Personal Privacy in Ubiquitous Computing

RESEARCH GROUP FOR
Distributed Systems

Marc Langheinrich
ETH Zurich

http://www.inf.ethz.ch/~langhein/

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

What's Up?

- What Is Privacy, Anyway?
  - Privacy Definitions
  - Privacy Motivation
- How Is Privacy Changing?
  - Privacy Evolution
  - Privacy Threats
- How Can We Achieve Privacy?
  - Privacy Solutions

1. Definitions and Motivations

What is Privacy, Anyway?

RESEARCH GROUP FOR

Distributed Systems

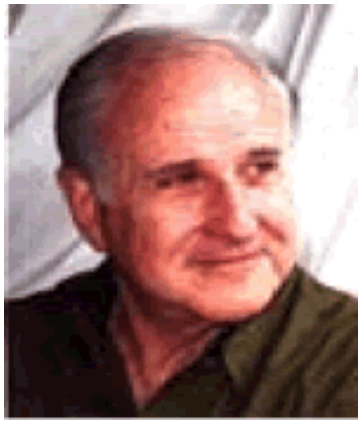
1. What is Privacy?
   Definitions and Motivation
2. How is Privacy Changing?
   Evolution and Threats
3. How can We Achieve Privacy?
   Concepts and Solutions

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, ...)

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
  - 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)

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

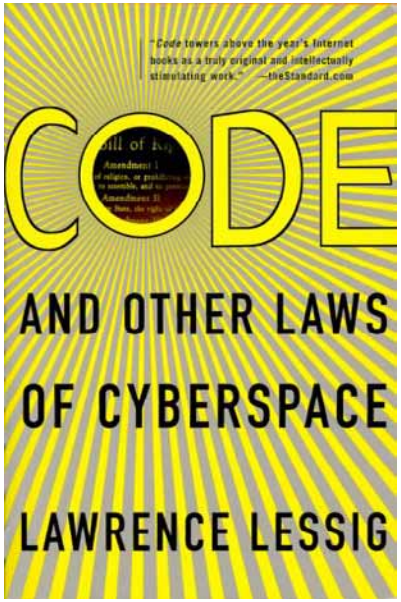
Privacy History

- 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)

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?

2. Evolution and Threats

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 Does One 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?

Virtual Dad

sit

- 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$150.- 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, ...

3. Concepts and Solutions

RESEARCH GROUP FOR

Distributed Systems

How can We Achieve Privacy?

1. What is Privacy?
   Definitions and Motivation
2. How is Privacy Changing?
   Evolution and Threats
3. How can We Achieve Privacy?
   Concepts and Solutions

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. What is Privacy?
   Definitions and Motivation
2. How is Privacy Changing?
   Evolution and Threats
3. How can We Achieve Privacy?
   Concepts and Solutions

Defining Privacy

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

Solution Space

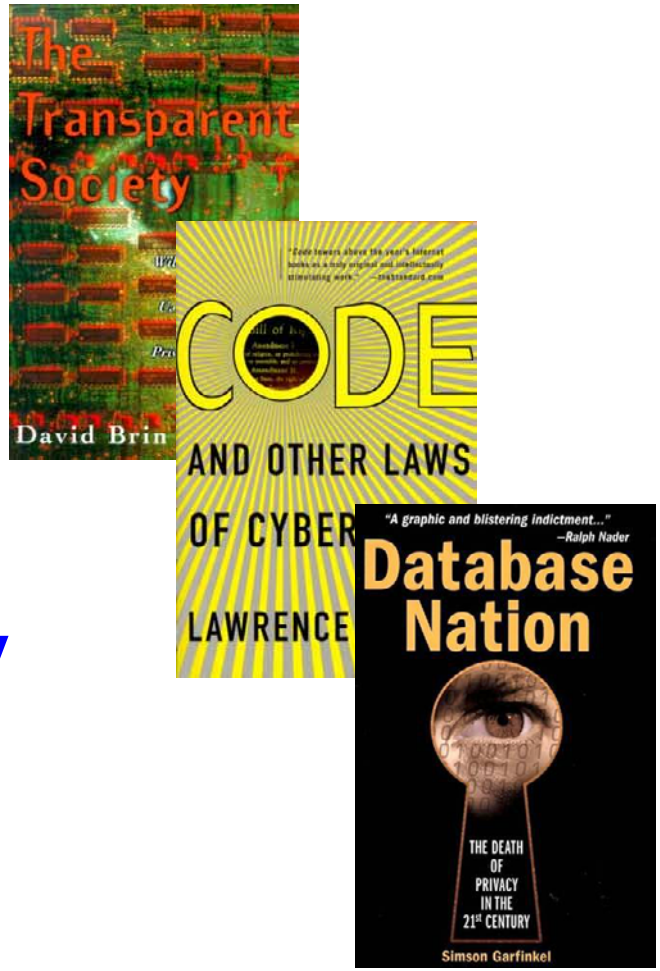
- Inspired By OECD Fair Information Practices
  - Notice & Disclosure
  - Choice & Consent
  - Security
  - Access & Control
  - Recourse
  - Meeting Expectations*
- Interdependencies
  - Technical Possibilities
  - Legal Requirements
  - Social Issues

The Take Home Message

- Many questions, few answers
  - Technology, laws still to evolve
- Ubicomp adds a new quality to privacy
  - Invisible, real-world coverage, comprehensive collection, inconspicuous
- Ubicomp (privacy) challenges
  - User interface (notice, choice, consent)
  - Protocols (anonymity, security, access, locality)
  - Social acceptance (user expectations)

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



More Books

- Security for Ubiquitous Computing, by Frank Stajano
- The Privacy Law Sourcebook 2001: United States Law, International Law, and Recent Developments, by Marc Rotenberg
- Privacy & Human Rights, EPIC

Additional Slides

Laws & Regulations

RESEARCH GROUP FOR
Distributed Systems

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 favoured strong privacy laws
  - First data protection law in the world: State of Hesse, Germany (1970)
  - Privacy commissions in each country (some countries have national and state commissions)

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

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

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 favoured strong privacy laws
  - First data protection law in the world: State of Hesse, Germany (1970)
  - Privacy commissions in each country (some countries have national and state commissions)

EU Data Directive

- 1995 Data Protection Directive 95/46/EC
  - Sets a Benchmark For National Law For Processing Personal Information In Electronic And Manual Files
  - Follows OECD Fair Information Practices
    - Collection Limitation, Openness, Purpose Specification, Use Limitation, Access, Security, Participation, Accountability
  - Facilitates Data-flow Between Member States And Restricts Export Of Personal Data To „Unsafe“ Non-EU Countries

Safe Harbor

- Membership
  - US companies self-certify adherance to requirements
  - Dept. of Commerce maintains list (222 as of 08/02)
    `http://www.export.gov/safeharbor/SafeHarborInfo.htm`
- Signatories must provide
  - **notice** of data collected, purposes, and recipients
  - **choice** of opt-out of 3rd-party transfers, opt-in for sensitive data
  - **access** rights to delete or edit inaccurate information
  - **security** for storage of collected data
  - **enforcement** mechanisms for individual complaints
- Approved July 26, 2000 by EU
  - reserves right to renegotiate if remedies for EU citizens prove to be inadequate

Privacy around the World

- Australia*
  - Proposed: Privacy Amendment (Private Sector) Bill in 2000
  - In talks with EU officials
- Brazil
  - Proposed: Bill No. 61 in 1996 (pending)
- Canada*
  - Passed: Bill C-6 in 4/2000
  - Under review by EU
- Hong Kong*
  - Passed: Personal Data (Privacy) Ordinance in 1995
- Japan
  - Currently: self-regulation & prefectural laws
  - In talks with EU officials
- Russia
  - Law on Information, Informatization, and Inform. Protect. 1995
  - In Progress: updated to comply with EU directive
- South Africa
  - Planned: Privacy and Data Protection Bill
- Switzerland*
  - EU-certified safe third country for data transfers

http://www.privacyinternational.org/survey/

* Has National Privacy Commissioner

EU Directive (cont.)

- 1997 Telecommunications Directive 97/66/EC
  - establishes specific protections covering telecommunications systems
  - July 2000 proposal to strengthen and extend directive to cover „electronic communications“
- Member states responsible for passing relevant national laws by 10/1998
  - 13 out of 15 member states have passed legislation, 2 are still pending (as of 08/2002)

Post 9-11 Issues (EU)

- Directive on Privacy and Electronic Communications 2002/58/EC
  - Members States Have Until 11/03 to Implement National Law Allowing Traffic Data Retention
  - Retention Period: 12 Months – 7 Years (Proposal)
- Data to be Retained (Planned Requirement):
  - Email: IP address, message ID, sender, receiver, user ID
  - Web/FTP: IP address, User ID, Password, Full Request
  - Phone: numbers called (whether connected or not), date, time, length, geographical location for mobile subscribers

See also: http://www.epic.org/privacy/intl/data_retention.html

Example UK

- UK Terrorism Act, 2001
  - Telcos, ISPs Retain Traffic Data Longer Than for Billing Purposes
  - Purpose: National Security Investigations
- Regulation of Investigatory Powers Act, 2000
  - Allows Law Enforcement Access To Retained Data
  - Planned: Extend Access to Health and Transport, Local Authorities, ... (Halted 06/02)
- Other EU Countries With Existing Laws for Data Retention:
  - Belgium, France, Spain