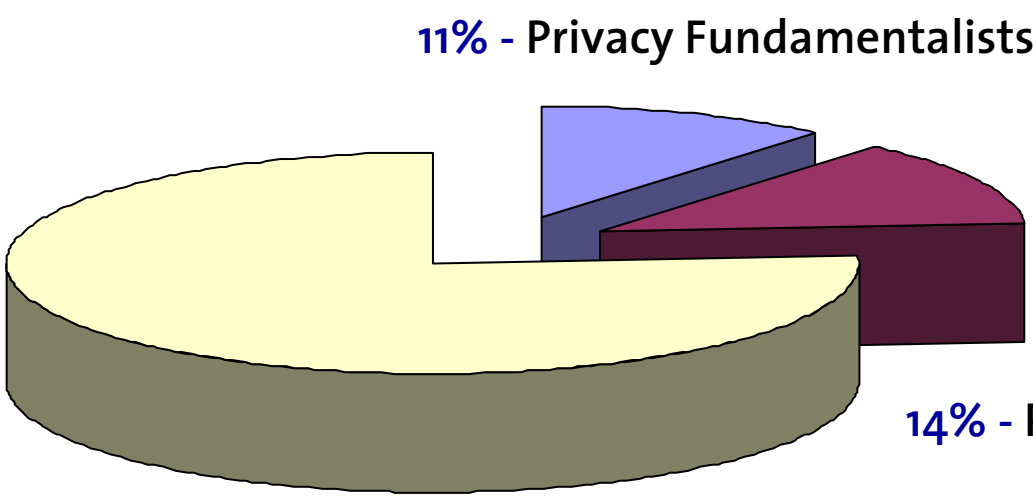
PAYBACK

Privacy Types

- Clustering According To Alan Westin, 1991
- Privacy Fundamentalist
  - Extremely Concerned
  - Generally Unwilling To Provide Data
- Privacy Pragmatic
  - Concerned, But Less So
  - Often Specific Concerns And Particular Tactics
- Privacy Unaware
  - Generally Willing To Provide Data
  - Often Expressing A Mild General Concern

Differing Dispositions

- 1999 Privacy & American Business National Survey (1014 Adults)



Source: http://www.privacyexchange.org/iss/surveys/sr990714.html

Functional Definition

- Privacy Invasive Effects Of Surveillance And Data Collection Due To Crossing Of Personal Borders
  - Prof. Gary T. Marx, MIT
- Privacy Boundaries
  - Natural
  - Social
  - Spatial / Temporal
  - Ephermal / Transitory

Privacy Boundaries

- Natural
  - Physical Limitations (Doors, Sealed Letters)
- Social
  - Group Confidentiality (Doctors, Colleagues)
- Spatial / Temporal
  - Family vs. Work, Adolescence vs. Midlife
- Transitory
  - Fleeting Moments, Unreflected Utterances

Examples: Border Crossings

- Smart Appliances
  - "Spy" On You In Your Own Home (Natural Borders)
- Family Intercom
  - Grandma Knows When You're Home (Social Borders)
- Consumer Profiles
  - Span Time & Space (Spatial/Temporal Borders)
- "Memory Amplifier"
  - Records Careless Utterances (Transitory Borders)

2. Privacy Motivation

Why Should We Want Privacy?

RESEARCH GROUP FOR

Distributed Systems

1. Privacy Definitions
   What is Privacy, Anyway?
2. Privacy Motivation
   Why Should We Want Privacy?
3. Privacy Evolution
   How is Privacy Changing?
4. Privacy Threats
   Why Should We Worry?
5. Privacy Solutions
   How can we achieve 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

Privacy History

- Justices Of The Peace Act (England, 1361)
- „The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter – but the king of england cannot enter; all his forces dare not cross the threshold of the ruined tenement“
  - William Pitt, English Parliamentarian, 1765

Privacy History II

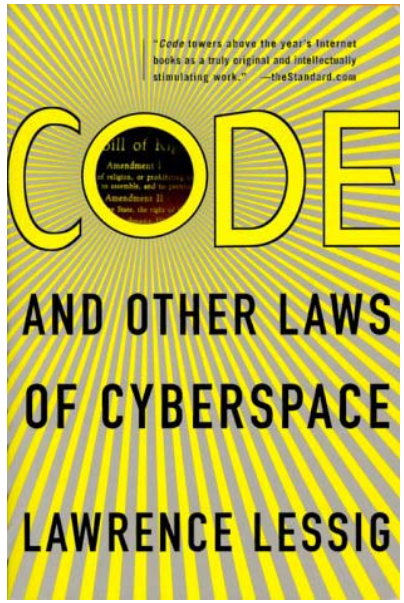
- 1948 United Nations, Universal Declaration Of Human Rights: Article 12
  - No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks
- 1970 European Convention On Human Rights: Article 8 – Right To Respect For Private And Family Life
  - Everyone has the right to respect for his private and family life, his home and his correspondence …
- First Data Protection Law Of The World: State Of Hesse, Germany (1970)

Privacy Sells

- 03/1999: IBM Shows Ads Only On Websites With Privacy Policy
  - 2nd Largest Web Advertiser
- 02/2000 Doubleclick Announces Plans To Merge "Anonymous" Online Data With Personal Information Obtained From Offline Databases
  - Stock Dropped From $125 (12/99) To $80 (03/00)

Driving Factors

- 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



Source: Lawrence Lessig, Code and Other Laws Of Cyberspace. Basic Books, 2000

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?

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, Knifes 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?

Privacy vs. Safety

- Strong Encryption
  - Prevents Law Enforcement From Watching Criminals
- Id-cards Including Biometrics
  - Better Protection From False Identities
- Compulsive HIV Testing Of Infants
  - Increases Life Expectations Of Infants Born To Hiv-positive Mothers
- Registration Of Released Prisoners
  - Informs Community About Potential Offenders

Megan's Law

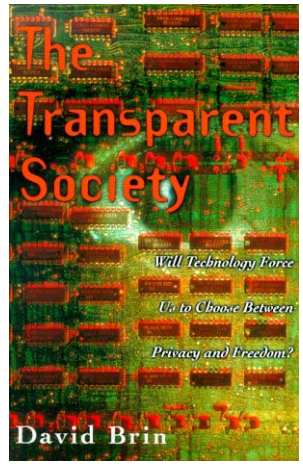
- Named After Megan Kanka (1987-1994)
  - Raped And Strangled By A (New) Neighbor, Who Had Previously Been Convicted Of Two Sexual Assaults Against Young Girls
- 1994 Congressional Guidelines
  - Encourages States To Pass Laws Requiring Registration Of "Sex Offenders" With Local Law Enforcement
  - Enacted By All US States (With Varying Requirements)

Megan's Law: Issues

- Privacy Of Offender Vs. Safety Of Community
  - Are Offenders Punished Twice For The Same Crime? (5th Amendment)
  - Often Compared To Jews Having To Wear Star Of David In Nazi Germany
  - Studies Find Between 76.9% (Switzerland, 1973), 55.6% (Mass., 1979) And 3.7% (UK, 1978) Repeated Offenders
    - Often Higher Numbers For Robberies, Assaults

Watching The Watchers

- Mutually Assured Surveillance
  - All Have Access To (Almost) All Data
- Reciprocal Accountability
  - Restaurant Analogy: No One Openly Stares
- "An Armed Society Is A Polite Society"
  - John Campell, 1940

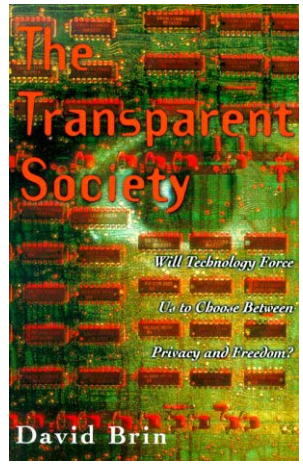


David Brin: The Transparent Society

- Reason: There Are No Secrets For The Powerful
  - Secrecy And Privacy Protects Only Elite

Brin's Assumptions

- Powerful Elite Will "Play Along"
  - Or At Least Will Be Caught Quickly When Trying Not To
- People Respect Non-conformists
  - Or At Least Learn To Tolerate Them



David Brin: The Transparent Society

- Reason: There Are No Secrets For The Powerful
  - Secrecy And Privacy Protects Only Elite

3. Privacy Evolution

How is Privacy Changing?

RESEARCH GROUP FOR

Distributed Systems

Collection Parameters

- Scale
  - To What Extend Is My Life Visible To Others?
- Manner
  - How Obviously Is Data Collected?
- Type
  - What Type Of Data Is Recorded?
- Motivation
  - What Are The Driving Factors?
- Accessibility
  - How Do I Find Anything in this Data?

Collection Scale

- Before: Public Appearances
  - Physically Separated In Space And Time
- Today: Online Time
  - Preferences & Problems (Online Shopping)
  - Interests & Hobbies (Chat, News)
  - Location & Address (Online Tracking)
- Tomorrow: The Rest
  - Home, School, Office, Public Spaces, ...
  - No Switch To Turn It Off?

Collection Manner

- Before: Reasonable Expectations
  - You See Me – I See You
- Today: Visible Boundaries
  - Online, Real-world Electronic Transactions
- Tomorrow: Invisible Interactions
  - Interacting With A Digital Service?
    - Life Recorders, Room Computers, Smart Coffee Cups
  - No Blinking „Recording Now“ LED?

Collection Types

- Before: Eyes & Ears
- Today: Electrical And Digital Surveillance Tools
- Tomorrow: Better Sensors
  - More Detailed & Precise Data
  - Cheaper, Smaller, Self-powered (Ubiquitous!)
- Do I Know Myself Best?
  - Body Sensors Detect Stress, Anger, Sadness
  - Health Sensors Alert Physician
  - Nervous? Floor & Seat Sensors, Eye Tracker

Collection Motivation

- Before: Collecting Out-of-ordinary Events
- Today: Collecting Routine Events
- Tomorrow: Smartness Through Pattern Prediction
  - More Data = More Patterns = Smarter
  - Context Is Everything, Everything Is Context
- Worthless Information? Data-mining!
  - Typing Speed (Dedicated?), Shower Habits (Having An Affair?), Chocolate Consumption (Depressed?)

Collection Accessibility

- Before: Natural Separations
  - Manual Interrogations, Word-of-Mouth
- Today: Online Access
  - Search Is Cheap
  - Database Federations
- Tomorrow: Cooperating Objects?
  - Standardized Semantics
  - What Is My Artifact Telling Yours?
  - How Well Can I Search Your Memory?

4. Privacy Threats

Why Should We Worry?

RESEARCH GROUP FOR

Distributed Systems

A Glimpse Of The Future?

See http://www.privacyfoundation.org/

Creative Labs Nomad JukeBox
Music transfer software reports all uploads to Creative Labs.

http://www.nomadworld.com/welcome.asp

Sony eMarker
Lets you figure out the artists and titles of songs you hear on the radio. And keeps a personal log of all the music you like on the emarker Web site.

http://www.emarker.com

Sportbrain
Monitors daily workout. Custom phone cradle uploads data to company Web site for analysis.

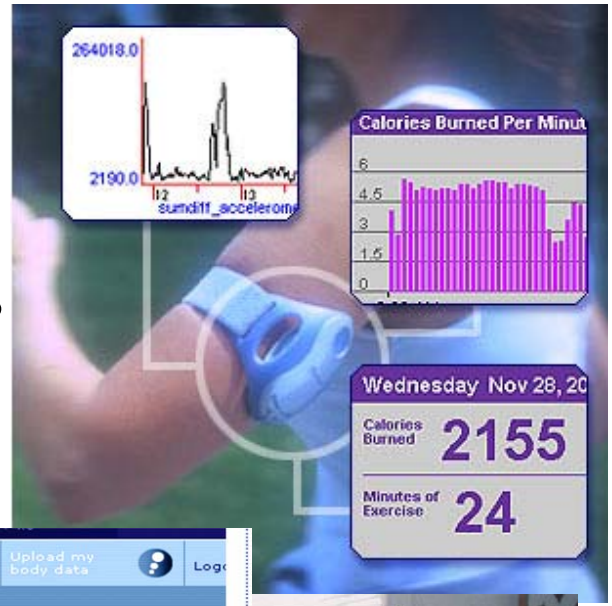
http://www.sportbrain.com/

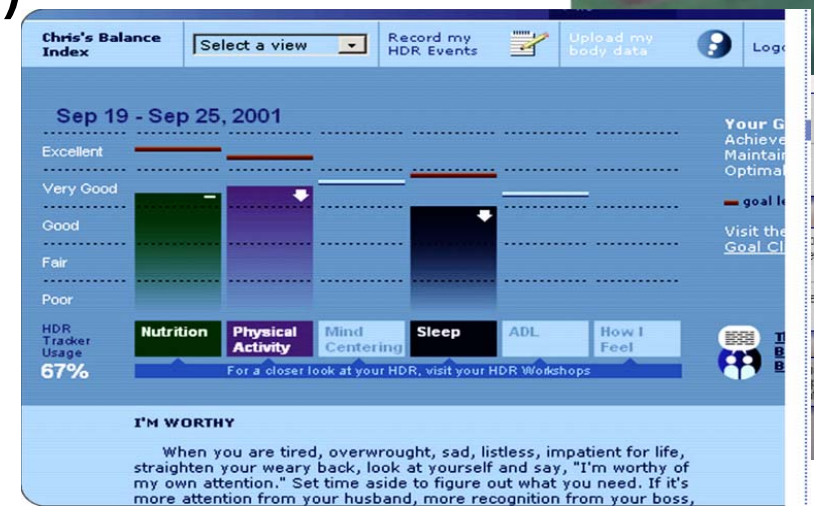
:CueCat
Keeps personal log of advertisements you're interested in (on CueCat Web site).

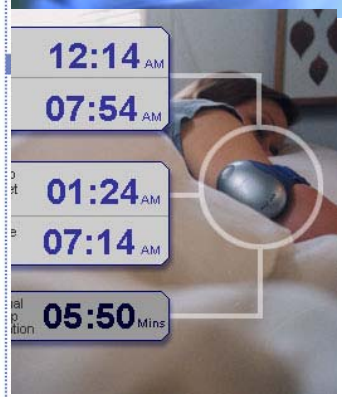
http://www.crq.com/cuecat.html

Bodymedia

- Communication Platform for wireless Transmission of Body Sensor Readings
- Bodymedia Data Center translates Raw Data into „Lifestyle Data“ (accessible via Web Interface on Company-Site)







Quelle: http://www.bodymedia.com

Virtual Dad

- Road Safety International Sells "Black Box" for Car
  - Detailed Recording of Position (soon), Acceleration, etc.
  - Audio Warnings When Speeding, Cutting Corners
  - Continuous Reckless Driving is Reported Home
- Sold as Piece of Mind for Parents
  - "Imagine if you could sit next to your teenager every second of their driving. Imagine the control you would have. Would they speed? Street race? Hard corner? Hard brake? Play loud music? Probably not. But how do they drive when you are not in the car? "

Source: http://www.roadsafety.com/Teen_Driver.htm

Car Monitoring

- ACME Rent-A-Car, New Jersey
  - Automatically Fines Drivers US$450.- at Speeds Over 79mph
  - GPS Records Exact Position of Speed Violation
- Autograph System
  - Pilot Program 1998/99, Houston, TX
  - Insurance based on individual driving habits (When, Where, How)
  - GPS Tracking, Mobile Communication, Data Center
- Future: Tracking Your Personal Mobile Phone

Source: **Insurance & Technology Online, Jan 2nd 2002** (http://www.insurancetech.com/story/update/IST20020108S0004)

Source: **http://news.com.com/2100-1040-268747.html?legacy=cnet**

Other Examples

- Electronic Toll Gates
- Consumer Loyalty Cards
- Electronic Patient Data
- Computer Assisted Passenger Screening (CAPS)
  - Improved Systems in the Works (post 9/11)
  - Plans: Link Travel Data, Credit Card Records, Address Information, ...

5. Privacy Solutions

How Can We Achieve Privacy?

RESEARCH GROUP FOR

Distributed Systems

Privacy Solution Issues

- Feasibility
  - What Can Technology Achieve, Prevent?
- Convenience
  - More Information = Better Service?
- Communitarian
  - Will Less Privacy Benefit Society As A Whole?
- Egalitarian (Brin)
  - What If We All Watch Each Other?

Differing Viewpoints

- "Strong Privacy" Advocates
  - No-limits Technology As Empowerment
- European Model
  - Comprehensive Rules And Regulations To Govern Personal Data Exchange
- Transparency Advocates
  - Free Flow Of Information
  - Reciprocal Effect: Watching The Watchers

Fair Information Principles

- Organization for Economic Cooperation and Development (OECD), 1980
- Voluntary Guidelines for Members to Ease International Flow of Information:

1. Collection limitation
2. Data quality
3. Purpose specification
4. Use limitation
5. Security safeguards
6. Openness
7. Individual participation
8. Accountability

Simplified Principles

1. Notice and Disclosure
   - Purpose Specification
2. Choice and Consent
   - Individual Participation
3. Anonymity and Pseudonymity
   - Collection Limitation
4. Data Security
   - Security Safeguards
   - Use Limitation
5. Access and Recourse
   - Data Quality
   - Accountability
6. Meeting Expectations
   - Openness

1. Notice And Disclosure

- No hidden data collection!
  - Legal requirement in many countries
- Established means: privacy policies
  - Who, what, why, how long, etc. …
- How to publish policies in Ubicomp?
  - Periodic broadcasts
  - Privacy service?
- Too many devices?
  - Countless announcements an annoyance

2. Choice & Consent

- Participation requires *explicit consent*
  - Usually a signature or pressing a button
- True consent requires *true choice*
  - More than „take it or leave it“
- How to ask without a screen?
  - Designing UI‘s for embedded systems, or
  - Finding means of delegation (is this legal?)
- Providing conditional services
  - Can there be levels of location tracking?

3. Anonymity, Pseudonymity

- Anonymous data comes cheap
  - no consent, security, access needed
- Pseudonyms allow for customization
  - user can discard at any time
- Sometimes one cannot hide!
  - No anonymizing cameras & microphones
- Real-world data hard to anonymized
  - Even pseudonyms can reveal true identity

4. Security

- No one-size-fits-all solutions
  - High security for back-end storage
  - Low security for low-power sensors
- Real-world has complex situation-dependant security requirements
  - Free access to medical data in emergency situations
- Context-specific security?
  - Depending on device battery status
  - Depending on types of data, transmission
  - Depending on locality, situation

5. Access & Recourse

- Identifiable data must be accessible
  - Users can review, change, sometimes delete
- Collectors must be accountable
  - Privacy-aware storage technology?
- Ubicomp applications like lots of data
  - Increased need for accounting and access
- Carefully consider what is relevant
  - How much data do I really need?

6. Meeting Expectations

- Ubicomp: *invisibly* augments real-world
- Old habits adapt slowly (if ever)
  - People expect solitude to mean privacy
  - Strangers usually don't know me
- No spying, please (Proximity)
  - Devices only record if owner is present
- Rumors should not spread (Locality)
  - Local information stays local
  - Walls and Flower-Pots can talk (but won't do so over the phone)

Social Issues

- Peer Pressure
  - No Way to Opt-Out (Even Temporary)
- Loss Of Control
  - Smart Vs. Omniscient
- Trust
  - Inter-Object, Inter-Personal, Person-to-Object
- Equality
  - Extensive Profiling Categorizes People (Example: Frequent Flyer Cards)

Summary & Outlook

The Take Home Message

RESEARCH GROUP FOR
Distributed Systems

1. Privacy Definitions
   What is Privacy, Anyway?
2. Privacy Motivation
   Why Should We Want Privacy?
3. Privacy Evolution
   How is Privacy Changing?
4. Privacy Threats
   Why Should We Worry?
5. Privacy Solutions
   How can we achieve Privacy?

Defining Privacy

- Different Facets
  - Informational, Communication, Territorial, Bodily
- Border Crossings
  - Natural, Social, Spatial/ Temporal, Ephermal
- Different Motivations
  - Empowerment, Dignity, Utility, Constrain Of Power, By-product
- Not Limitless
  - Accountability Important Part Of Social Fabric

Solution Space

- Inspired By OECD Fair Information Practices
  - Notice, Choice & Consent, Anonymity, Security, Access & Recourse, Expectations
- Ubicomp Privacy
  - New Options
  - New Challenges

Tomorrow:
Privacy Laws And Technical Tools

Recommended Reading

- David Brin: The Transparent Society. Perseus Publishing, 1999
- Lawrence Lessig: Code and Other Laws of Cyberspace. Basic Books, 2000
- Simson Garfinkel: Database Nation – The Death of Privacy in the 21st Century. O'Reilly, 2001