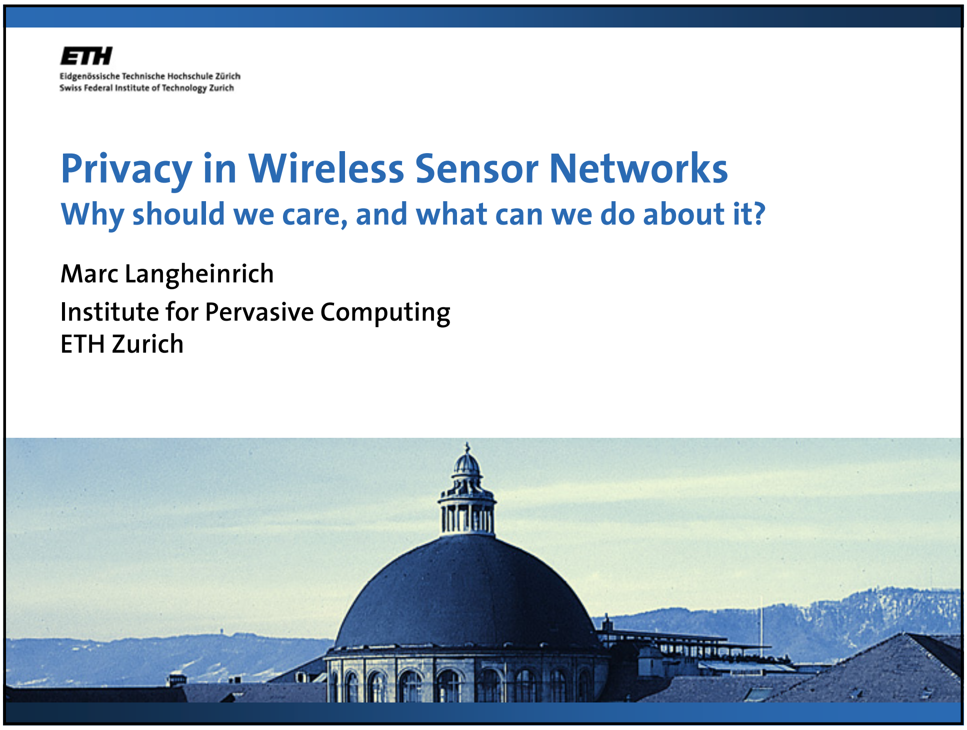


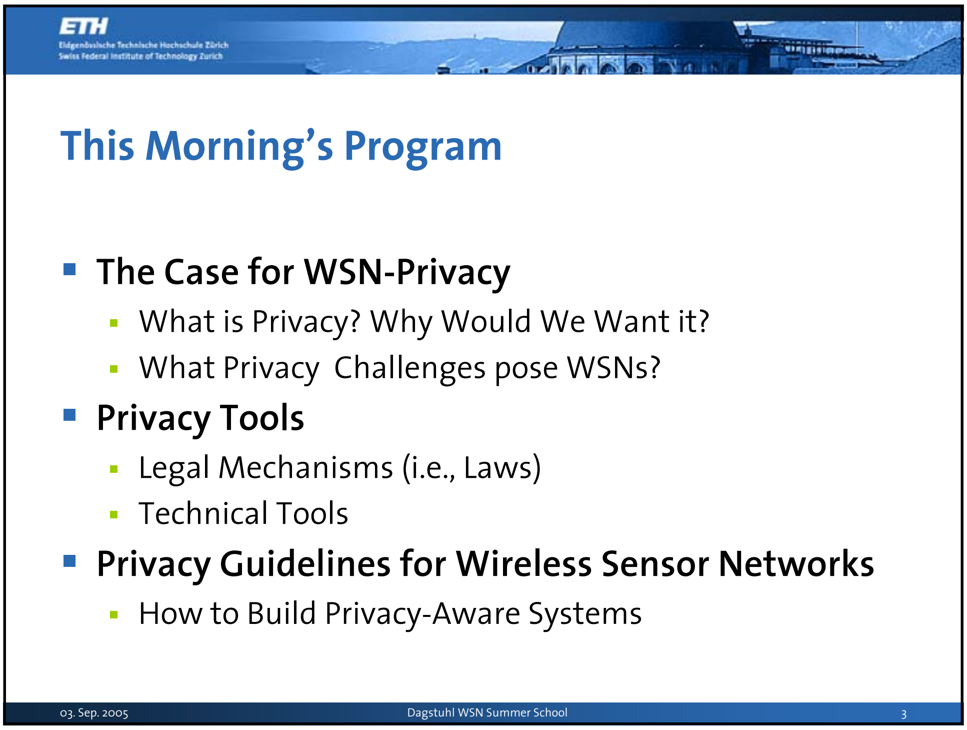
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

# Privacy in Wireless Sensor Networks

## Why should we care, and what can we do about it?

Marc Langheinrich

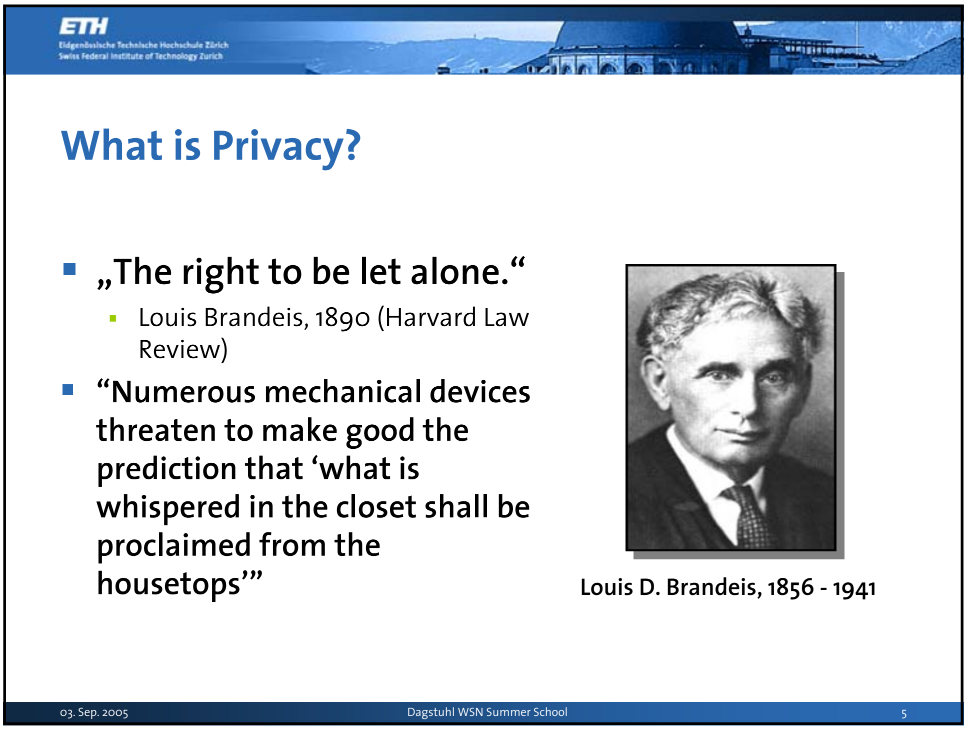
Institute for Pervasive Computing
ETH Zurich



ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

## This Morning's Program

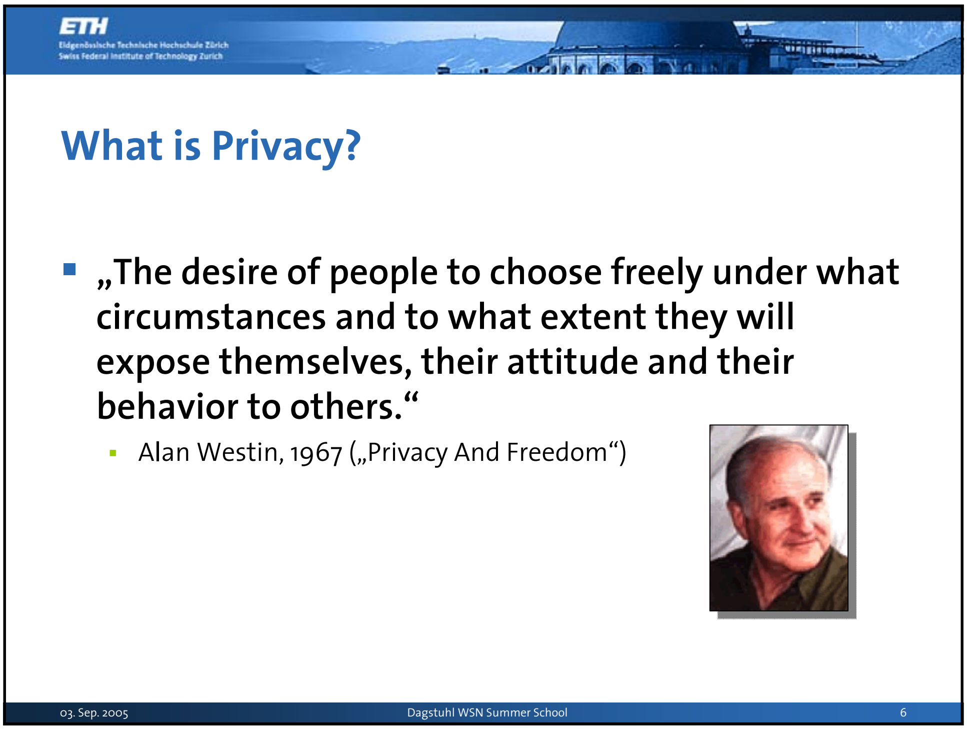
- The Case for WSN-Privacy
  - What is Privacy? Why Would We Want it?
  - What Privacy  Challenges pose WSNs?
- Privacy Tools
  - Legal Mechanisms (i.e., Laws)
  - Technical Tools
- Privacy Guidelines for Wireless Sensor Networks
  - How to Build Privacy-Aware Systems



## What is Privacy?

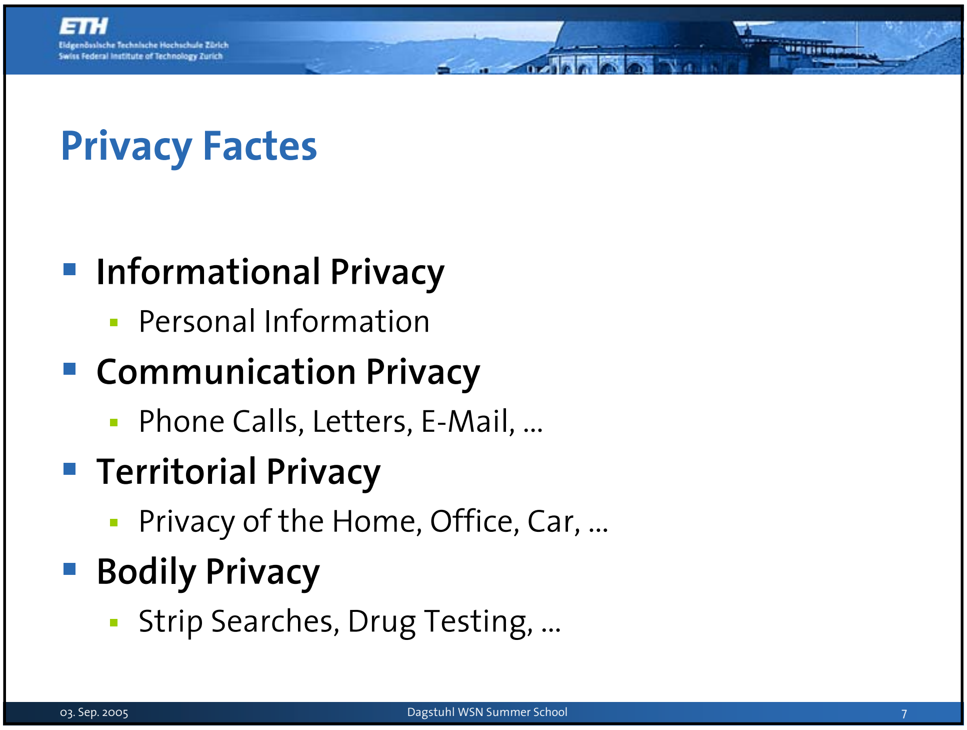
- „The right to be let alone.“
  - Louis Brandeis, 1890 (Harvard Law Review)
- “Numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the housetops’”

Louis D. Brandeis, 1856 - 1941



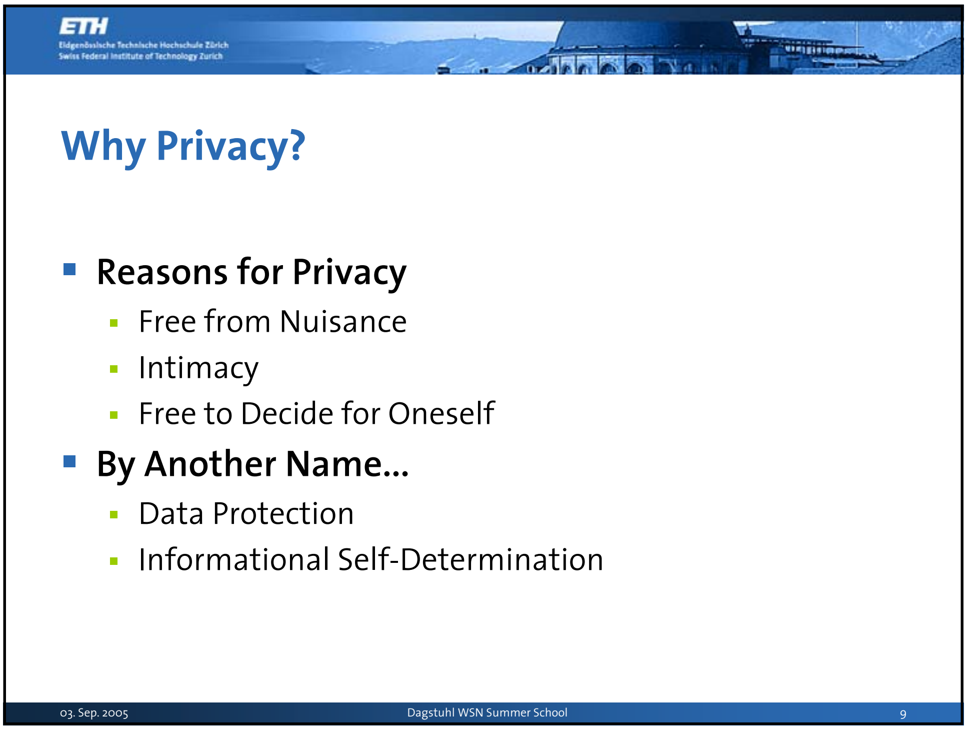
## What is Privacy?

- „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“)



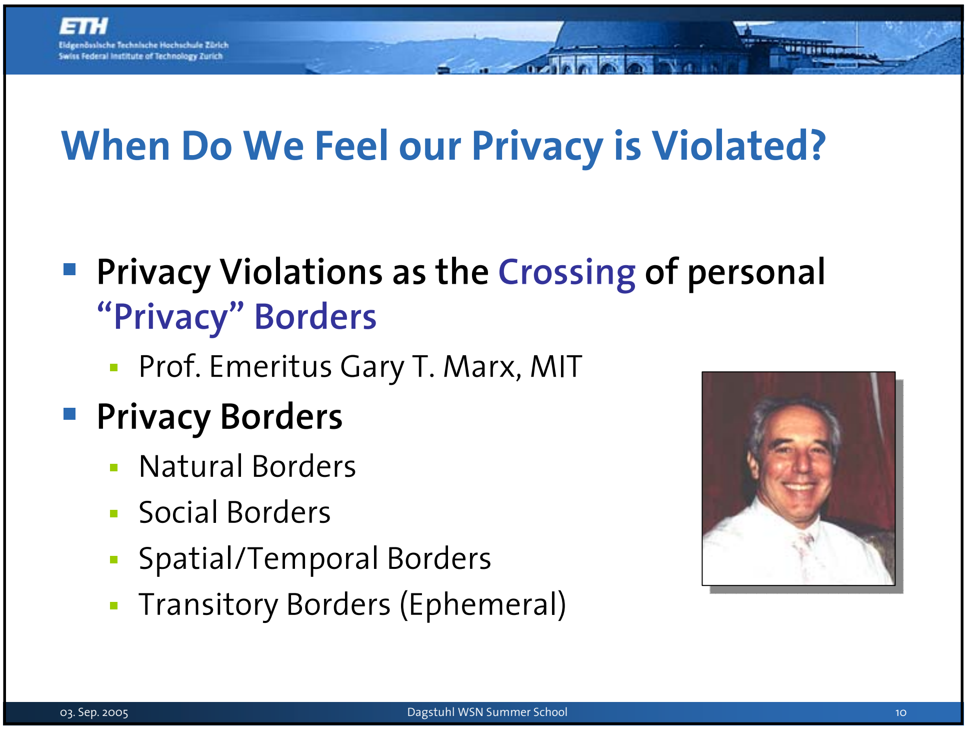
## Privacy Factes

- Informational Privacy
  - Personal Information
- Communication Privacy
  - Phone Calls, Letters, E-Mail, ...
- Territorial Privacy
  - Privacy of the Home, Office, Car, ...
- Bodily Privacy
  - Strip Searches, Drug Testing, ...



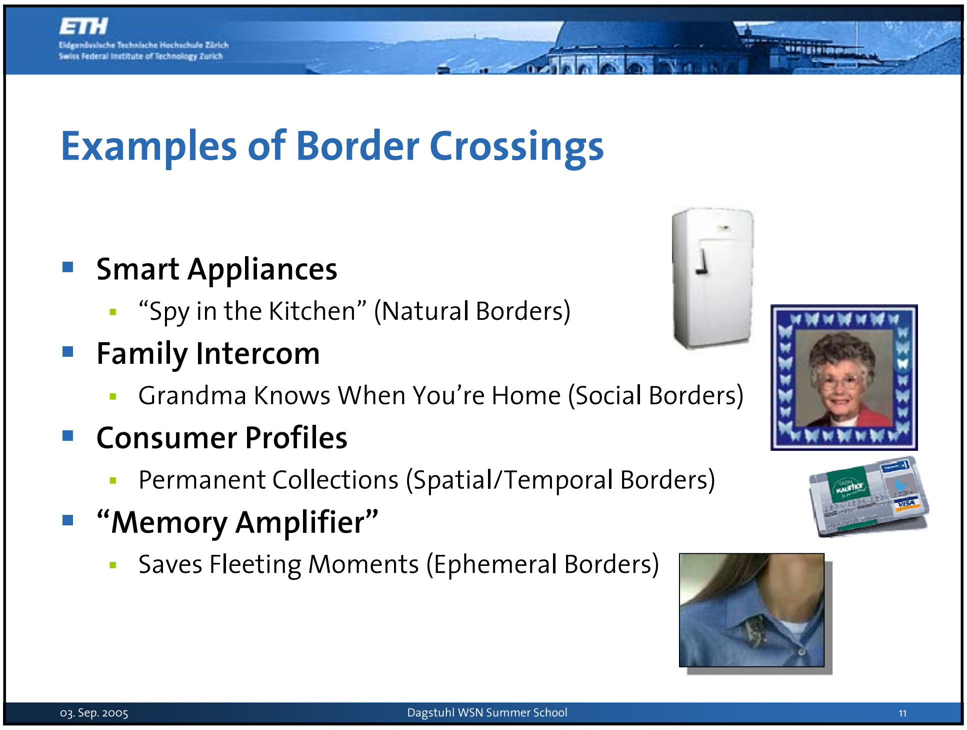
## Why Privacy?

- Reasons for Privacy
  - Free from Nuisance
  - Intimacy
  - Free to Decide for Oneself
- By Another Name...
  - Data Protection
  - Informational Self-Determination



## When Do We Feel our Privacy is Violated?

- Privacy Violations as the Crossing of personal "Privacy" Borders
  - Prof. Emeritus Gary T. Marx, MIT
- Privacy Borders
  - Natural Borders
  - Social Borders
  - Spatial/Temporal Borders
  - Transitory Borders (Ephemeral)



## Examples of Border Crossings

- Smart Appliances
  - "Spy in the Kitchen" (Natural Borders)
- Family Intercom
  - Grandma Knows When You're Home (Social Borders)
- Consumer Profiles
  - Permanent Collections (Spatial/Temporal Borders)
- "Memory Amplifier"
  - Saves Fleeting Moments (Ephemeral Borders)

# A Brief History of Privacy

- 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; 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 the Elder (1708-1778)
    English Parliamentarian
    Addressing the House of Commons in 1763

# Privacy in the 20th Century

- 1948 United Nations, Universal Declaration of Human Rights: Article 12
  - “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.“
- 1970 Europäische Menschenrechtskonvention: Artikel 8 – Recht auf Achtung des Privat- und Familienlebens
  - “Everyone has the right to respect for his private and family life, his home and his correspondence.“
- First Data Protection Law in the World in Hesse (1970)

## Informational Self-Determination

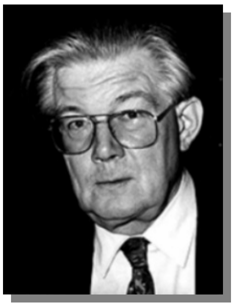
### "Informationelle Selbstbestimmung"

- German Federal Constitutional Court (Census Decision '83)
  - "If one cannot with sufficient surety be aware of the personal information about him that is known in certain part of his social environment, . . . can be seriously inhibited in his freedom of self-determined planning and deciding. A society in which the individual citizen would not be able to find out who knows what when about them, would not be reconcilable with the right of self-determination over personal data. Those who are unsure if differing attitudes and actions are ubiquitously noted and permanently stored, processed, or distributed, will try not to stand out with their behavior. . . . This would not only limit the chances for individual development, but also affect public welfare, since self-determination is an essential requirement for a democratic society that is built on the participatory powers of its citizens."

## Informational Self-Determination

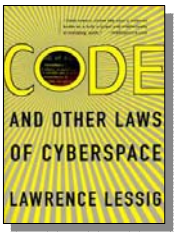
### "Informationelle Selbstbestimmung"

- Federal Constitutional Court President Ernst Benda ('83):
  - "The problem is the possibility of technology taking on a life of its own, so that the actuality and inevitability of technology creates a dictatorship. Not a dictatorship of people over people with the help of technology, but a dictatorship of technology over people."



**Ernst Benda, *1925**
BVG President 1971-1983

## Why Privacy Laws?

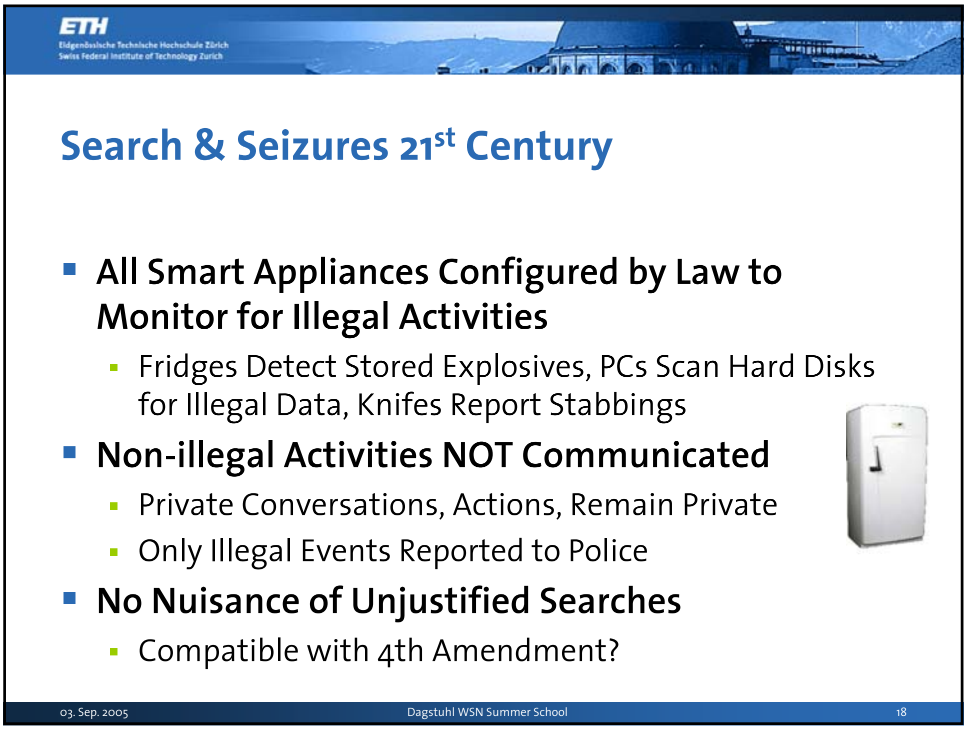


- As Empowerment
  - "Ownership" Of Personal Data
- As Utility
  - Protection From Nuisances (e.g., Spam)
- As Dignity
  - Balance Of Power ("Nakedness")
- As Constraint Of Power
  - Limits Enforcement Capabilities Of Ruling Elite
- As By-Product?
  - Result of Inefficient Data Collection Methods

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

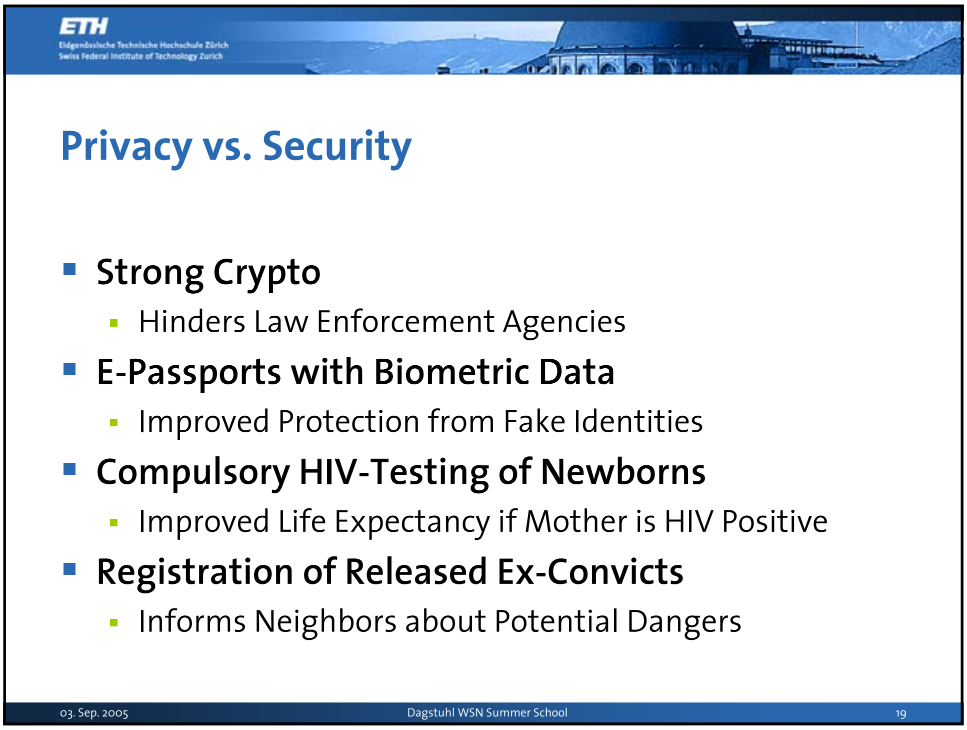
## Example: Search And Seizures

- 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 21$^{st}$ 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. Security

- Strong Crypto
  - Hinders Law Enforcement Agencies
- E-Passports with Biometric Data
  - Improved Protection from Fake Identities
- Compulsory HIV-Testing of Newborns
  - Improved Life Expectancy if Mother is HIV Positive
- Registration of Released Ex-Convicts
  - Informs Neighbors about Potential Dangers

## Privacy vs. Economic Interest

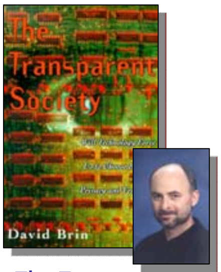
- Customer Loyalty Card
  - Purchases Accumulate “Points”
- Often Sweeping Privacy Statements
  - Consumers Agree To Usage Of Data For Marketing Purposes And Transmission To Undisclosed Recipients
- Emnid Survey, March 2002 (Germany)
  - 50% Got At Least 1 Loyalty Card
  - 72% Think Positively About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

PAYBACK

## No Privacy?

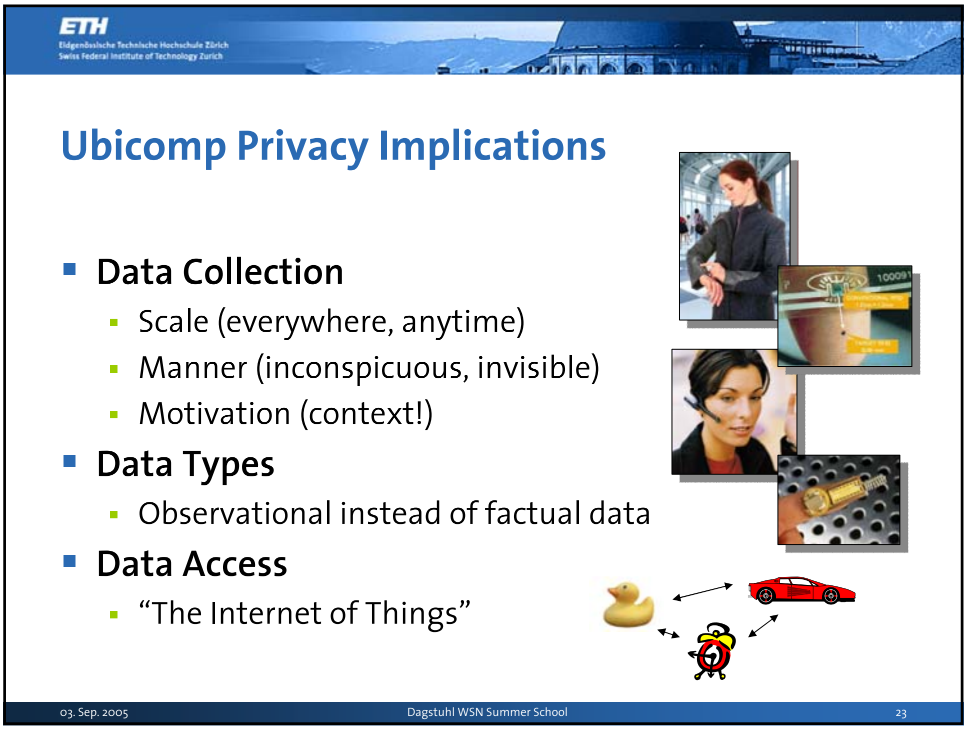
### The Transparent Society

- 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

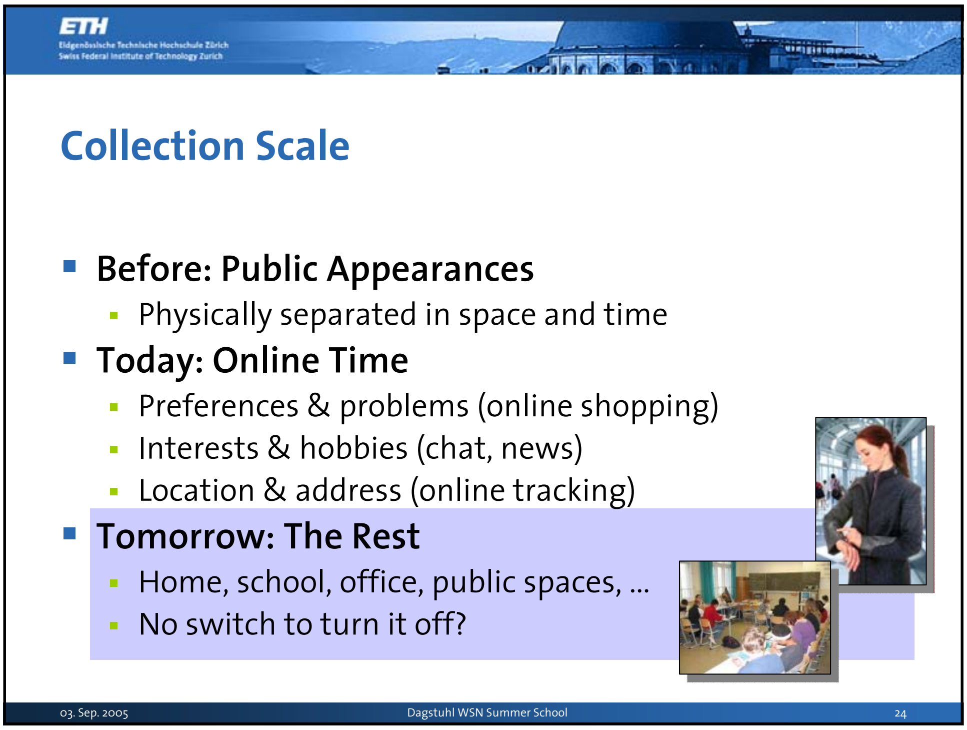
- Assumption: There Are No Secrets For The Powerful
  - Secrecy And Privacy Protects Only Elite



## Ubicomp Privacy Implications

- Data Collection
  - Scale (everywhere, anytime)
  - Manner (inconspicuous, invisible)
  - Motivation (context!)
- Data Types
  - Observational instead of factual data
- Data Access
  - “The Internet of Things”

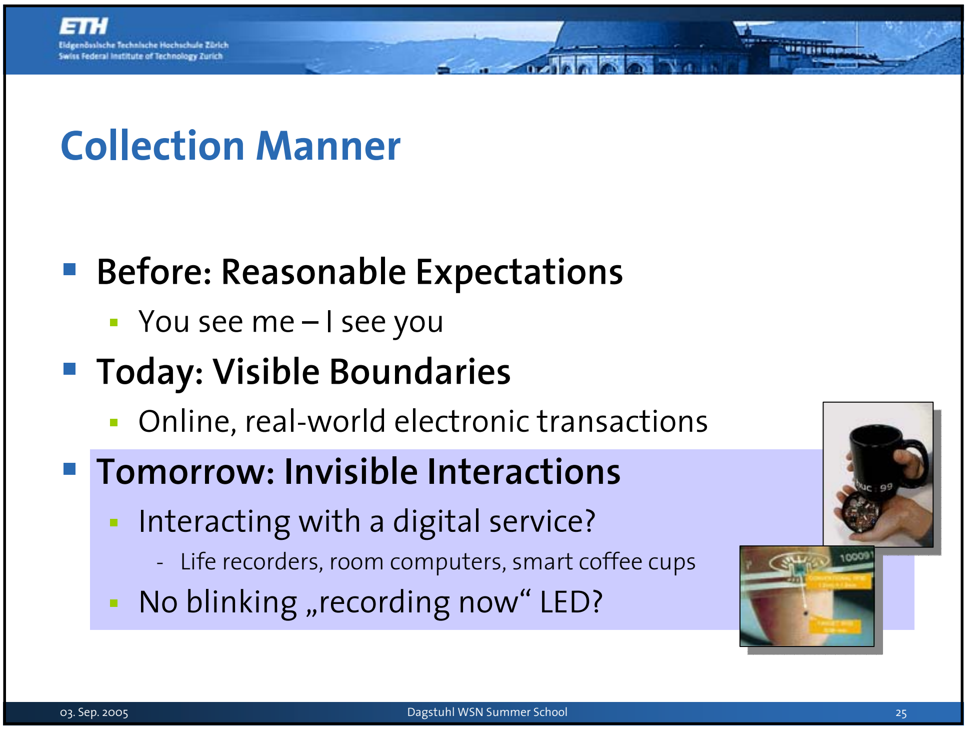
03. Sep. 2005 Dagstuhl WSN Summer School 23



## Collection Scale

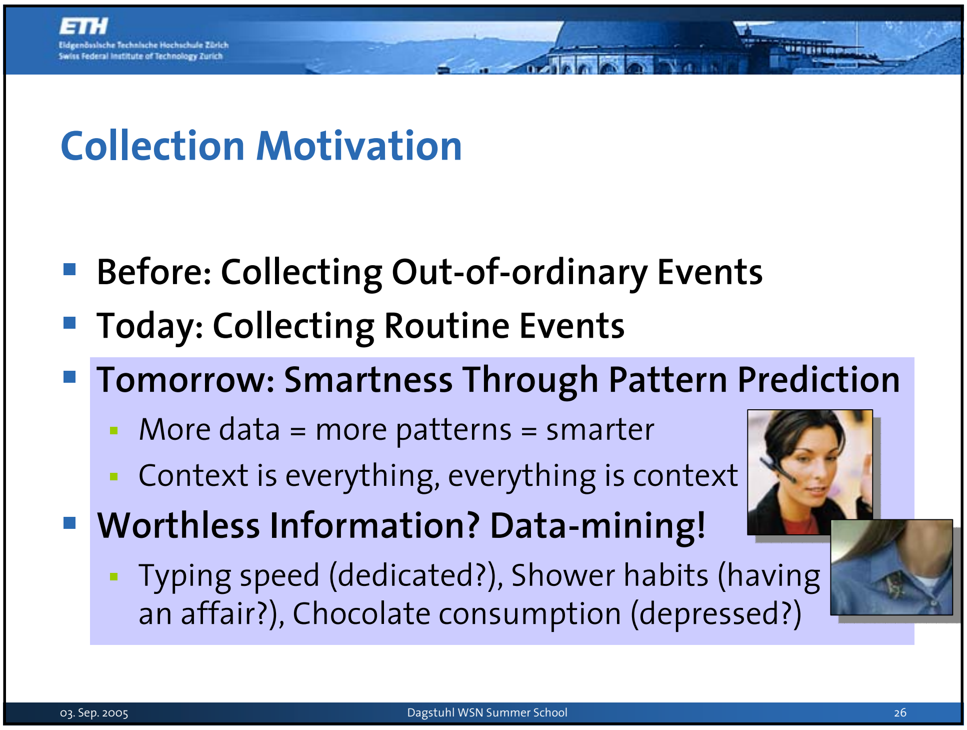
- Before: Public Appearances
  - Physically separated in space and time
- Today: Online Time
  - Preferences & problems (online shopping)
  - Interests & hobbies (chat, news)
  - Location & address (online tracking)
- Tomorrow: The Rest
  - Home, school, office, public spaces, …
  - No switch to turn it off?

03. Sep. 2005 Dagstuhl WSN Summer School 24



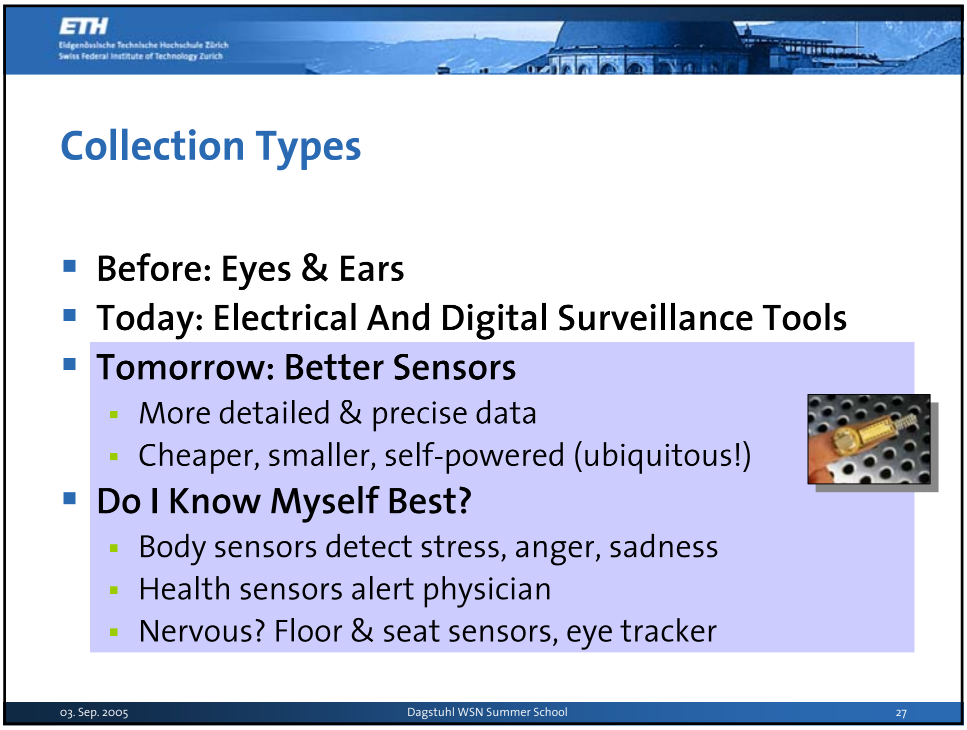
## Collection Manner

- **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?



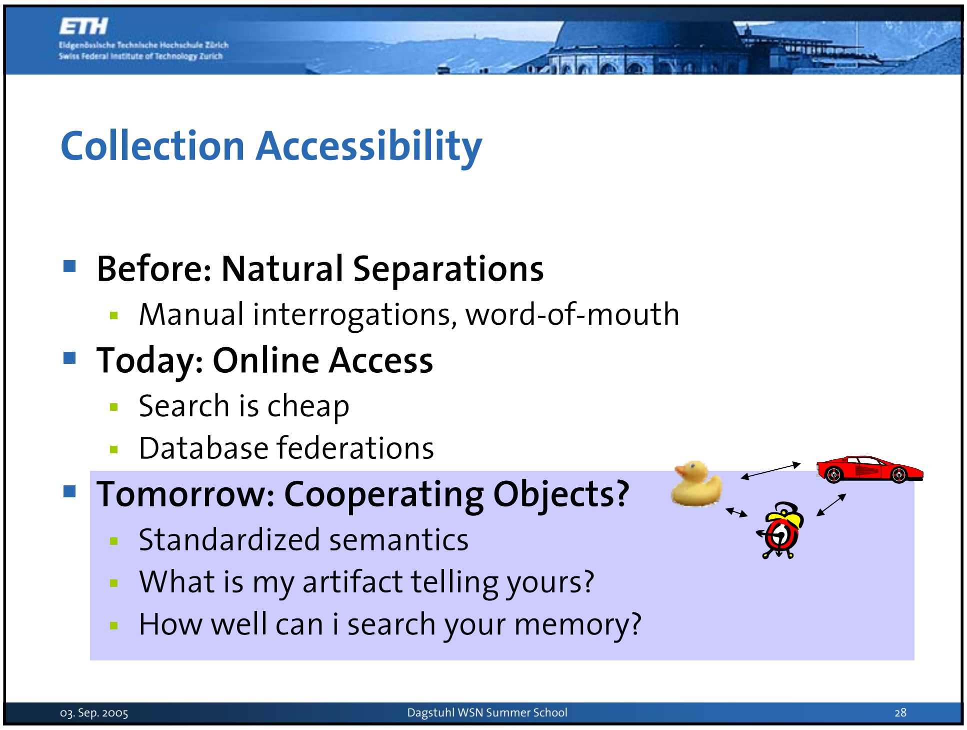
## Collection Motivation

- **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?)



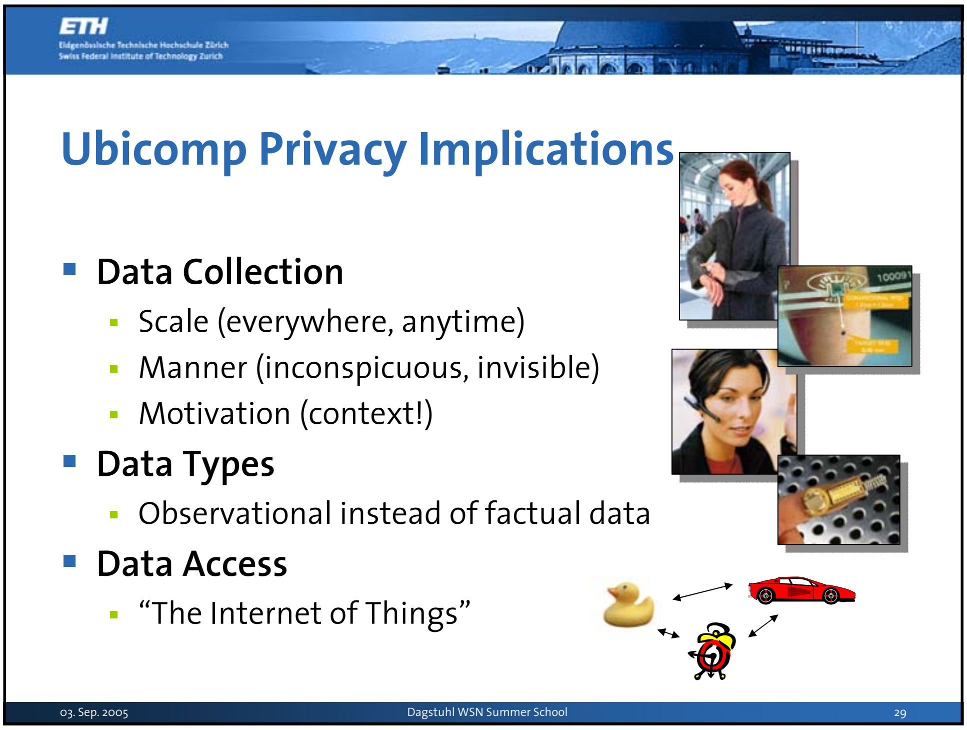
## Collection Types

- 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 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?

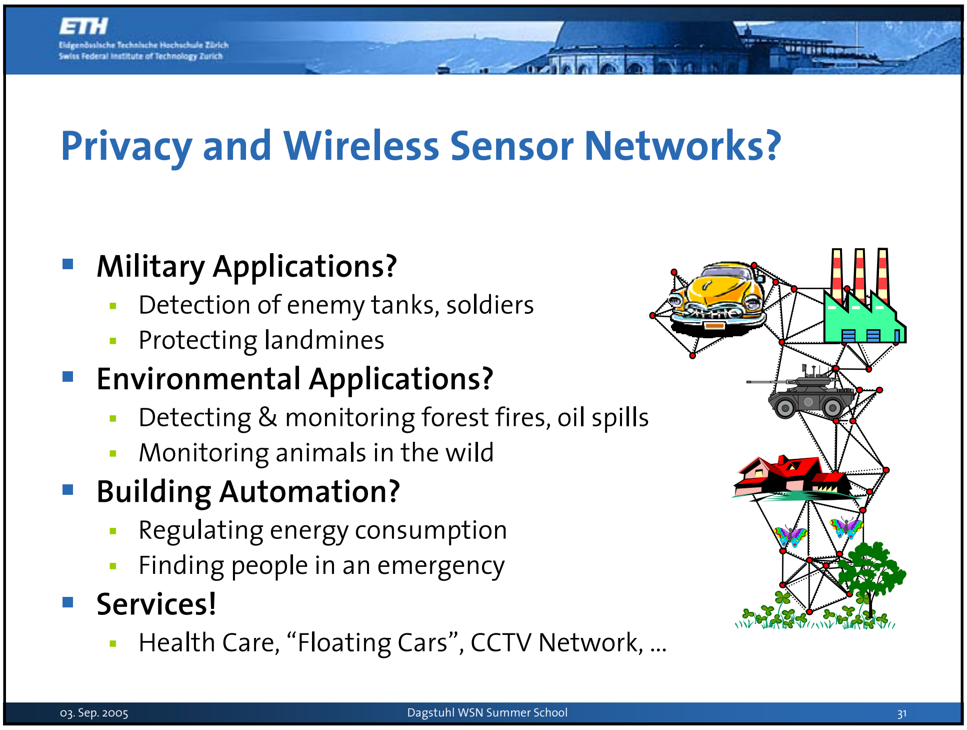


ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

## Ubicomp Privacy Implications

- Data Collection
  - Scale (everywhere, anytime)
  - Manner (inconspicuous, invisible)
  - Motivation (context!)
- Data Types
  - Observational instead of factual data
- Data Access
  - “The Internet of Things”

03. Sep. 2005 Dagstuhl WSN Summer School 29

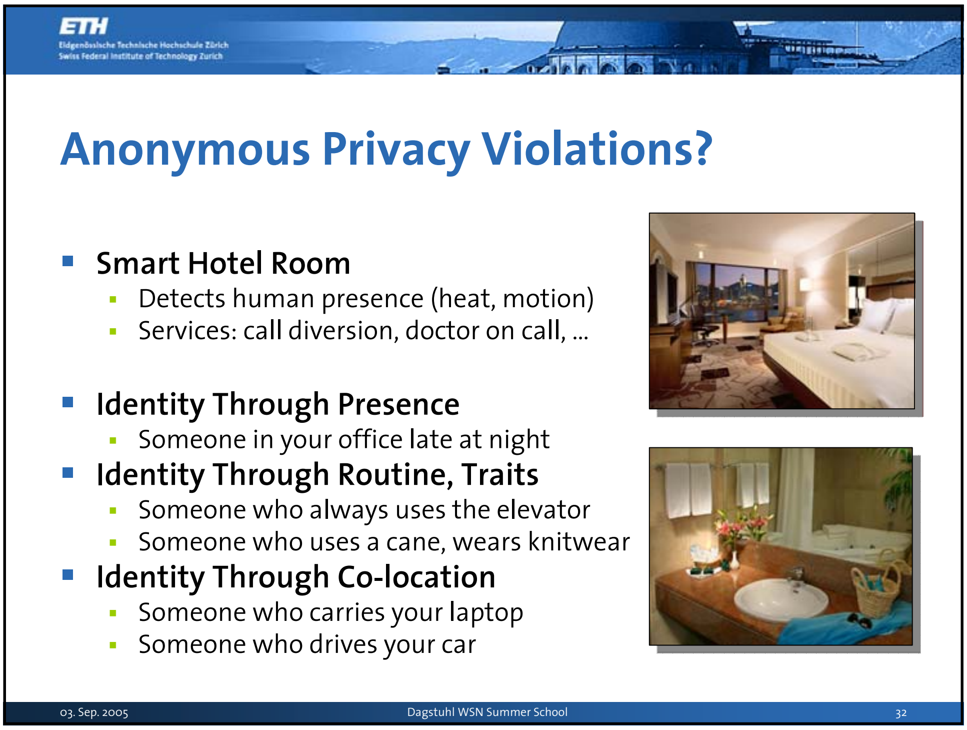


ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

## Privacy and Wireless Sensor Networks?

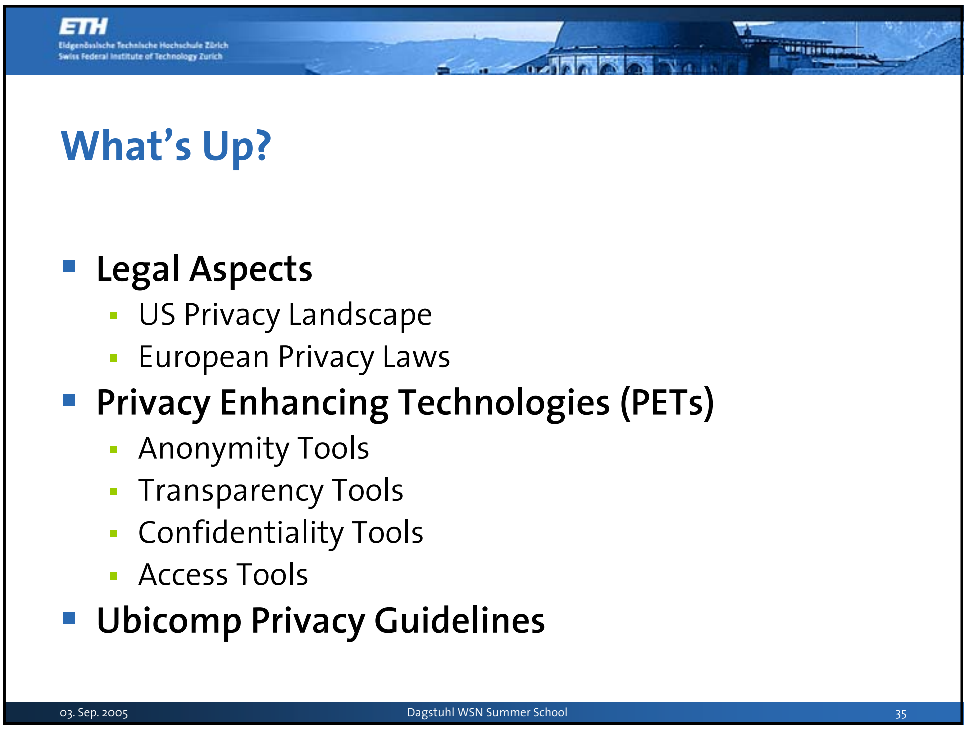
- Military Applications?
  - Detection of enemy tanks, soldiers
  - Protecting landmines
- Environmental Applications?
  - Detecting & monitoring forest fires, oil spills
  - Monitoring animals in the wild
- Building Automation?
  - Regulating energy consumption
  - Finding people in an emergency
- Services!
  - Health Care, “Floating Cars”, CCTV Network, ...

03. Sep. 2005 Dagstuhl WSN Summer School 31



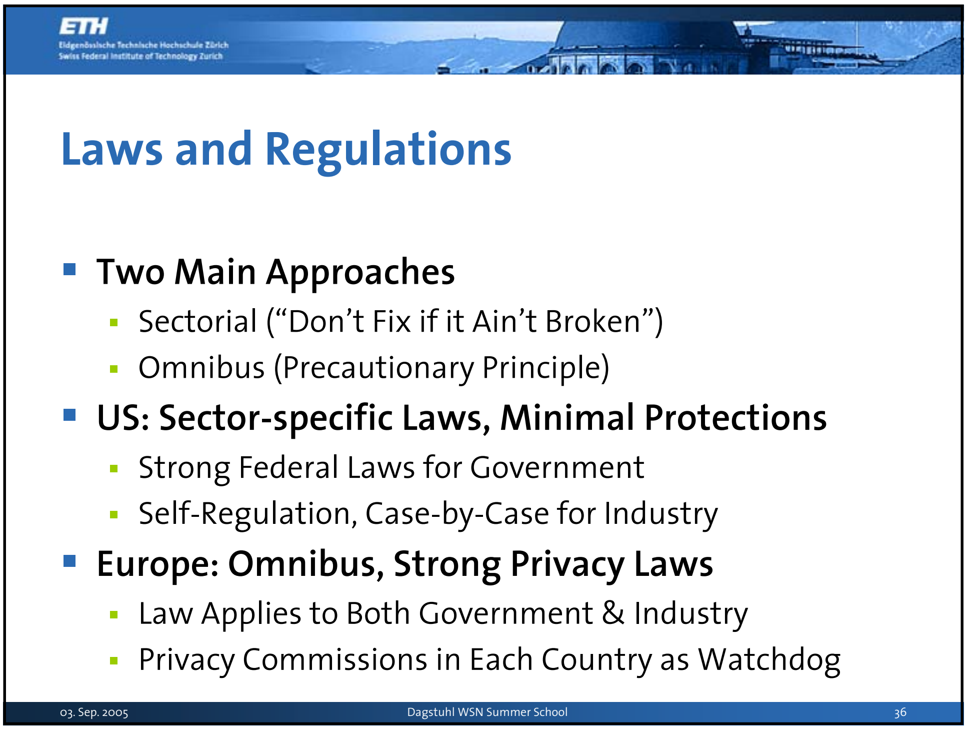
# Anonymous Privacy Violations?

- Smart Hotel Room
  - Detects human presence (heat, motion)
  - Services: call diversion, doctor on call, …
- Identity Through Presence
  - Someone in your office late at night
- Identity Through Routine, Traits
  - Someone who always uses the elevator
  - Someone who uses a cane, wears knitwear
- Identity Through Co-location
  - Someone who carries your laptop
  - Someone who drives your car



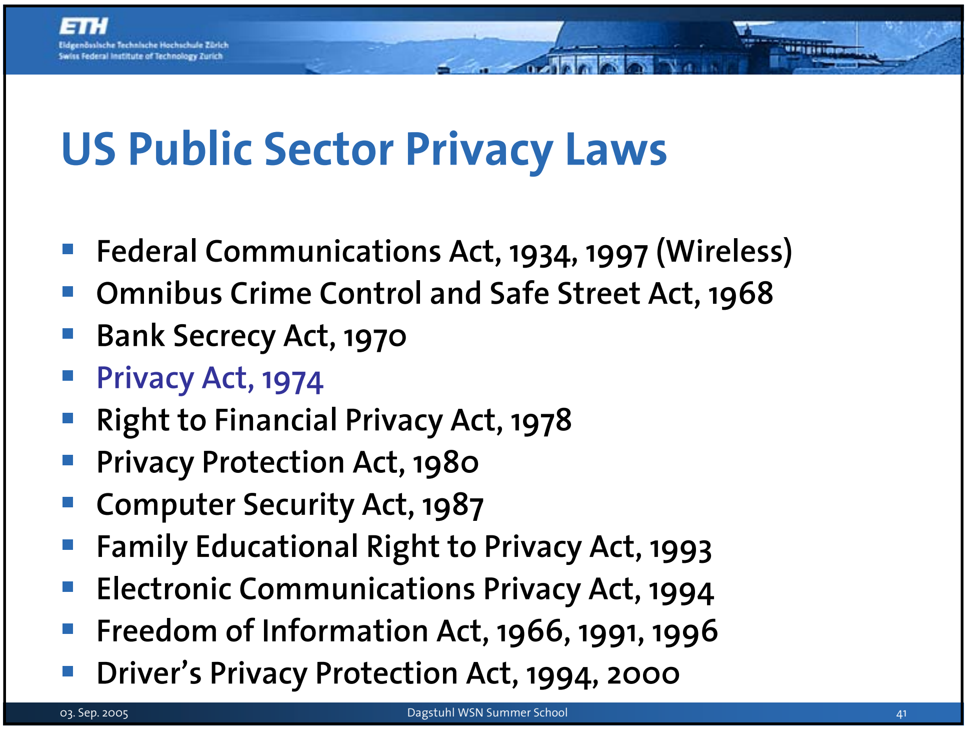
# What's Up?

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



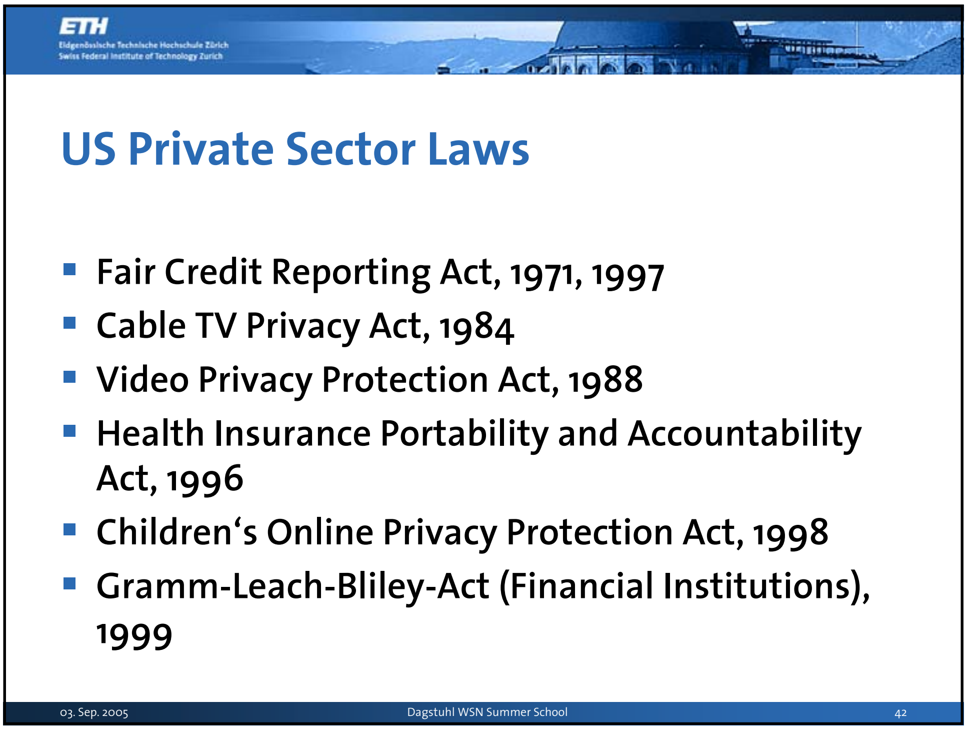
# Laws and Regulations

- 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



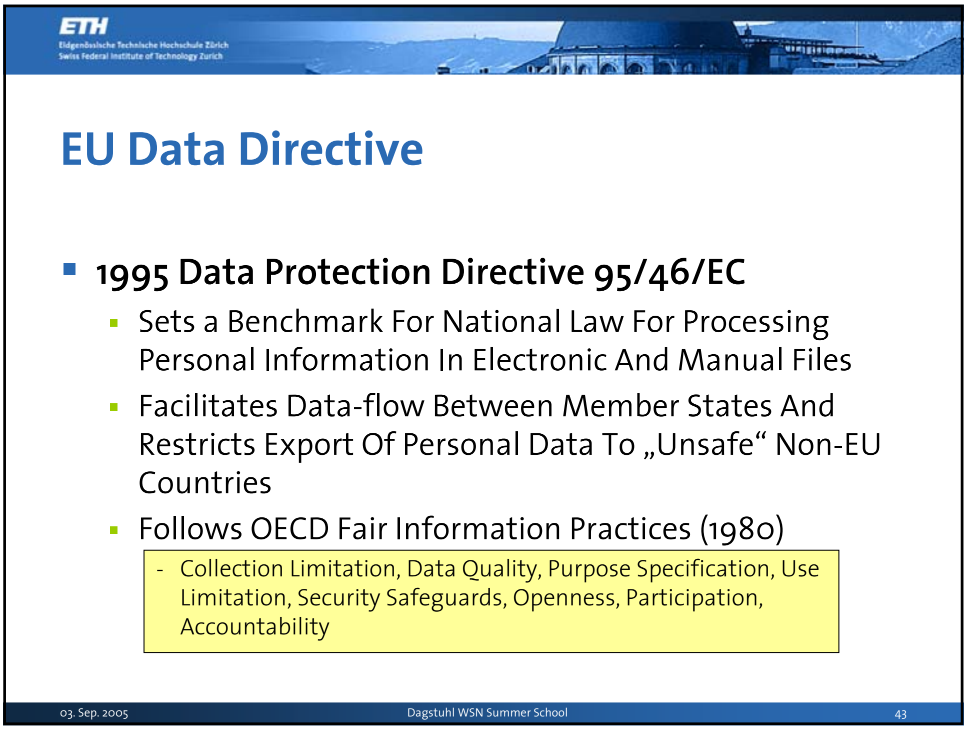
# US Public Sector Privacy Laws

- 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



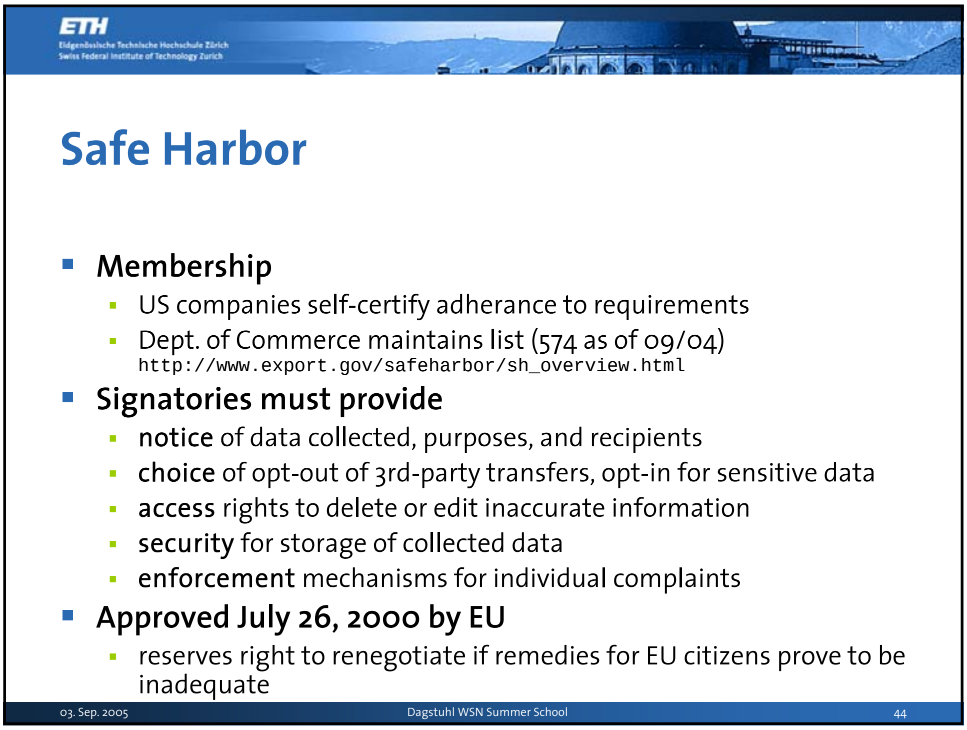
## US Private Sector Laws

- 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



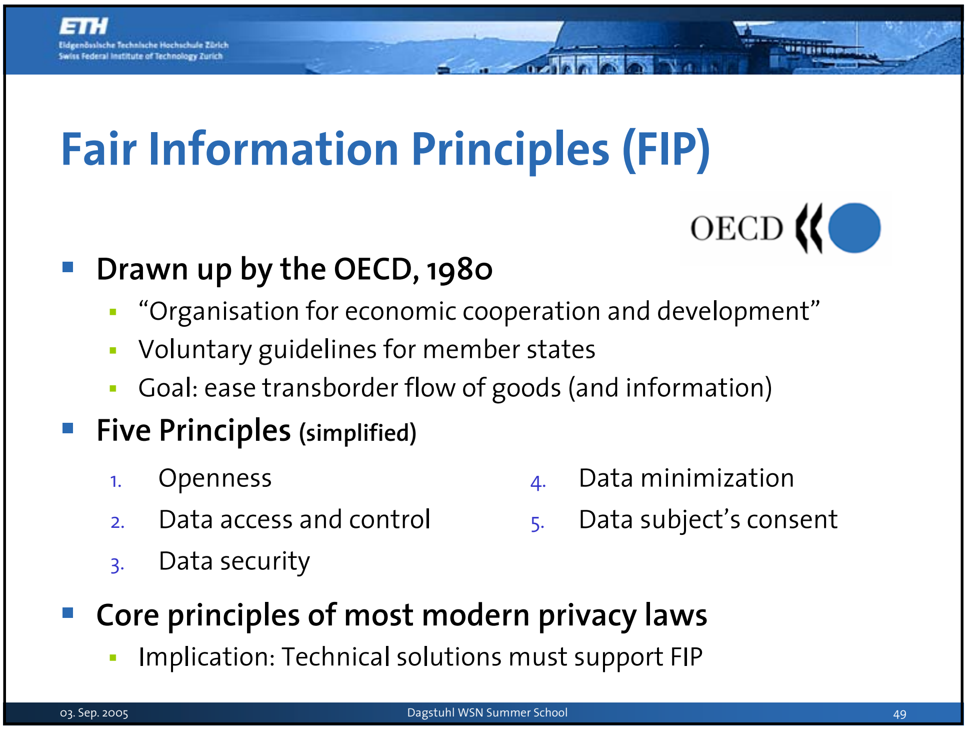
## EU Data Directive

- 1995 Data Protection Directive 95/46/EC
  - Sets a Benchmark For National Law For Processing Personal Information In Electronic And Manual Files
  - Facilitates Data-flow Between Member States And Restricts Export Of Personal Data To „Unsafe“ Non-EU Countries
  - Follows OECD Fair Information Practices (1980)
    - Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Participation, Accountability



## Safe Harbor

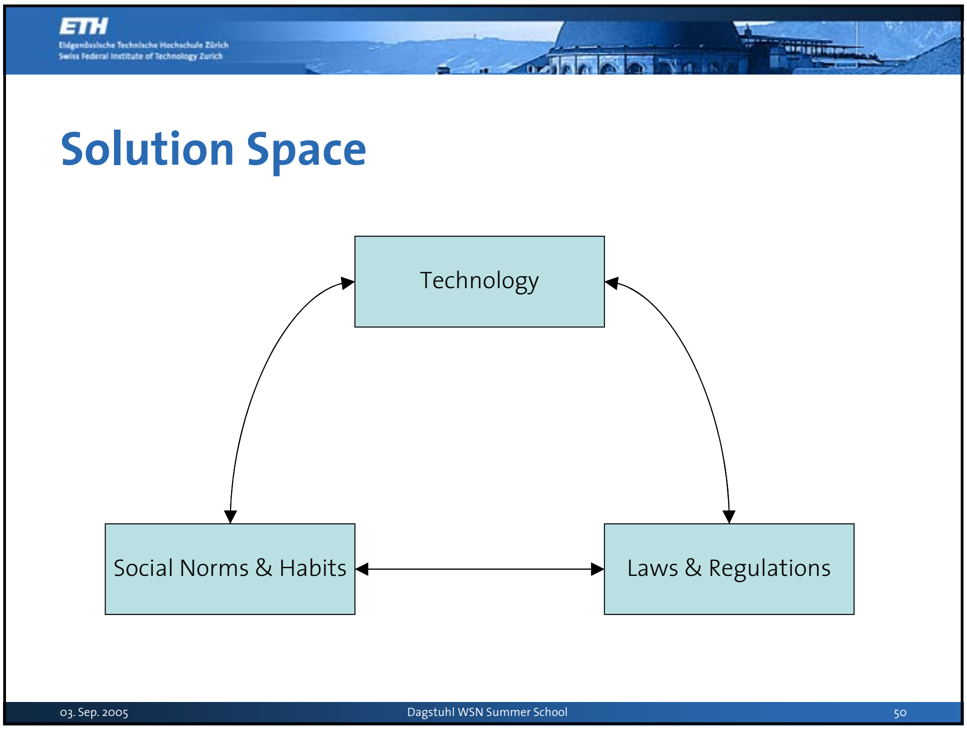
- Membership
  - US companies self-certify adherance to requirements
  - Dept. of Commerce maintains list (574 as of 09/04)
    `http://www.export.gov/safeharbor/sh_overview.html`
- Signatories must provide
  - **notice** of data collected, purposes, and recipients
  - **choice** of opt-out of 3rd-party 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



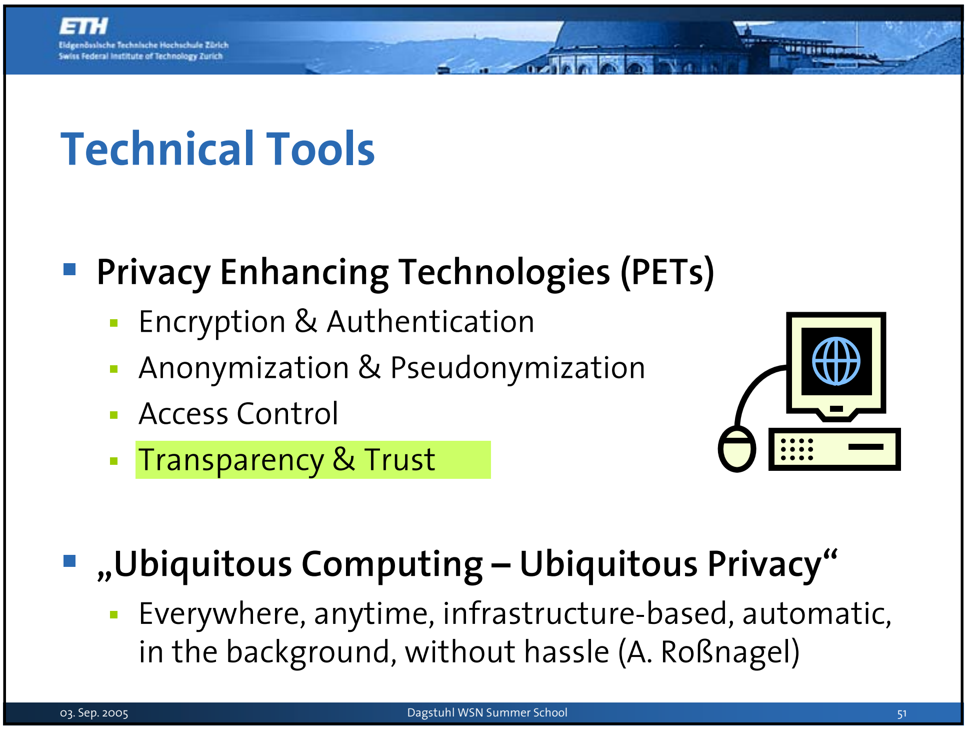
## Fair Information Principles (FIP)

OECD

- Drawn up by the OECD, 1980
  - "Organisation for economic cooperation and development"
  - Voluntary guidelines for member states
  - Goal: ease transborder flow of goods (and information)
- Five Principles (simplified)
  1. Openness
  2. Data access and control
  3. Data security
  4. Data minimization
  5. Data subject's consent
- Core principles of most modern privacy laws
  - Implication: Technical solutions must support FIP



## Solution Space

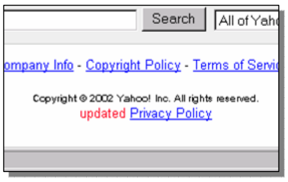


## Technical Tools

- **Privacy Enhancing Technologies (PETs)**
  - Encryption & Authentication
  - Anonymization & Pseudonymization
  - Access Control
  - Transparency & Trust
- **„Ubiquitous Computing – Ubiquitous Privacy“**
  - Everywhere, anytime, infrastructure-based, automatic, in the background, without hassle (A. Roßnagel)

## Transparency on the Web

- 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



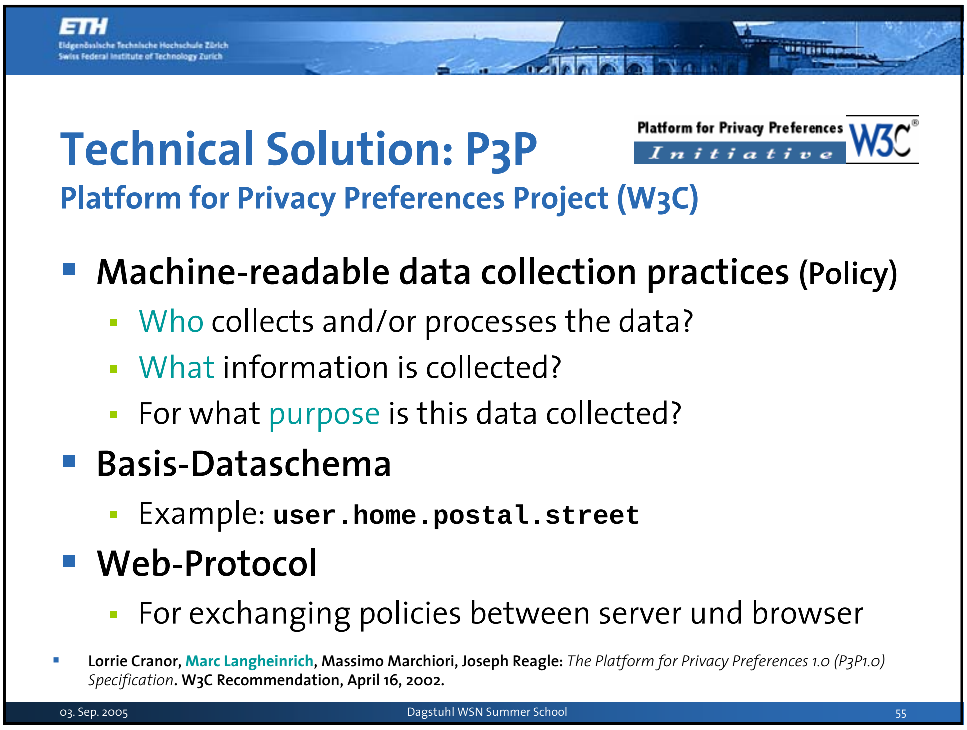
ompany Info - Copyright Policy - Terms of Servic

Copyright © 2002 Yahoo! Inc. All rights reserved.
updated Privacy Policy

## Privacy Policies Drawbacks

- **But**, Policies are Often...
  - difficult to understand
  - hard to find
  - lengthy to read
    - usually 3-4 pages!
  - changed without notice

Amazon.com Privacy Policy



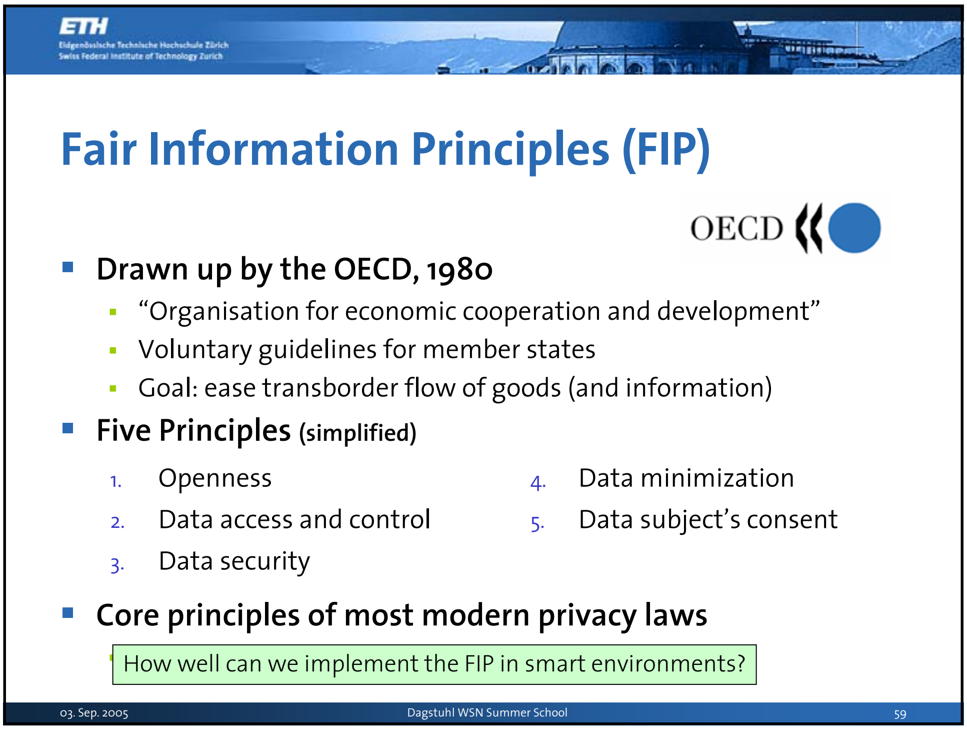
## Technical Solution: P3P

### Platform for Privacy Preferences Project (W3C)

Platform for Privacy Preferences Initiative W3C®

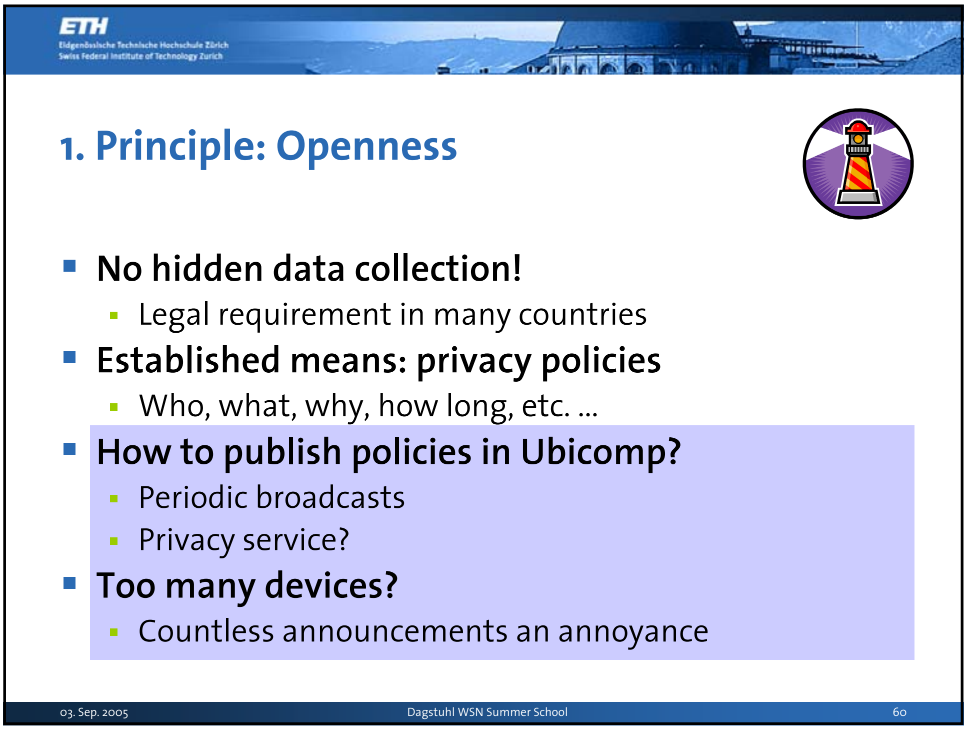
- Machine-readable data collection practices (Policy)
  - Who collects and/or processes the data?
  - What information is collected?
  - For what purpose is this data collected?
- Basis-Dataschema
  - Example: `user.home.postal.street`
- Web-Protocol
  - For exchanging policies between server und browser

- Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Joseph Reagle: *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*. W3C Recommendation, April 16, 2002.



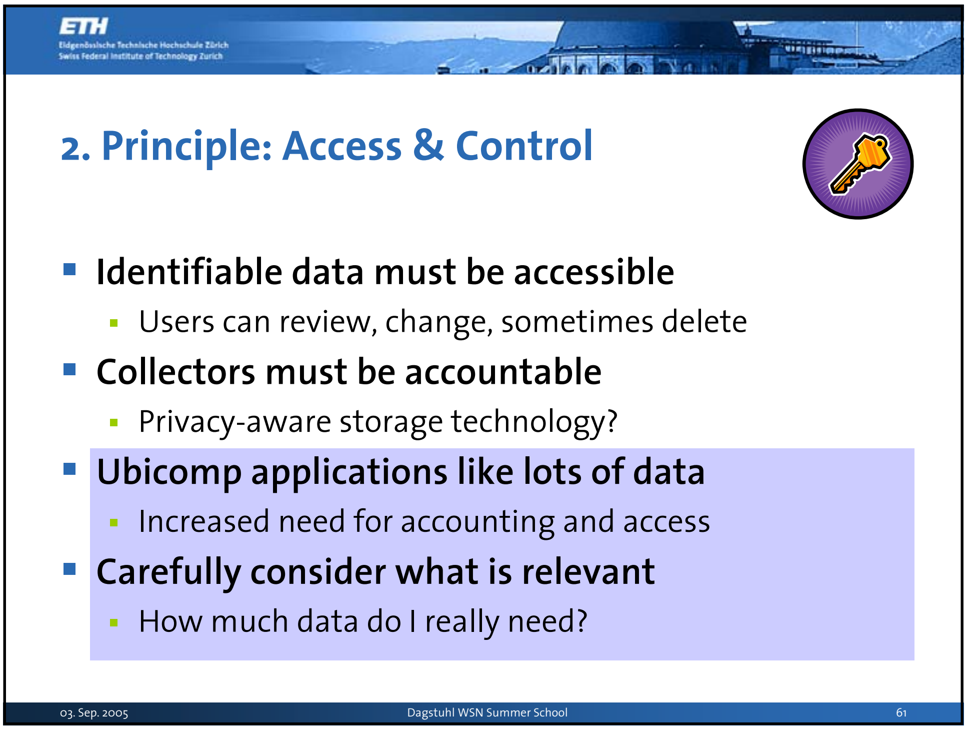
## Fair Information Principles (FIP)

- Drawn up by the OECD, 1980
  - "Organisation for economic cooperation and development"
  - Voluntary guidelines for member states
  - Goal: ease transborder flow of goods (and information)
- Five Principles (simplified)
  1. Openness
  2. Data access and control
  3. Data security
  4. Data minimization
  5. Data subject's consent
- Core principles of most modern privacy laws
  - How well can we implement the FIP in smart environments?



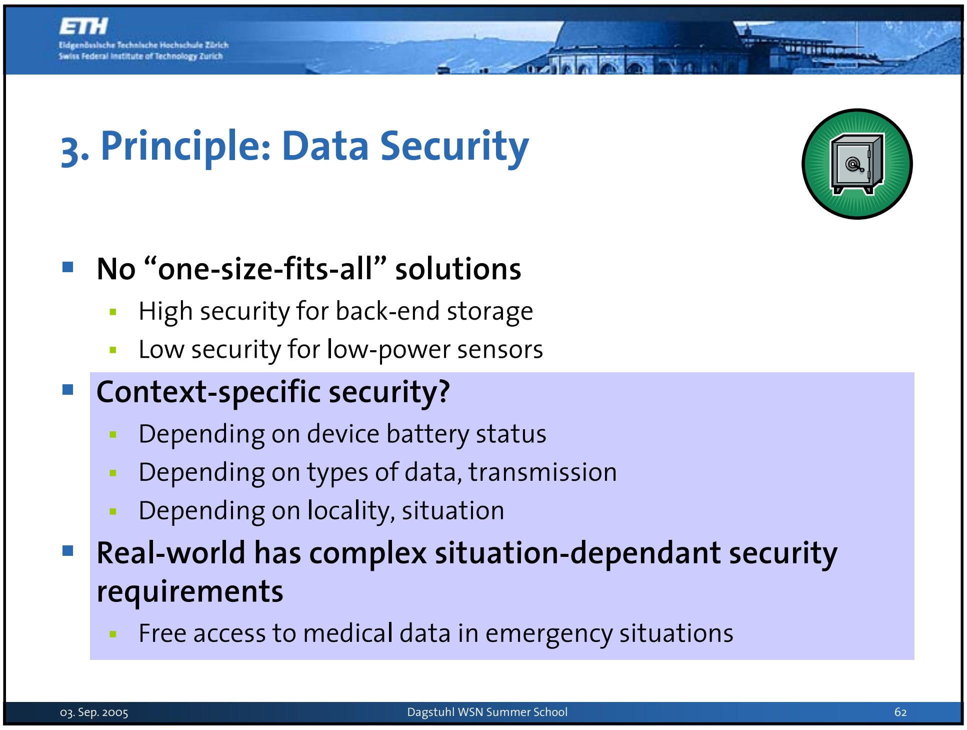
## 1. Principle: Openness

- 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



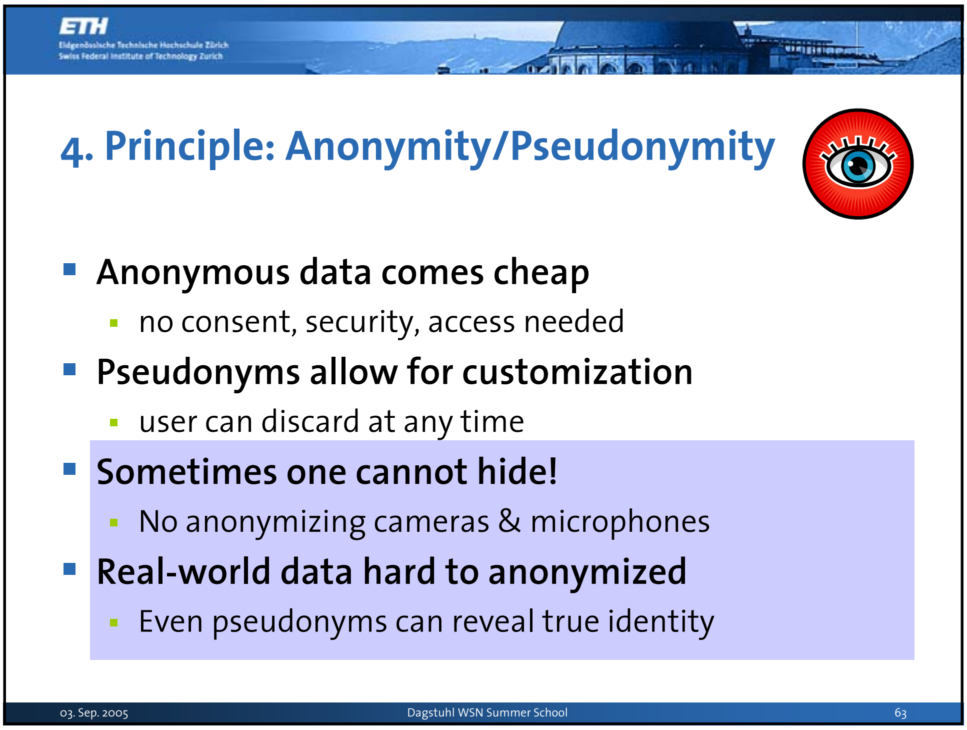
## 2. Principle: Access & Control

- 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?



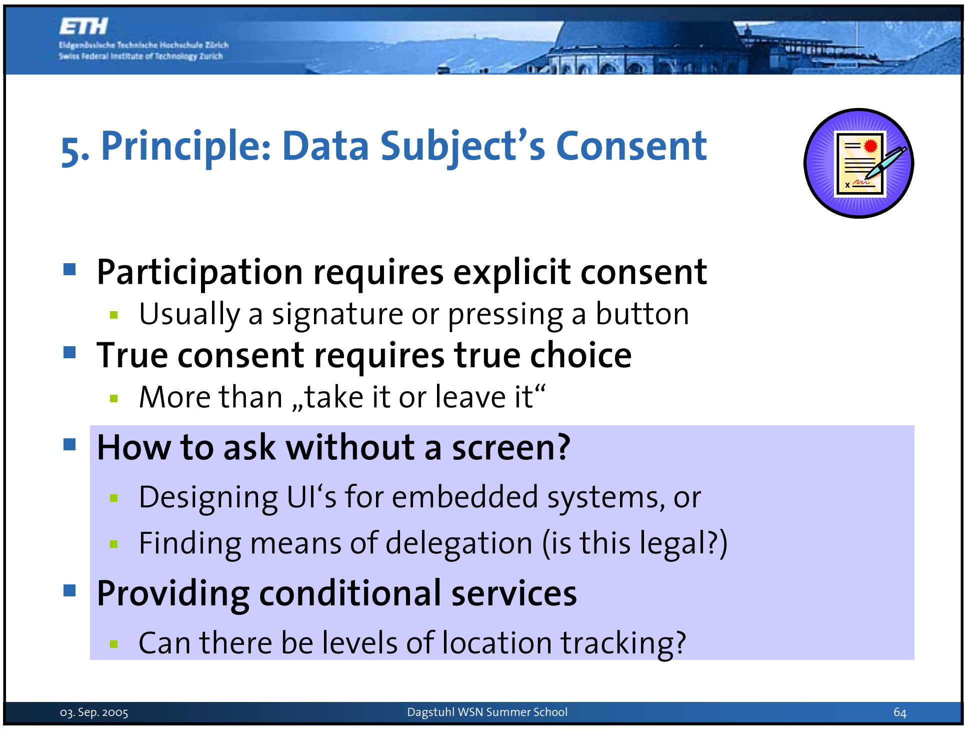
## 3. Principle: Data Security

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



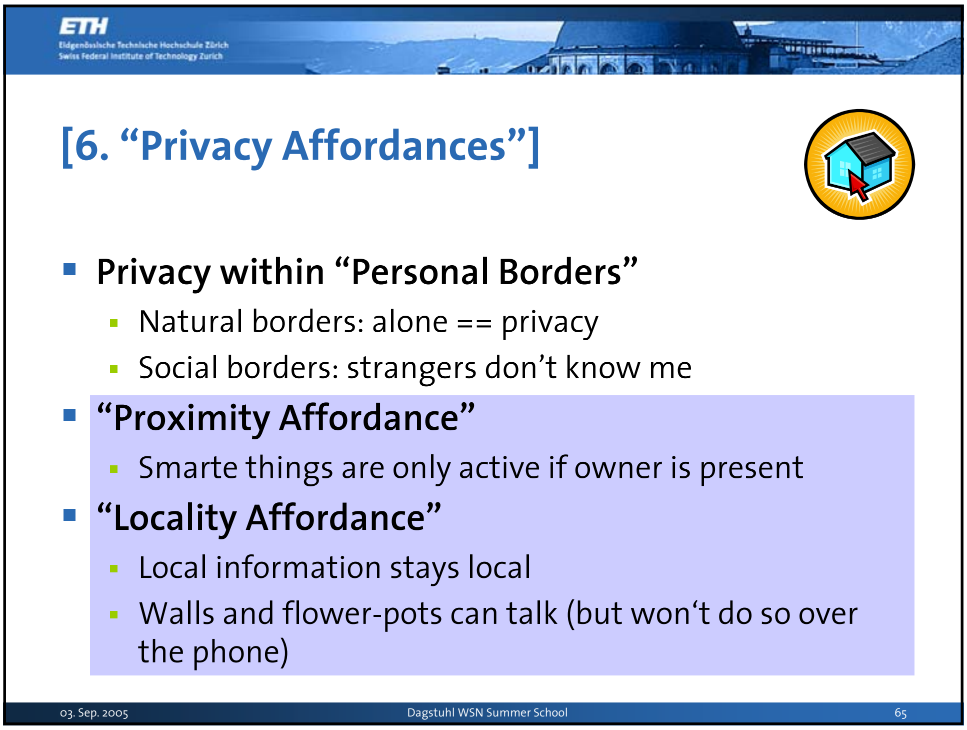
## 4. Principle: Anonymity/Pseudonymity

- 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



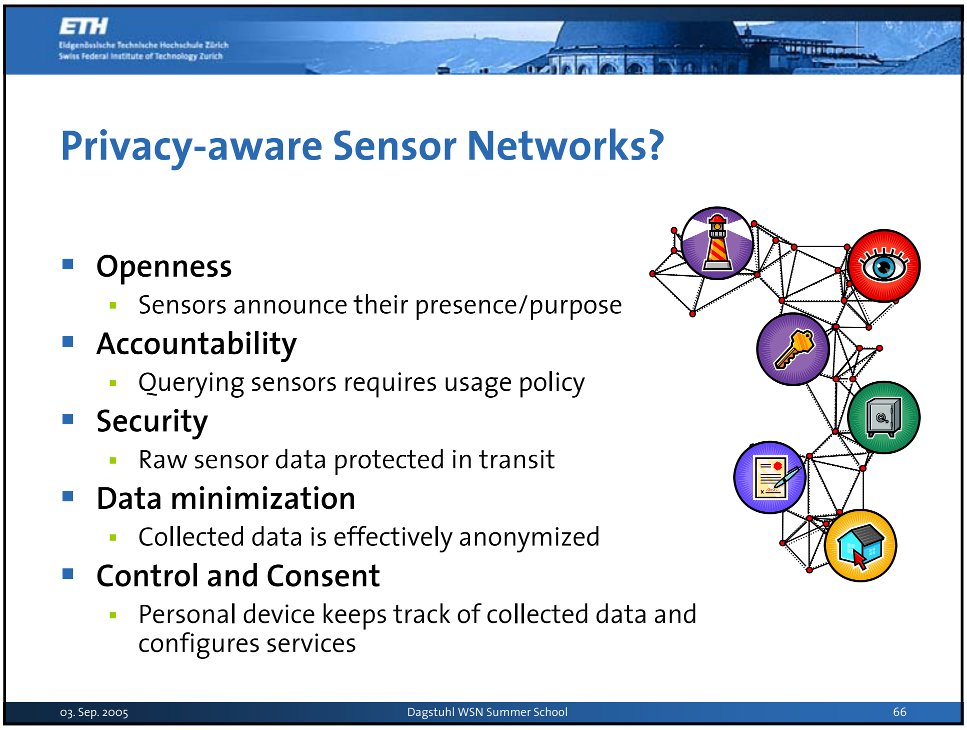
## 5. Principle: Data Subject’s Consent

- 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?



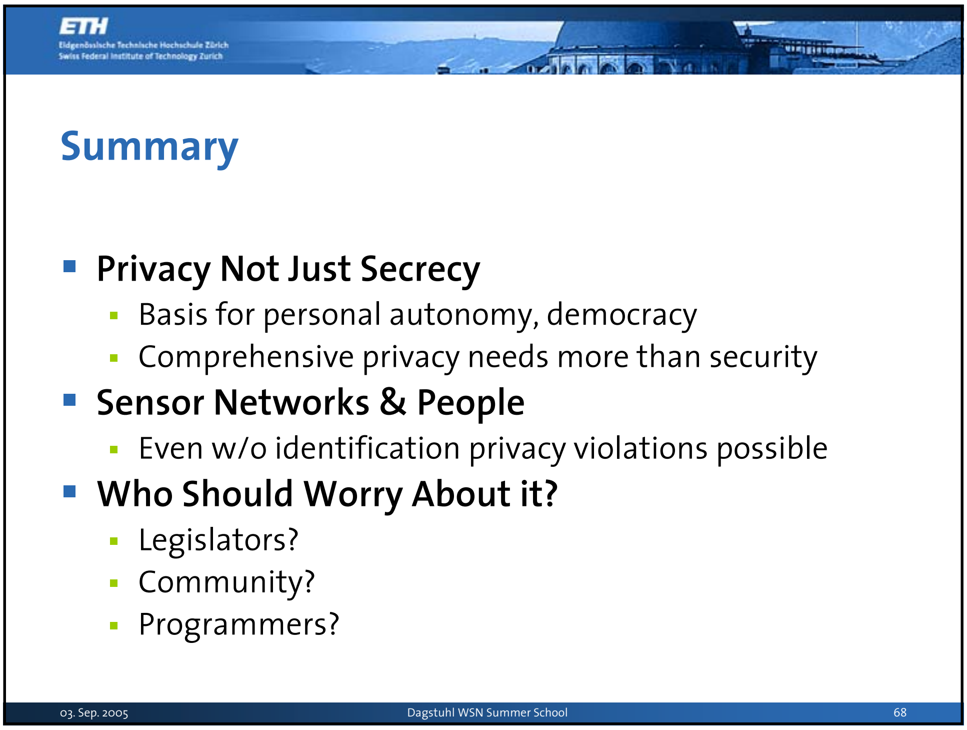
## [6. “Privacy Affordances”]

- Privacy within “Personal Borders”
  - Natural borders: alone == privacy
  - Social borders: strangers don’t know me
- “Proximity Affordance”
  - Smarte things are only active if owner is present
- “Locality Affordance”
  - Local information stays local
  - Walls and flower-pots can talk (but won‘t do so over the phone)



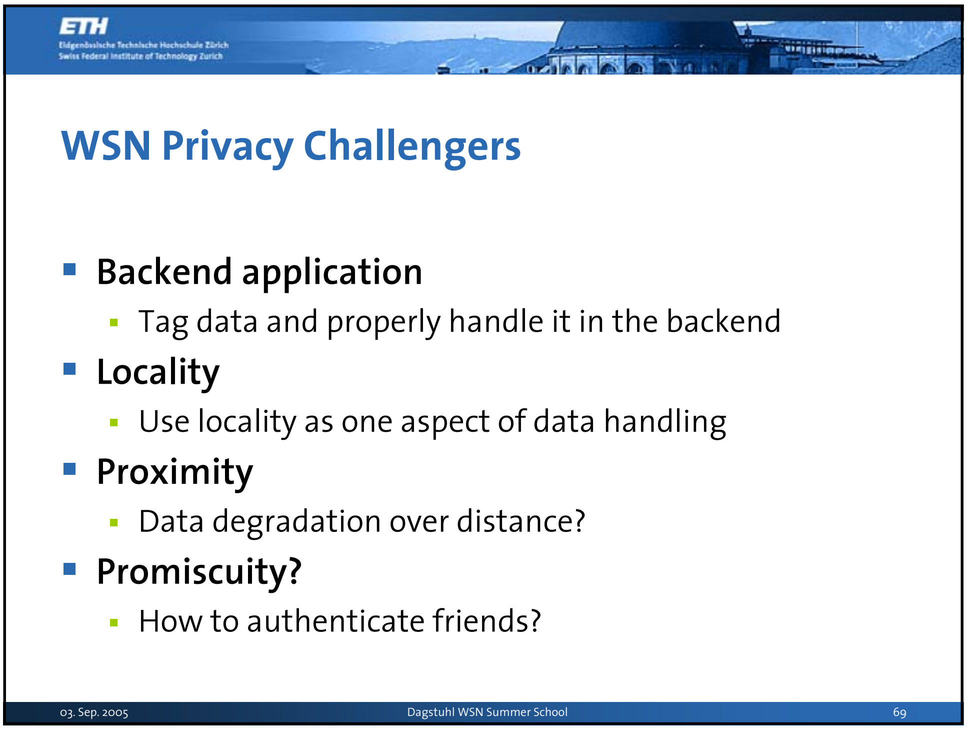
## Privacy-aware Sensor Networks?

- Openness
  - Sensors announce their presence/purpose
- Accountability
  - Querying sensors requires usage policy
- Security
  - Raw sensor data protected in transit
- Data minimization
  - Collected data is effectively anonymized
- Control and Consent
  - Personal device keeps track of collected data and configures services



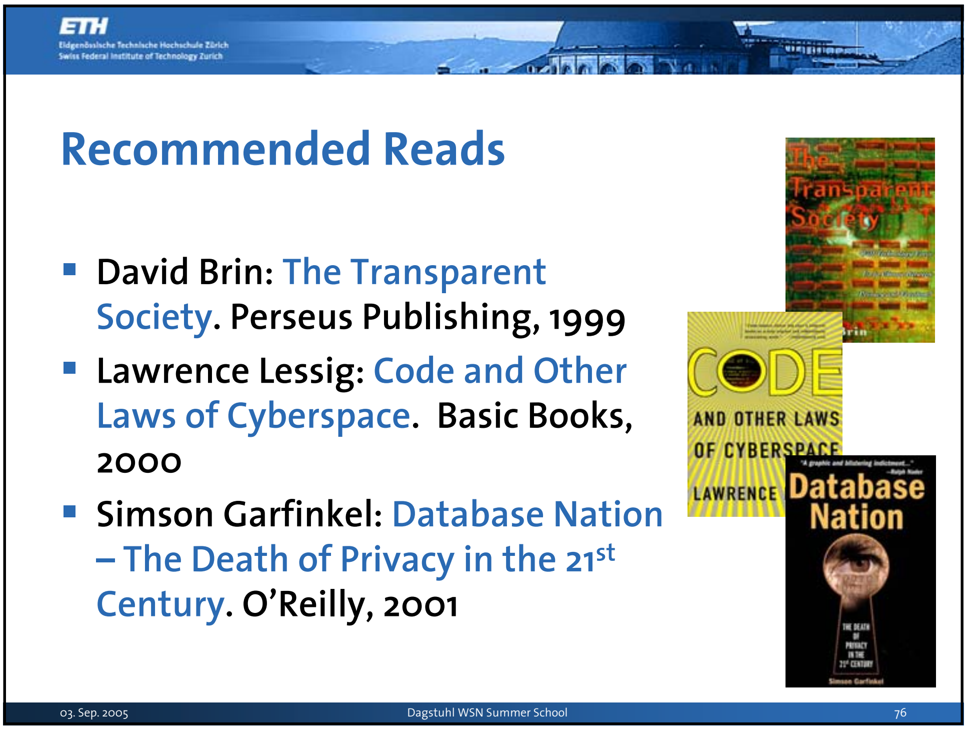
## Summary

- Privacy Not Just Secrecy
  - Basis for personal autonomy, democracy
  - Comprehensive privacy needs more than security
- Sensor Networks & People
  - Even w/o identification privacy violations possible
- Who Should Worry About it?
  - Legislators?
  - Community?
  - Programmers?



## WSN Privacy Challengers

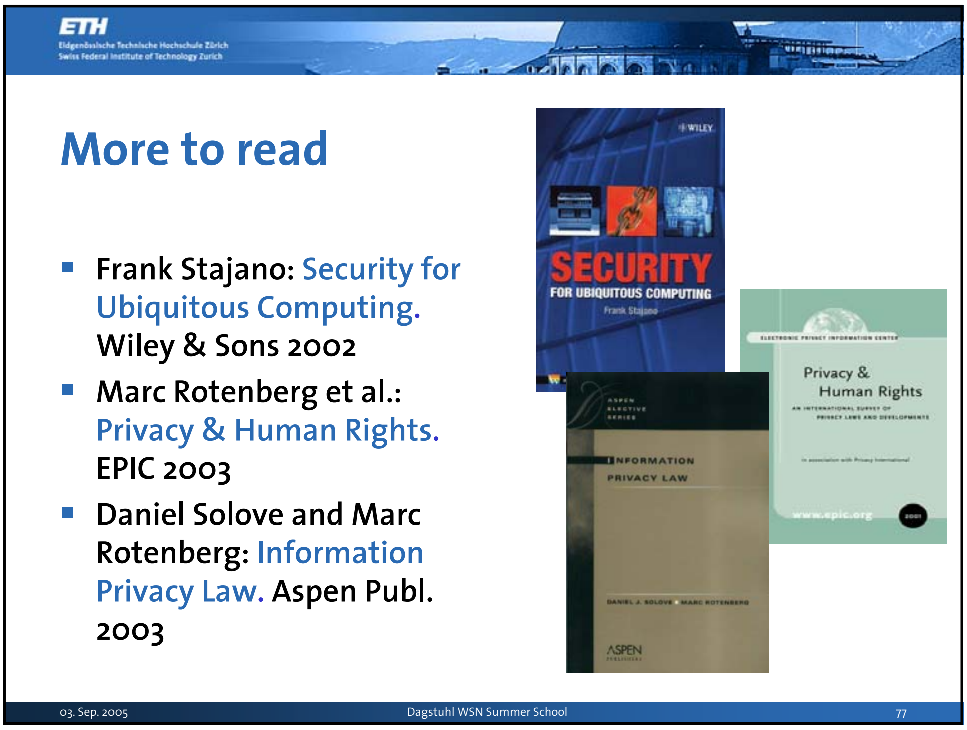
- Backend application
  - Tag data and properly handle it in the backend
- Locality
  - Use locality as one aspect of data handling
- Proximity
  - Data degradation over distance?
- Promiscuity?
  - How to authenticate friends?



## Recommended Reads

- 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 21$^{st}$ Century. O'Reilly, 2001

The Transparent Society
CODE
AND OTHER LAWS
OF CYBERSPACE
LAWRENCE
Database Nation
THE DEATH OF PRIVACY IN THE 21ST CENTURY
Simson Garfinkel



WILEY
SECURITY
FOR UBIQUITOUS COMPUTING
Frank Stajano
ELECTRONIC PRIVACY INFORMATION CENTER
Privacy &
Human Rights
AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS
www.epic.org
2001
ASPEN ELECTIVE SERIES
INFORMATION
PRIVACY LAW
DANIEL J. SOLOVE · MARC ROTENBERG
ASPEN

# More to read

- 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