Personal Privacy in Ubiquitous Computing

RESEARCH GROUP FOR
Distributed Systems

Marc Langheinrich
ETH Zurich

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

Privacy Excuses

- Optimists: "All you need is really good firewalls."
- Self-Regulation: "It's maybe about letting them find their own ways of cheating, you know..."
- Not my problem: "For [my colleague] it is more appropriate to think about privacy issues. It's not really the case in my case."
- Gets in the way: "Somehow [privacy] also destroys this, you know, sort of, like, creativity..."
- Impossible: "I think you can't think of privacy when you are trying out... it's impossible, because if I do it, I have troubles with finding [a] Ubicomp future"

This Afternoon's Program

- The Case for Ubicomp Privacy
  - What is Privacy? Why Would We Want it?
  - What is Different with Ubicomp Privacy?
- Tools for Ubicomp Privacy
  - Legal Mechanisms (i.e., Laws)
  - Technical Tools
- Privacy Guidelines for Ubicomp
  - How to Build Privacy-Aware Systems

The Case For Ubicomp Privacy

Why Should We Care About Personal Privacy in Pervasive Computing?

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?

1. Privacy Definitions

What is Privacy, Anyway?

RESEARCH GROUP FOR

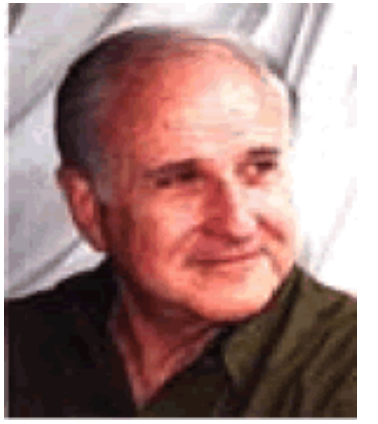
Distributed Systems

What Is Privacy?

- „The right to be let alone.“
  - L. Brandeis, S. Warren 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. Emeritus 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 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

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

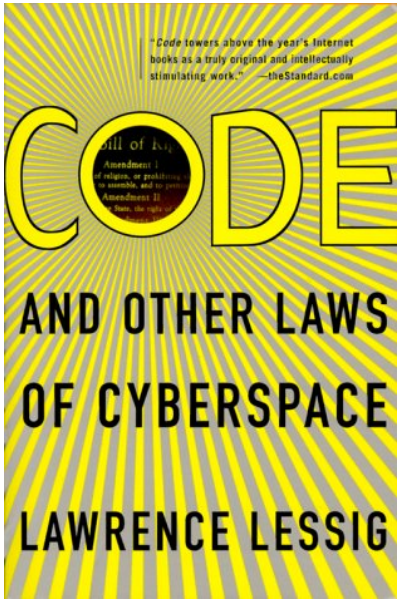
Privacy History

- Justices Of The Peace Act (England, 1361)
  - Protection against Eavesdroppers & 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; the wind may blow through 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

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 Smart Appliances 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

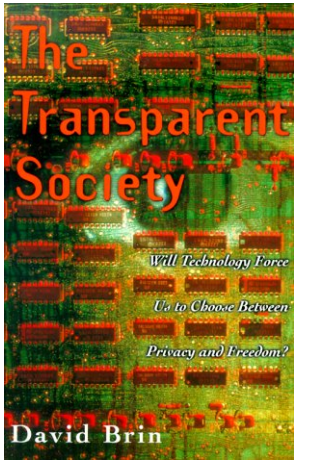
- Strong Encryption
  - Prevents Law Enforcement From Watching Criminals
- ID-Cards Including Biometrics
  - Better Protection From False Identities
- Compulsive HIV Testing of Infants
  - Increases Life Expectations of Infants Born To HIV-positive Mothers
- Registration of Released Prisoners
  - Informs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

Privacy vs. Economic Interest

- Customer Loyalty 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

No Privacy?

- 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

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

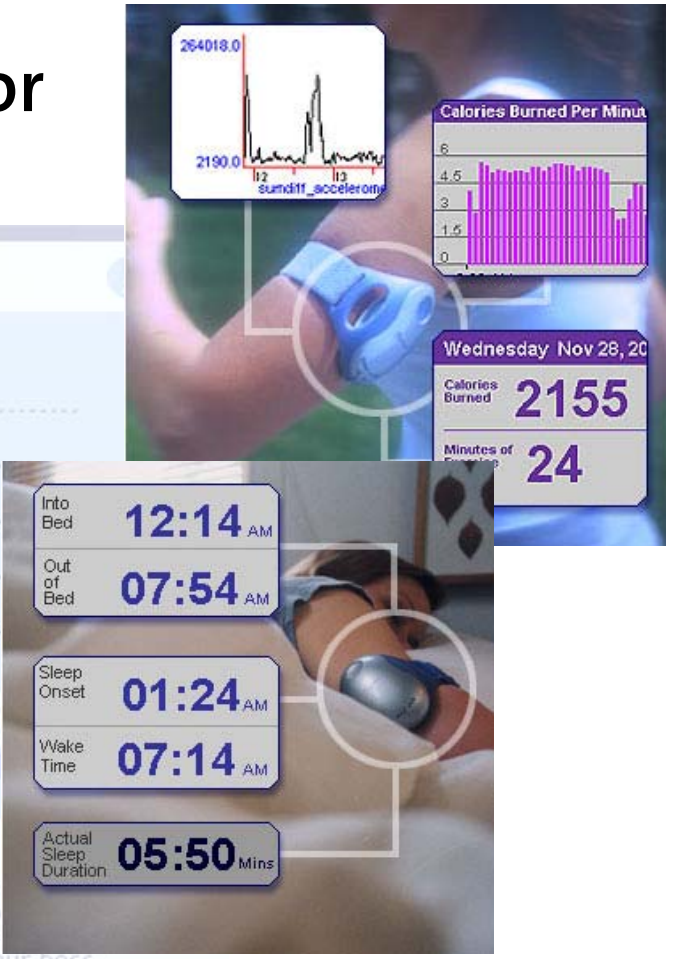
Why Should We Worry?

RESEARCH GROUP FOR

Distributed Systems

Bodymedia

- Communication Platform for wireless Transmission of Body Sensor Readings
- Bodymedia Data Center translates Raw Data into „Lifestyle Data“
- Accessible only 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 Peace 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 Haven, CT
  - Fined James Turner US$450.- for Three Separate Speeding Violations (10/2000)
  - GPS Recorded Exact Position of Speed Violations
- Autograph System (Progressive Insurance Corp)
  - 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, ...

Tools for Ubicomp Privacy

Technical and Legal Means for Protecting (or Restricting) Personal Privacy in Pervasive Computing

RESEARCH GROUP FOR
Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

What's Up?

- Legal Aspects
  - US Privacy Landscape
  - European Privacy Laws
- Privacy Enhancing Technologies (PETs)
  - Anonymity Tools
  - Transparency Tools
  - Confidentiality Tools
  - Access Tools
- Ubicomp Privacy Guidelines

1. Legal Aspects

What are we obliged to do?

RESEARCH GROUP FOR
Distributed Systems

Laws and Regulations

- Two Main Approaches
  - Sectorial ("Don't Fix if it Ain't Broken")
  - Omnibus (Precautionary Principle)
- US: Sector-specific Laws, Minimal Protections
  - Strong Federal Laws for Government
  - Self-Regulation, Case-by-Case for Industry
- Europe: Omnibus, Strong Privacy Laws
  - Law Applies to Both Government & Industry
  - Privacy Commissions in Each Country as Watchdog

US Privacy: 4th Amendment

- Basis for many privacy issues in US
  - "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."
- "Constitutional Right to Privacy"
  - From 1st, 3rd, 4th, 5th and 9th Amendment
  - US Supreme Court, *Grisworld vs. Connecticut*, 1965

Olmstead vs. US, 1928

- Police caught bootlegger by placing wiretaps to phone lines outside his house
- Defendant claimed 4th Amendment
- Supreme Court claimed no physical trespassing occurred
  - Judge Brandeis disagreed: Phone Tapping a Search, Recording Conversation a Seizure
- What Conception of Privacy?
  - Privacy as Utility vs. Privacy as Limit of Power!

Katz vs. US, 1967

- Police Placed Microphone outside Public Phone in Front of Defendants House
  - Federal Communications Act, 1934, Forbid Wire Tapping (Exceptions Possible)
- Overruled Olmstead case: Reasonable Expectation of Privacy
- Law "protects people, not places."
  - Microphone was Unreasonable Search, Recording was Unreasonable Seizure

Kyllo vs. US, 2001

- Police used Thermal Image Scanner to Detect Heat Lamps Growing Marijuana Plants
- Supreme Court: Unreasonable Search Barred By 4th Amendment
  - Device Not In General Use By Public, Gives Expectation of Privacy
  - But: Visual Search Still Allowed

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

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 (1980)
    - Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, 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 (574 as of 09/04)
    `http://www.export.gov/safeharbor/sh_overview.html`
- 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
- Argentina *
  - Passed: Personal Data Protection Act No. 25.326 in 2000
  - EU-certified safe third country
- Canada*
  - Passed: Bill C-6 in 4/2000
  - EU-certified safe third country
- 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*
  - Data Protection Act of 1992
  - EU-certified safe third country

http://www.privacyinternational.org/

* Has National Privacy Commissioner

Post 9-11 Issues (US)

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, 2001
  - simplifies monitoring online activities, video surveillance, money laundering, immigration
- Operation TIPS (Terrorist Information & Prevention System)
  - One Million Volunteers in 10 US Cities to Report "Suspicious Activity" (Goal: 4% of Population)
  - Targeted: Letter Carriers, Utility Technicians, ...
  - Rejected by Congress 11/2002
- Relaunch: Total Information Awareness (TIA)
  - Nationwide Citizen Tracking (all Public & Private DBs)
  - Renamed to "Terrorist Information Awareness" (05/2003)

citizen corps
Learn more and join today!

Post 9-11 Issues (EU)

- Directive on Privacy and Electronic Communications 2002/58/EC*
  - Allows National Laws to Retain Traffic Data
  - Suggested Retention Period: 12 Months – 7 Years
- Data to be Retained (Proposed):
  - 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

* As of 1/2004, only 8 countries had taken action: Denmark, Spain, Ireland, Italy, Austria, Finland, Sweden, and UK

Example UK

- Anti-Terrorism, Crime & Security 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, Transport, Local Authorities, ... (On Hold Since 06/02)
- Other EU Countries With Existing Laws for Data Retention:
  - Belgium, Denmark, France, Spain, Austria, Italy, ...

2. Technical Tools

What is possible to do?

RESEARCH GROUP FOR
Distributed Systems

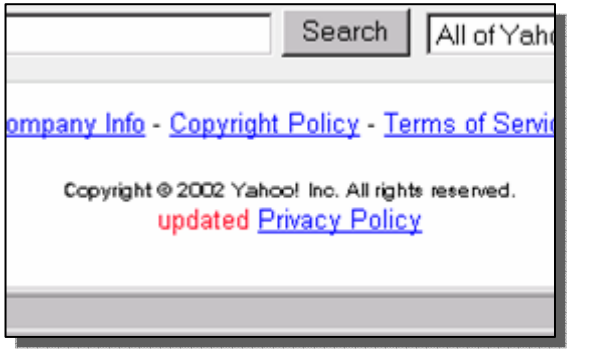
1. Legal Aspects
   What are we obliged to do?
2. Technical Tools
   What is possible to do?
3. Privacy Solutions
   How can we achieve privacy?

Technical Tools

- Privacy Enhancing Technologies (PETs)
  - Encryption & Authentication
  - Anonymization & Pseudonymization
  - Access & Control
  - Transparency & Trust
- Ubicomp Privacy Tools
  - RFID Privacy
  - Location Privacy

Example: Transparency

- Privacy Policies
  - Let consumers know about collector's privacy practices
- Consumers can then decide
  - whether or not practices are acceptable
  - when to opt-in or opt-out
  - who to do business with
- Increase consumer trust



Privacy Policy Drawbacks

- BUT policies are often
  - difficult to understand
  - hard to find
  - take a long time to read
    - usually 3-4 pages!
  - changed without notice

PET Solution: P3P

- Platform for Privacy Preference Project
  - Chartered by World Wide Web Consortium (W3C)
  - 1997-2001 (Recommendation December 2001)
- A framework for automated privacy discussions
  - Web sites disclose their privacy practices in standard machine-readable formats
  - Web browsers automatically retrieve P3P privacy policies and compare them to users' privacy preferences
  - ~~Sites and browsers can then~~ negotiate ~~about privacy terms~~

P3P1.0 defines

- Data Schemas (**What** Data is being collected)
  - `User.name.given`, `User.name.family`, etc
  - Allows for Custom Extensions
- Vocabulary for Privacy Policies (**Why** is Data Collected, **How**, etc)
  - `Purpose=marketing`, `Recipient=ourselves`
- XML Format for Privacy Policies
- Methods to Associate Policies with Web Pages
- Transport Mechanism for Policies (via HTTP)
  - No Data Exchange Protocol!

P3P1.0 defines

- Data
  - Us
  - All
- Voca
  Colle
  - Pu
- XML
- Meth
- Trans
  - No

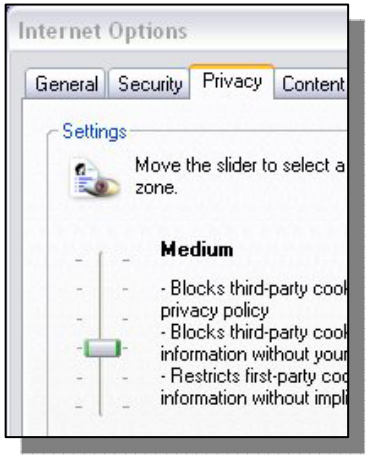
```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
        entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
     description="PrivacySeal, a third-party seal provider"
     image="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
    <CONSEQUENCE-GROUP>
      <CONSEQUENCE>a site with clothes you would  appreciate</CONSEQUENCE>
    </CONSEQUENCE-GROUP>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <PURPOSE><custom/><develop/></PURPOSE>
    <DATA-GROUP>
      <DATA name="dynamic.cookies" category="state"/>
      <DATA name="dynamic.miscdata" category="preference"/>
      <DATA name="user.gender"/>
      <DATA name="user.home." optional="yes"/>
    </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

P3P in Action (Web Browser)

- AT&T Privacy Bird (IE Plugin)
  - Displays Icons Summarizing Privacy Policy

  - Provides Quick Access to Additional Information

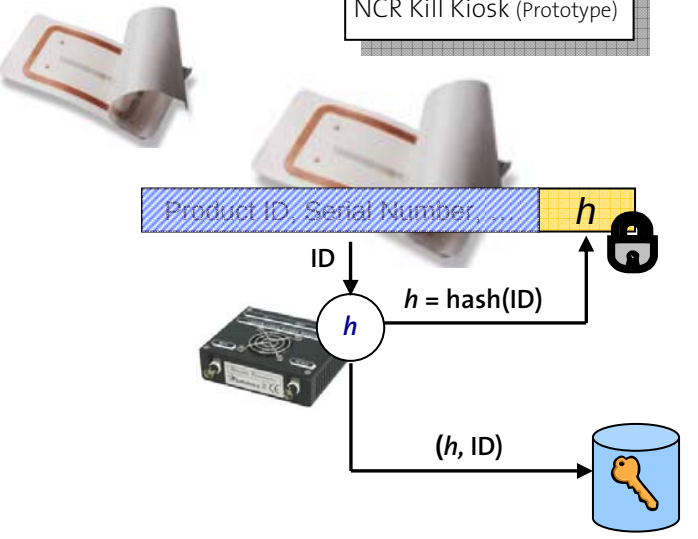
- IE6
  - P3P for Basic Cookie Control



RFID Privacy

- Tag Deactivation (Kill Tag)
  - Tags are deactivated at checkout
    - Expensive training / equipment
    - Prevents post point-of-sales applications
- Block Communication (Blocker Tag)
  - Special "noise-only" tag
    - Fails if not properly aligned
    - Interferes with tags of others
- Access Control (Hash Locks)
  - Key to lock/unlock tag data
    - Expensive chip design
    - Impractical key management

NCR Kill Kiosk (Prototype)



Location Privacy

- Problems of Location-Aware Services
  - Current Location => Current Activity?
  - Historic Movement Patterns in Logfiles
- Access Control to Limit Disclosure
  - More of a Social Problem
- Pseudonyms to Hide Identity (Limited)
  - Data Mining Cracks Fixed Nym (via Location)
  - Switching Nyms to Prevent Tracing/Mining
    - Often Trivial to Detect
    - Difficult with Multiple, Long-Standing Queries

3. Privacy Solutions

How Can We Achieve Privacy?

RESEARCH GROUP FOR

Distributed Systems

1. Legal Aspects
   What are we obliged to do?
2. Technical Tools
   What is possible to do?
3. Privacy Solutions
   How can we achieve privacy?

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
- Six Basic Principles (simplified)
  1. Notice & Disclosure
  2. Choice & Consent
  3. Anonymity & Pseudonymity
  4. Data Security
  5. Access & Recourse
  6. Meeting Expectations
- Guidance for Solution Design

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

RESEARCH GROUP FOR

Distributed Systems

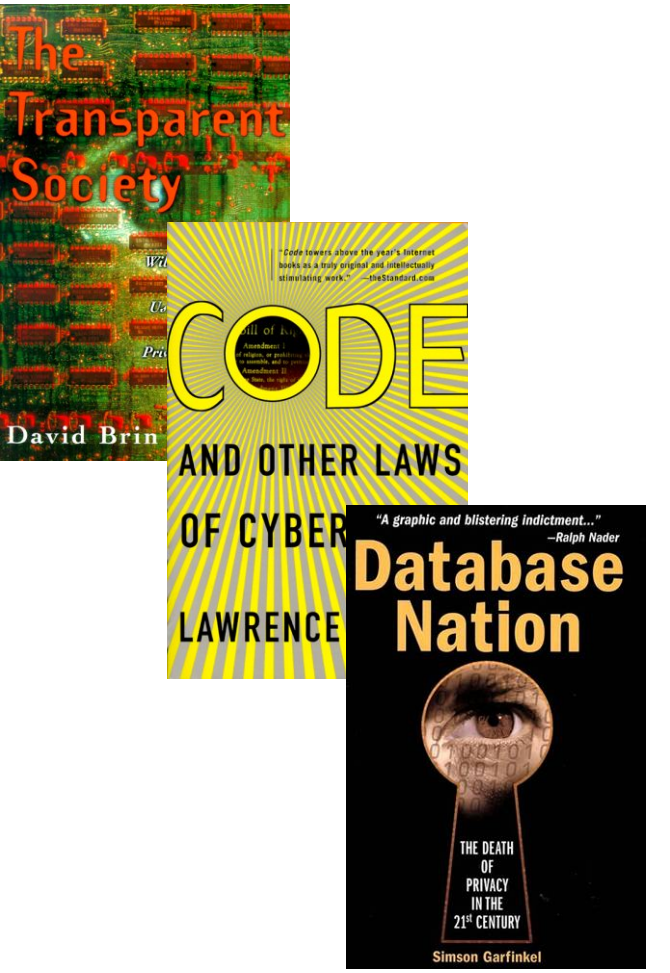
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Summary

- Privacy is Complex Legal and Social Problem
  - Different Facets, Extends, Borders, Motivations
  - Not Limitless (Security vs. Liberty)
  - Amplified by Ubicomp Technology
- A Variety of Tools
  - Legal Tools (US vs. EU Approach, National Security?)
  - Technical Tools (How to Apply to Location, RFID?)
- Impact on Ubicomp System Design
  - Fair Information Principles (What Data to Collect? How to Use? How to Communicate?)
  - Not just “Good Firewalls”!

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

- Frank Stajano: Security for Ubiquitous Computing. Wiley & Sons 2002
- Marc Rotenberg et al.: Privacy & Human Rights. EPIC 2003
- Daniel Solove and Marc Rotenberg: Information Privacy Law. Aspen Publ. 2003