Personal Privacy in Pervasive 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

This Morning's Program

- The Case for Ubicomp Privacy
  - What is Privacy?
  - Why Would We Want it?
- Coffee Break
- Tools for Ubicomp Privacy
  - Technical Tools
  - Legal Mechanisms

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?
- Privacy Solutions
  - How Can We Achieve Privacy?

1. Privacy Definition

What is Privacy, Anyway?

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?

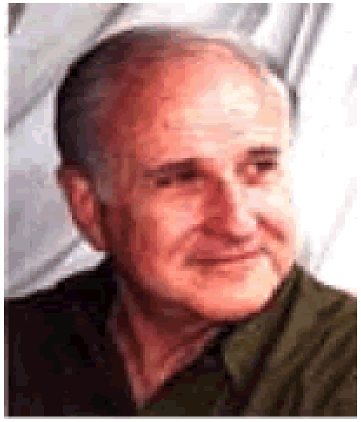
What Is Privacy?

- „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“)



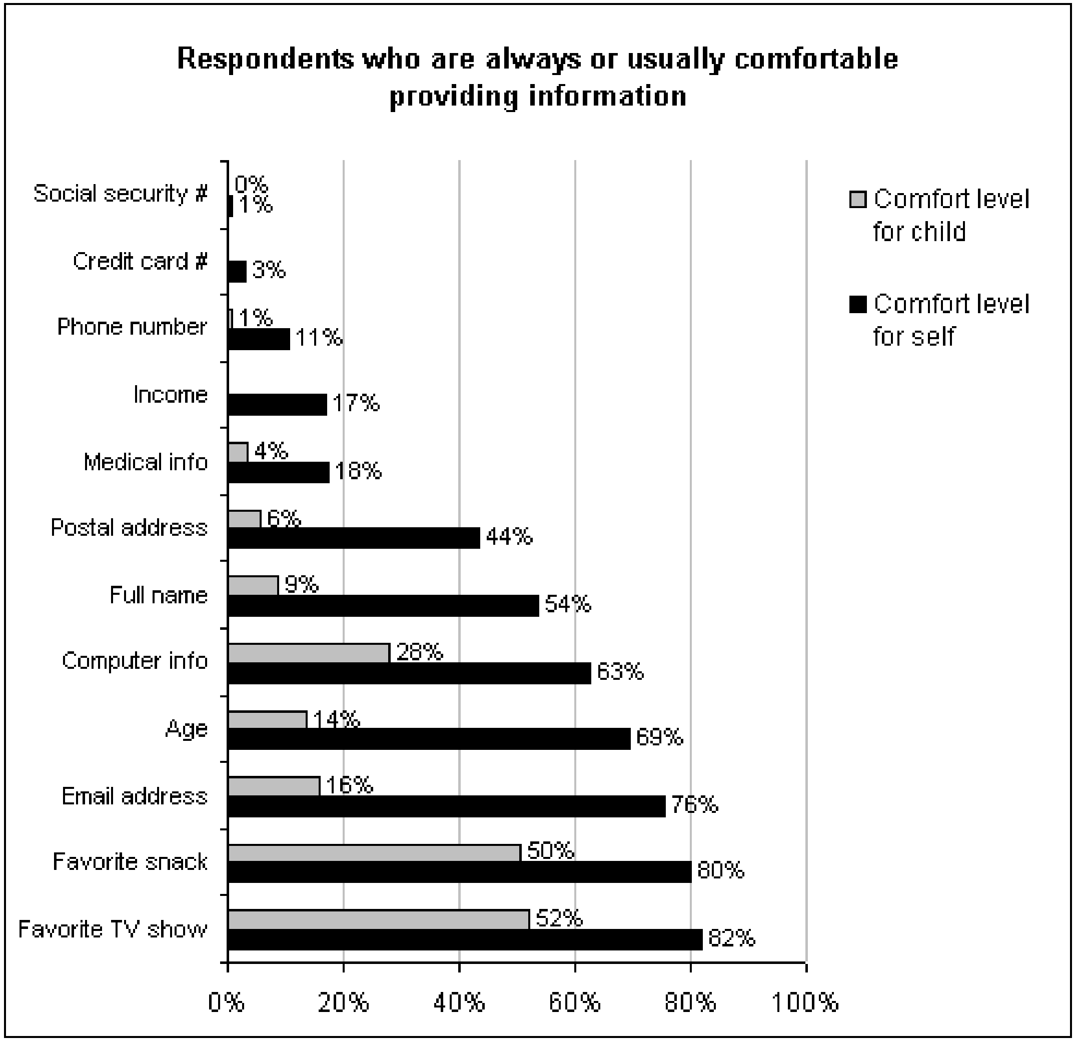
Facets

- 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

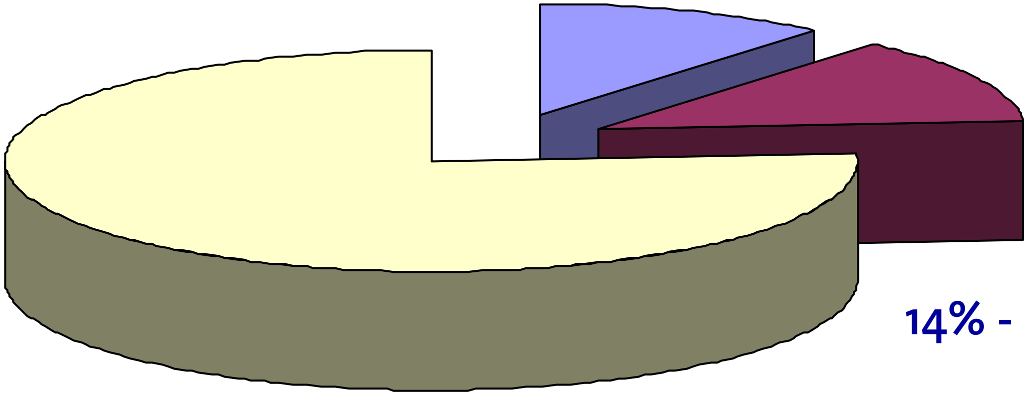
PAYBACK

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)



11% - Privacy Fundamentalists

14% - Privacy Unconcerned

76% - Privacy Pragmatists

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

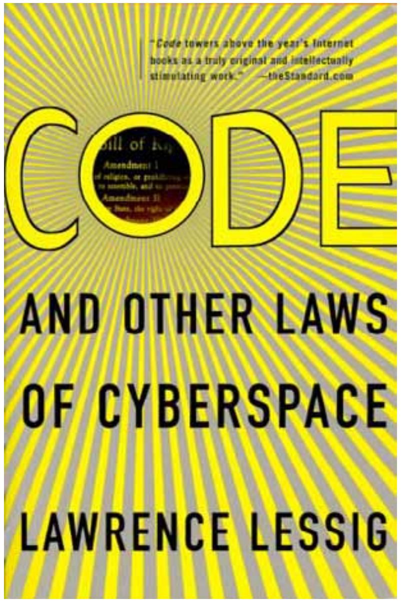
- 1948 United Nations, Universal Declaration Of Human Rights: Article 12
  - No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences 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


"Code towers above the year's Internet books as a truly original and intellectually stimulating work." —theStandard.com
CODE
AND OTHER LAWS OF CYBERSPACE
LAWRENCE LESSIG

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

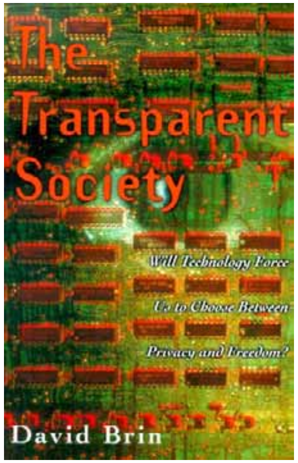
- Named After Megan Kanka (1987-1994)
  - Raped And Strangled By A (New) Neighbor, Who Had Previously Been Convicted Of Two Sexual Assaults Against Young Girls
- 1994 Congressional Guidelines
  - Encourages States To Pass Laws Requiring Registration Of "Sex Offenders" With Local Law Enforcement
  - Enacted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

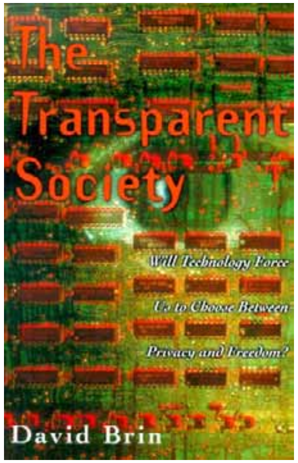

The Transparent Society
Will Technology Force Us to Choose Between Privacy and Freedom?
David Brin

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



The Transparent Society
Will Technology Force Us to Choose Between Privacy and Freedom?
David Brin

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

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?

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

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?

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.

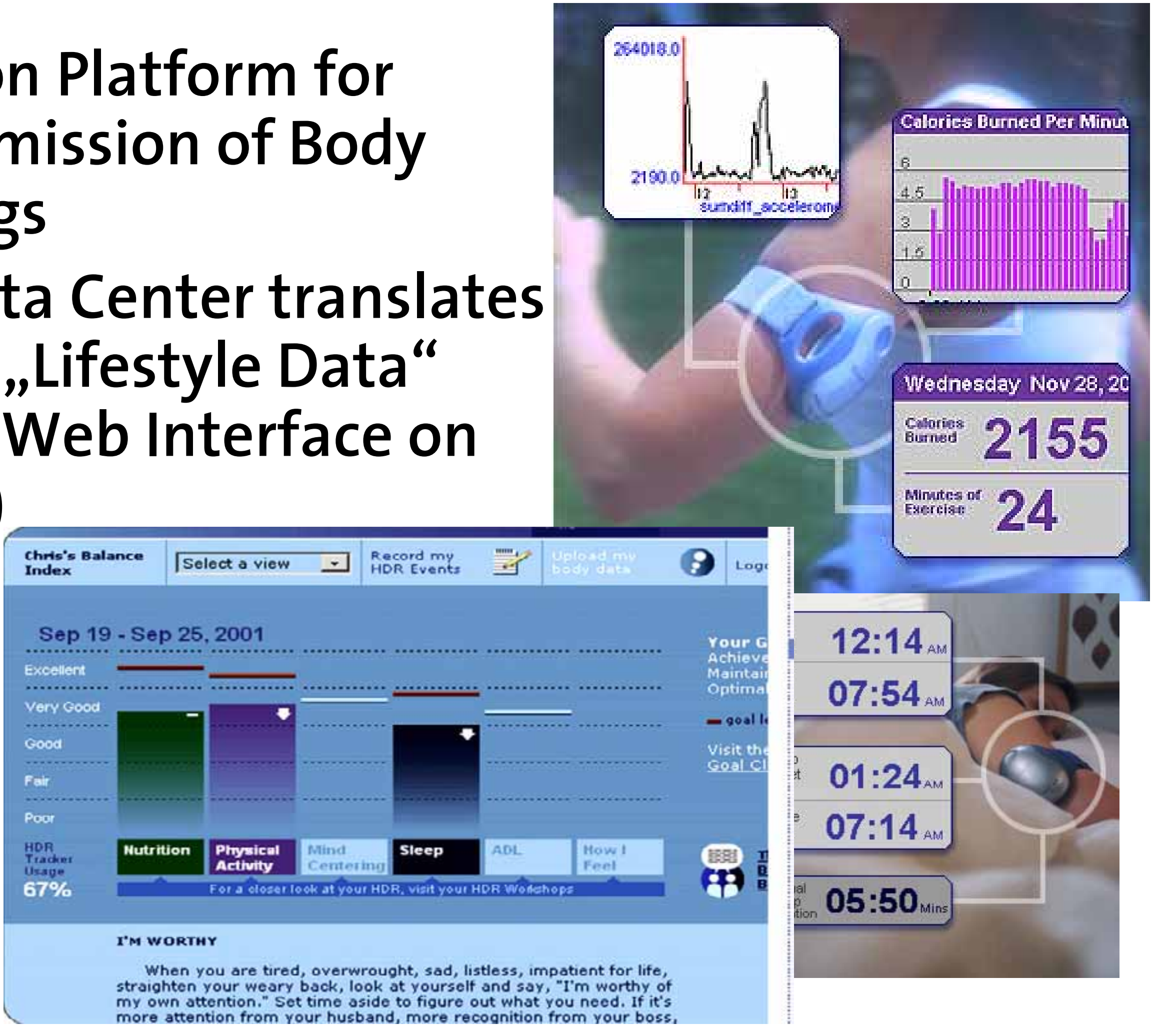
http://www.sportbrain.com/

: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)



I'M WORTHY

When you are tired, overwrought, sad, listless, impatient for life, straighten your weary back, look at yourself and say, "I'm worthy of my own attention." Set time aside to figure out what you need. If it's more attention from your husband, more recognition from your boss,

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

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?

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 Mid-Term 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, 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, Choice & Consent, Anonymity, Security, Access & Recourse, Expectations
- Privacy in Pervasive Computing
  - New Options
  - New Challenges

After the Break:
Privacy Laws And Technical Tools

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?

- Privacy Enhancing Technologies (PETs)
  - Encryption & Authentication
  - Anonymization & Pseudonymization
  - Access & Control
  - Transparency & Trust
- Legal Aspects
  - US Privacy Landscape
  - European Privacy Laws

Solution Space Revisited

- Notice and Disclosure
  - Transparency Tools
- Choice and Consent
  - Anonymity and Pseudonymity Tools
- Security
  - Encryption and Authentication Tools
- Access and Control
  - PETs in the Enterprise
- Recourse
  - Laws and Regulations

Anonymity & Pseudonymity

RESEARCH GROUP FOR

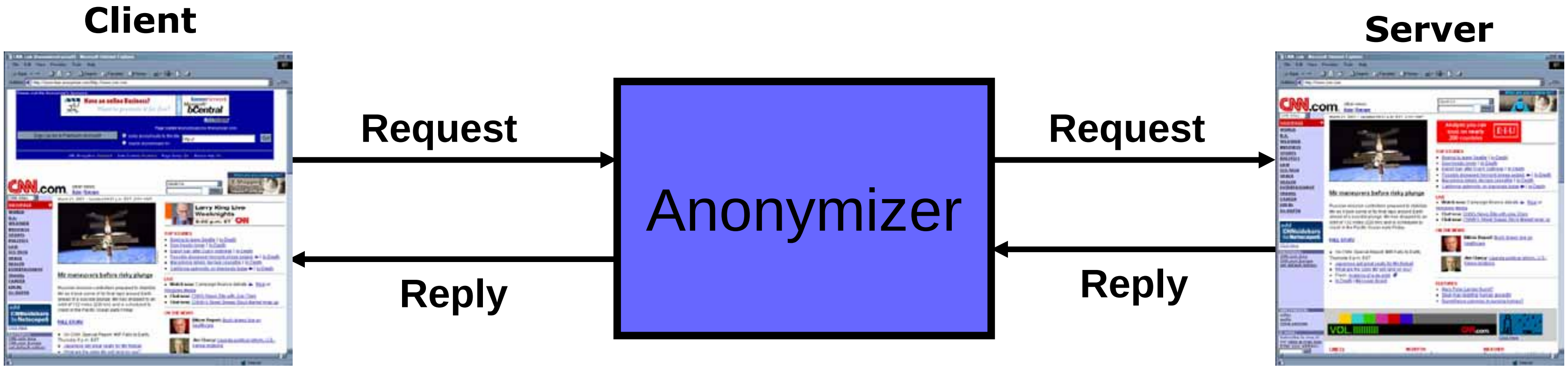
Distributed Systems

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Anonymizing Proxies

- Acts as a proxy for users
- Hides information from end servers



Client

Request

Reply

Anonymizer

Request

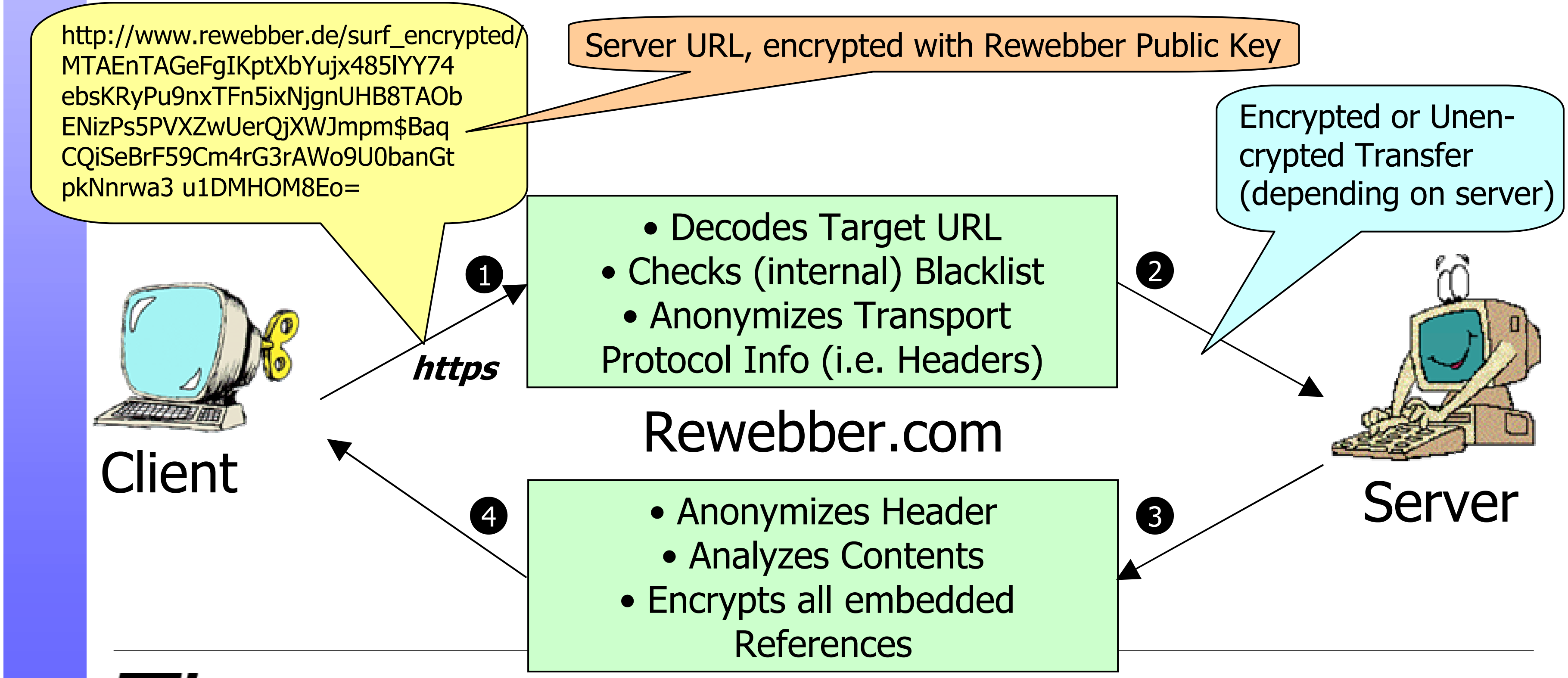
Reply

Server

- Proxy Sees all traffic
- User Identity Easily Compromisable
- Note: Server Identity Protectable (Rewebber)

Rewebber.com

- Created at Hagen University, Germany
- Provides both Client- and Server-Anonymity
- Only as subscription service ($5-$15 per month)



http://www.rewebber.de/surf_encrypted/
MTAEnTAGeFgIKptXbYujx485lYY74
ebsKRyPu9nxTFn5ixNjgnUHB8TAOb
ENizPs5PVXZwUerQjXWJmpm$Baq
CQiSeBrF59Cm4rG3rAWo9U0banGt
pkNnrwa3 u1DMHOM8Eo=

Server URL, encrypted with Rewebber Public Key

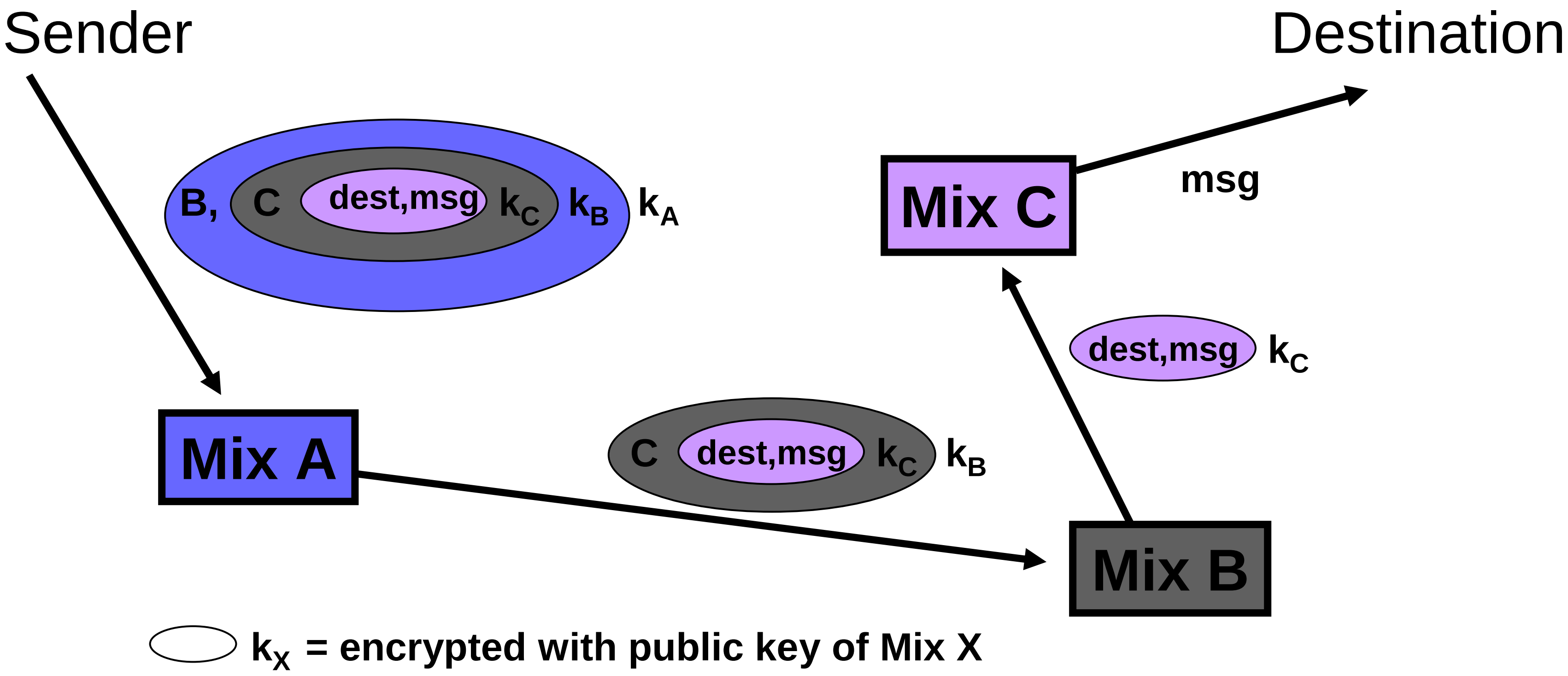
Encrypted or Unencrypted Transfer (depending on server)

- Decodes Target URL
- Checks (internal) Blacklist
- Anonymizes Transport Protocol Info (i.e. Headers)

Rewebber.com

- Anonymizes Header
- Analyzes Contents
- Encrypts all embedded References

Mixes [Chaum81]



Sender routes message randomly through network of “Mixes”, using layered public-key encryption.

Realization of Mixes

- Onion Routing (Office of Naval Research)
  - http://www.onion-router.net
  - service ended 01/2000
- Freedom (Zero-Knowledge Systems, Canada)
  - http://www.zeroknowledge.com
- Java Anon Proxy (TU Dresden)
  - http://anon.inf.tu-dresden.de

Further Issues

- Mobile IPv4/IPv6 Node Mobility
  - Binding Updates Can be Tracked
  - Unencrypted Home Network Address
  - Integration into Mix Networks necessary
- IPv6 Stateless Address Configuration
  - Address Based on Fixed Interface Identifier
  - Better: Fake Identifiers (Random/Statistical)
- Bluetooth BD_ADDR Problem

IPv6 Privacy See also: Alberto Escudero Pascale, KHT Sweden. http://www.it.kth.se/~aep/

Transparency Tools

RESEARCH GROUP FOR

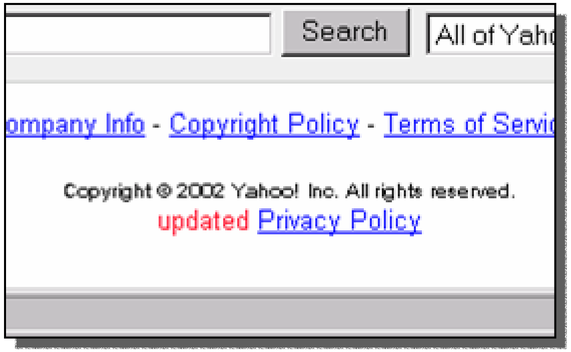
Distributed Systems

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Example: 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 Servi

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

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

Seal Programs

- TRUSTe – http://www.truste.org
- BBBOnline – http://www.bbbonline.org
- CPA WebTrust – http://www.cpawebtrust.org/
- Japanese Privacy Mark http://www.jipdec.or.jp/security/privacy/

Seal Program Problems

- Basic Principle:
  - Publish a policy (*any* policy) and follow it
- Only few require base-level standard
  - BBBOnline requires client in good standing with Better Business Bureau
- Effect:
  - Good notices of bad practices

P3P

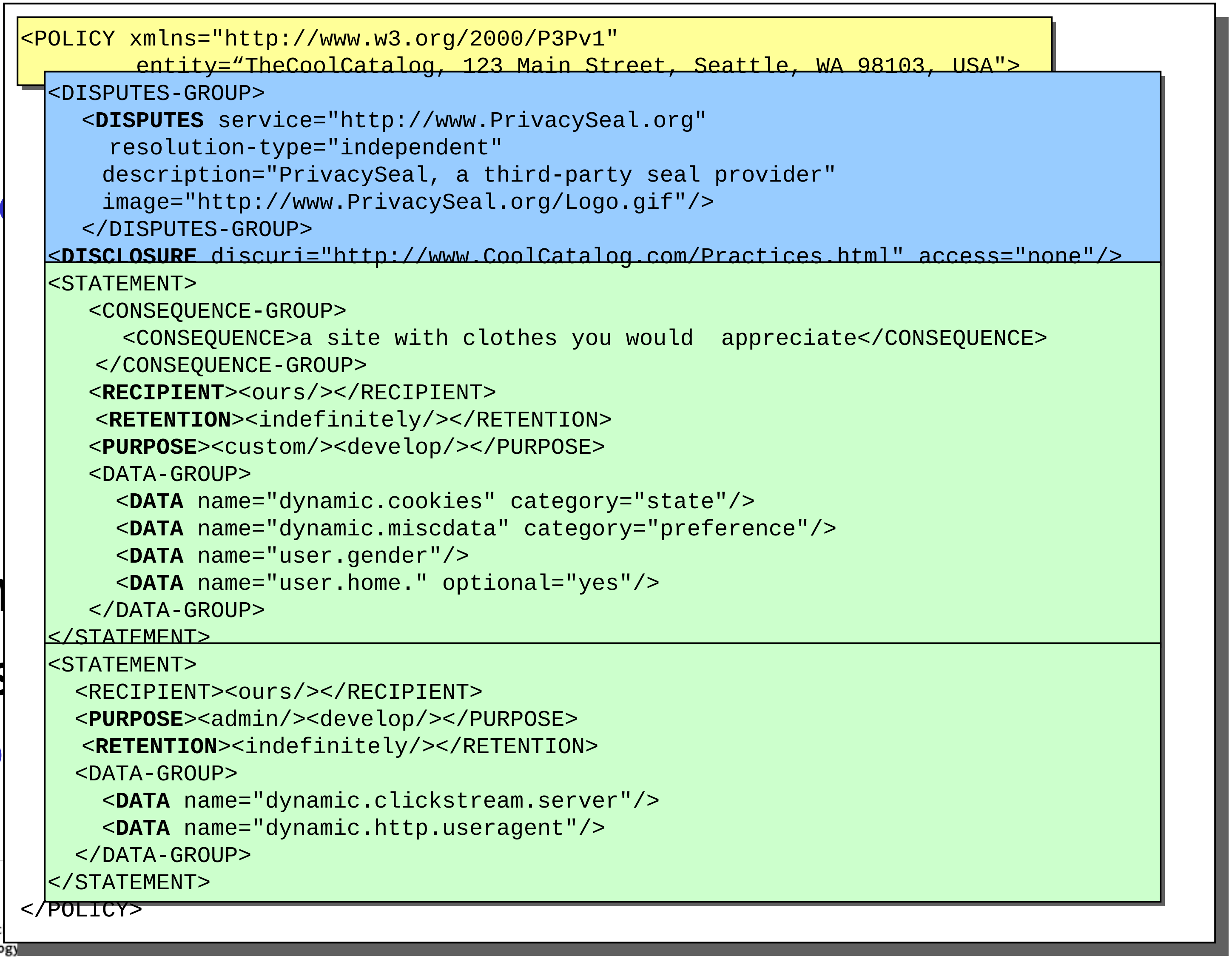
- Platform for Privacy Preference Project
  - Chartered by World Wide Web Consortium (W3C)
  - 1997-2001 (Recommendation December 2001)
- A framework for automated privacy discussions
  - Web sites disclose their privacy practices in standard machine-readable formats
  - Web browsers automatically retrieve 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

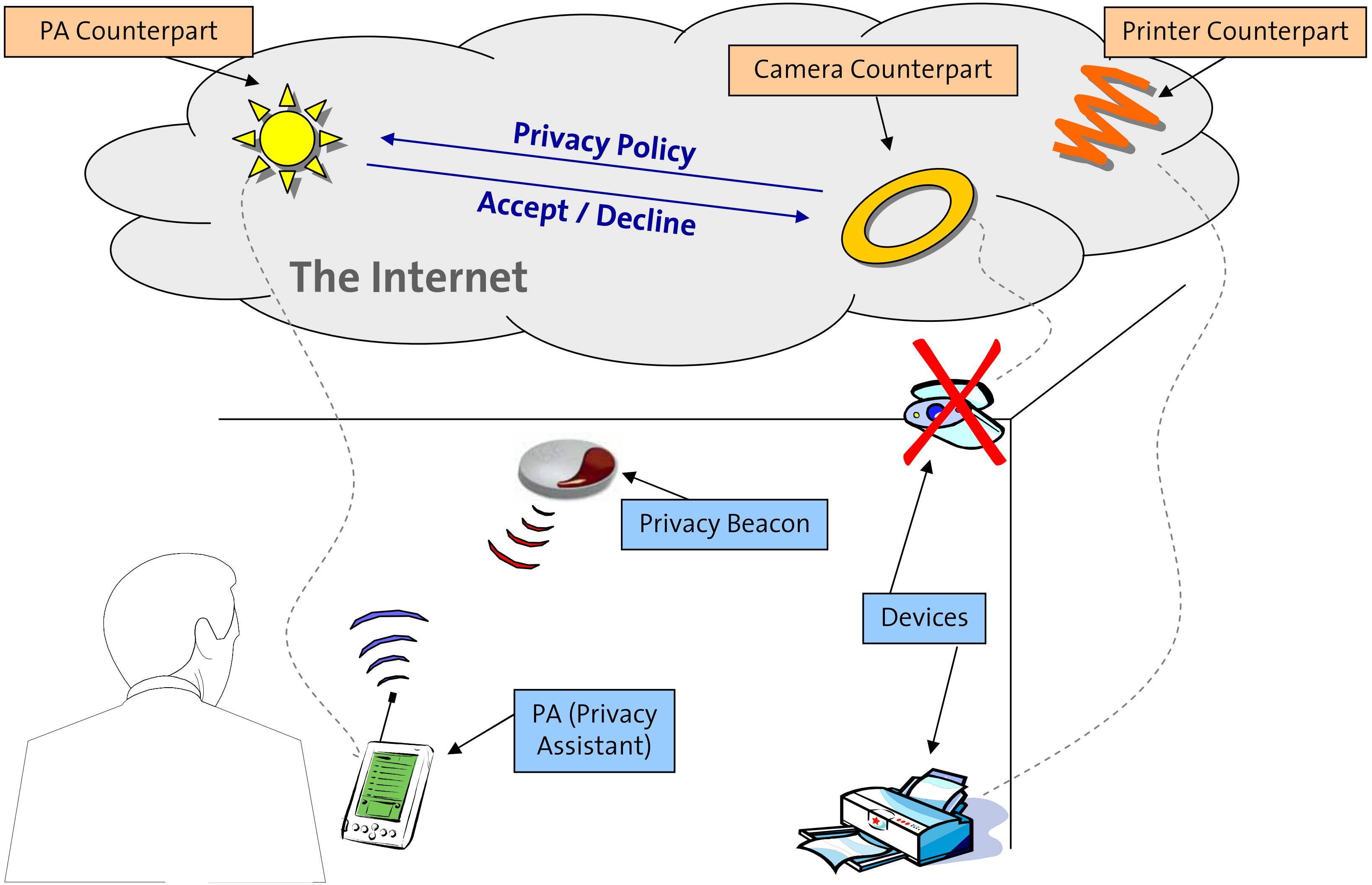


```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
        entity=“TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
<DISPUTES-GROUP>
  <DISPUTES service="http://www.PrivacySeal.org"
    resolution-type="independent"
   description="PrivacySeal, a third-party seal provider"
   image="http://www.PrivacySeal.org/Logo.gif"/>
  </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>
```

The P3P Vocabulary

- Who is collecting data?
- What data is collected?
- For what purpose will data be used?
- Is there an ability to change preferences about (opt-in or opt-out) of some data uses?
- Who are the data recipients (anyone beyond the data collector)?
- To what information does the data collector provide access?
- What is the data retention policy?
- How will disputes about the policy be resolved?
- Where is the human-readable privacy policy?

Privacy Infrastructures



PA Counterpart

Printer Counterpart

Camera Counterpart

Privacy Policy

Accept / Decline

The Internet

Privacy Beacon

Devices

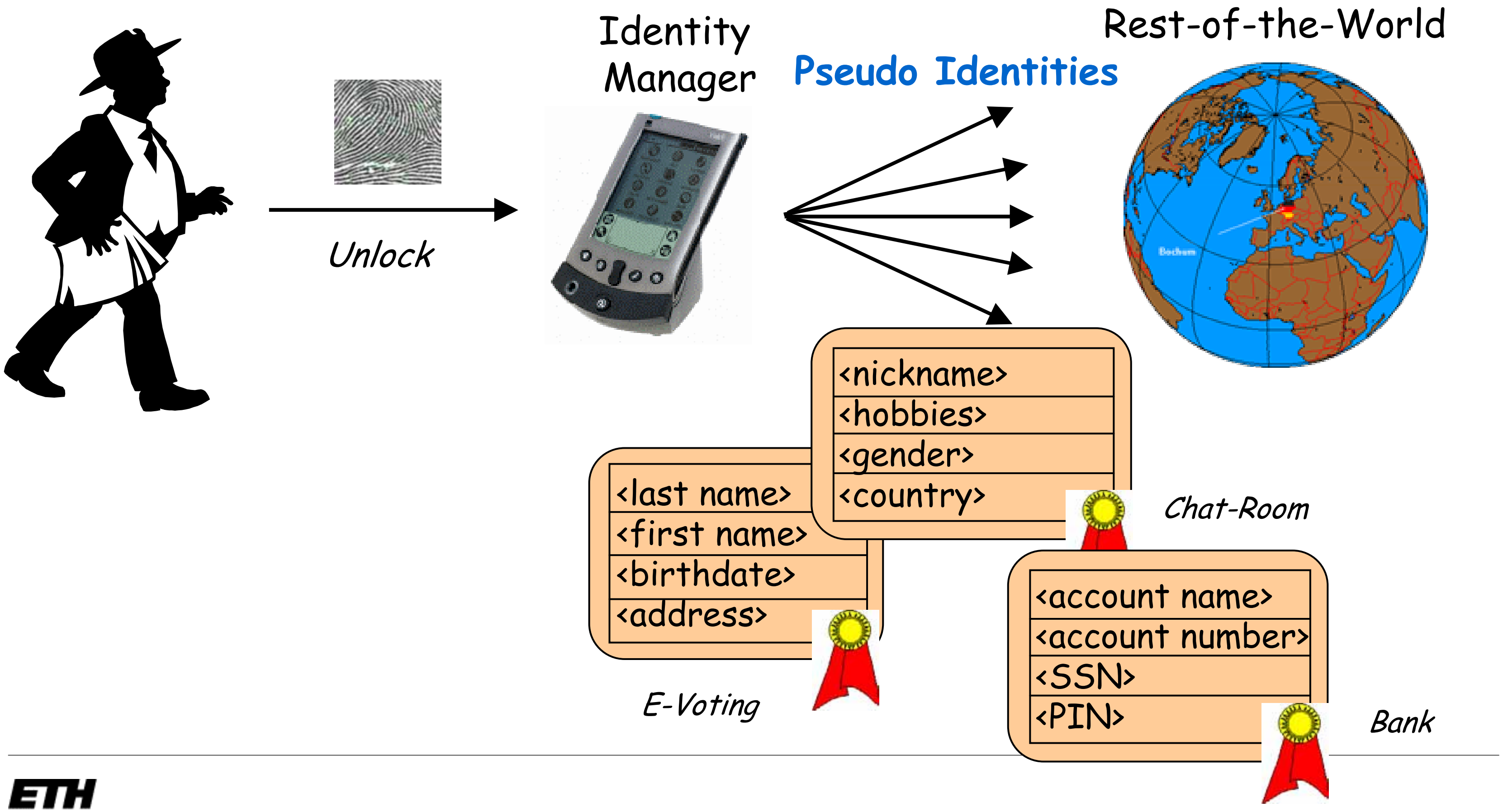
PA (Privacy Assistant)

P3P Issues

- Legal Applicability of XML-Policies?
  - Lawyers Do Not Like Binary Stuff
- Expressability of Personal Preferences?
  - Not All Situations Foreseeable and Definable
- User Proficiency?
  - Can the Layman Configure Sufficiently?
- Who Sets the Defaults?
  - Most Users Will Not Bother to Change Prefs
- Promises, Promises, Promises
  - Who Says That Policies Will Be Followed?
- Do We Need Negotiations?

The Identity Protector

- John Borking, 1996 (Dutch Data Protection Comm.)



Identity Manager

Pseudo Identities

Rest-of-the-World

Unlock

E-Voting

<last name>
<first name>
<birthdate>
<address>

Chat-Room

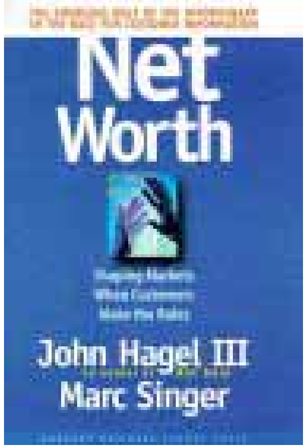
<nickname>
<hobbies>
<gender>
<country>

Bank

<account name>
<account number>
<SSN>
<PIN>

Infomediaries

- Hagel/Singer: „Net Worth“ 1997



- Services and tools that help people manage their online identities
  - Digitalme - http://www.digitalme.com
  - Lumeria - http://www.lumeria.com
  - Privaseek – http://www.privaseek.com

digitalme

Lumeria Inc.

Persona℠

Identity Managers

- History: Open Profiling Standard (Netscape, 97)
  - Inspired P3P, Local Storage, Soon Abandoned
- XNS.ORG (Open Source by *OneName Inc.*)
  - Implements Subset of P3P + Identity Services
- Microsoft Passport (“My Services”)
  - Mounting Criticism Led to Number of Alterations
- Liberty Alliance (Sun, 2001)
  - AmEx, HP, IBM, Nokia, GM, NTT, Philips, Visa, SAP, ...
- IDSec (Open Source, IETF-Draft, 05/2002)

See also: http://weblog.digital-identity.info/

More Identity Managers

- PISA – Privacy Incorporating Software Agent (EU 5th Framework Project)
  - Uses Software Agent Technology
  - Partners: ZeroKnowledge, NRCC, TU Delft, ...
  - http://www.tno.nl/instit/fel/pisa/
- Freiburg University Identity Manager
  - Mobile Applications
  - Incorporate with Location Privacy System
  - http://www.iig.uni-freiburg.de/telematik/atus/

Encryption and Authentication

RESEARCH GROUP FOR

Distributed Systems

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Confidentiality

- Plenty of Options
  - IPSec, SSH, SSL, SET, PGP, WEP (Flawed)…
- Bulk Traffic Encryption Possible
  - But Power Consumption a Factor
- Most Important Question: Who You Are Talking To?
  - Authentication Primary Concern
  - Difficult Due to Lack of Infrastructure!

Making ”Friends”

- Resurrecting Duckling Model (Stajano)
  - Security Principal Imprinted on “Blank” Unit
  - ”Secure Transient Association:” Deassociation Possible After Imprinting
- Interface Challenge
  - Example: Smart-Its

Image: TecO

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Making ”Friends”

- The shaking motion establishes a shared context (i.e., acceleration pattern) that no other devices will have

Image: TecO

Access & Control

RESEARCH GROUP FOR

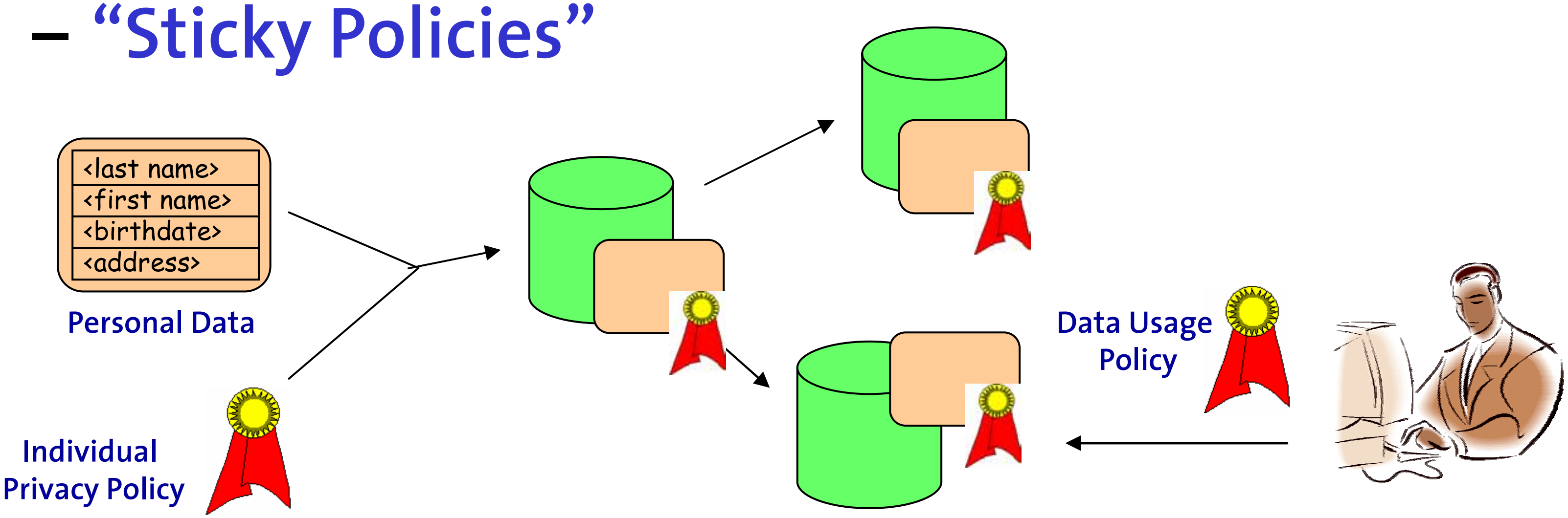
Distributed Systems

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Keeping Your Promises

- Goal: Data Processing in Synch with Data Collection Policies
  - Enterprise-wide PETs
  - Metadata Controls Back-End Processing
  - “Sticky Policies”



Enterprise PETs

- Advantages
  - Allows Individual Policies
  - Simplifies Data Management (Metadata)
  - Provides Accountability (Privacy Audits)
- Players
  - IBM (e.g., pASL, Zurich Research Labs)
  - PricewaterhouseCoopers (Consulting)
  - NCR Teradata (Warehousing Software)

More PET Issues

- Digital Watermarking
  - Protecting Personal Information with Digital Copyright Protection?
- Individual Access
  - Authenticating Users to Edit Personal Data
  - Costs?
- Negotiation
  - How Much Do We Need?
- ...

Solution Space Revisited

- Notice and Disclosure
  - Transparency Tools
- Choice and Consent
  - Anonymity and Pseudonymity Tools
- Security
  - Encryption and Authentication Tools
- Access and Control
  - PETs in the Enterprise
- Recourse
  - Laws and Regulations

Laws & Regulations

RESEARCH GROUP FOR

Distributed Systems

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

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)

Privacy Laws In the US

- Basis
  - 4th Amendment
- Historical Development (Surveillance)
  - Olmstead vs. US
  - Katz vs. US
  - Kyllo vs US
- Modern Privacy Laws (Informational)

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."

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
- Privacy as By-Product 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 Privacy Law (Tort)

- Allows Recovery of Damages (Prosser, 1960)
  - Intrusion
  - Disclosure of Private Facts
  - False Light
  - Appropriation ("Identity Theft")
- Other Torts
  - Intentional Infliction of Emotional Distress
  - Assault
  - Trespass
- But: No Privacy Protection in Public Places
  - Unless "Reasonable Expectation of Privacy"

Source: **Ronald B. Sandler, „Privacy Law in the USA"** (http://www.rbs2.com/privacy.htm)

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)

Data Protection Agencies

- Australia: **`http://www.privacy.gov.au/`**
- Canada: **`http://www.privcom.gc.ca/`**
- France: **`http://www.cnil.fr/`**
- Germany: **`http://www.bfd.bund.de/`**
- Hong Kong: **`http://www.pco.org.hk/`**
- Italy: **`http://www.privacy.it/`**
- Spain: **`http://www.ag-protecciondatos.es/`**
- Switzerland: **`http://www.edsb.ch/`**
- UK: **`http://www.dataprotection.gov.uk/`**

... And many more

Post 9-11 Issues (US)

- Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, 2001
  - online activities, surveillance, money laundering, immigration
- Operation TIPS (Terrorist Information and Prevention System)
  - Begin Scheduled August 2002
  - One Million Volunteers in 10 US Cities to Report “Suspicious Activity” (Goal: 4% of Population)
  - Targets: Letter Carriers, Utility Technicians, ...

citizen corps

Learn more and join today!

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

EU Private Video Surveillance

- Usually Governed By General Data Protection Principles (EU Directive)
  - Justified (by Agreement, Public/Private Interest, Law)
  - Proportional (Sufficient to Achieve Purpose)
    - Footage Selection
    - Storage Duration
  - Clearly Identified (Signs, maybe Contact Info)
  - Secure Storage (If Any)
  - Use Limitation (No Secondary Uses)

For Example of Swiss Law see http://www.edsb.ch/e/doku/merkblaetter/video.htm

Summary & Outlook

RESEARCH GROUP FOR

Distributed Systems

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Summary

- Privacy Enhancing Technologies (PETs)
  - Large Body of Existing Technology (Internet)
  - Many New Challenges in Ubicomp
    - Authentication and Authorization
    - User Interfaces, Configuration for Consent
- Legal Aspects
  - Strong Differences US vs Europe
  - New Legal Developments Re. Data Retention

Privacy in Pervasive Computing

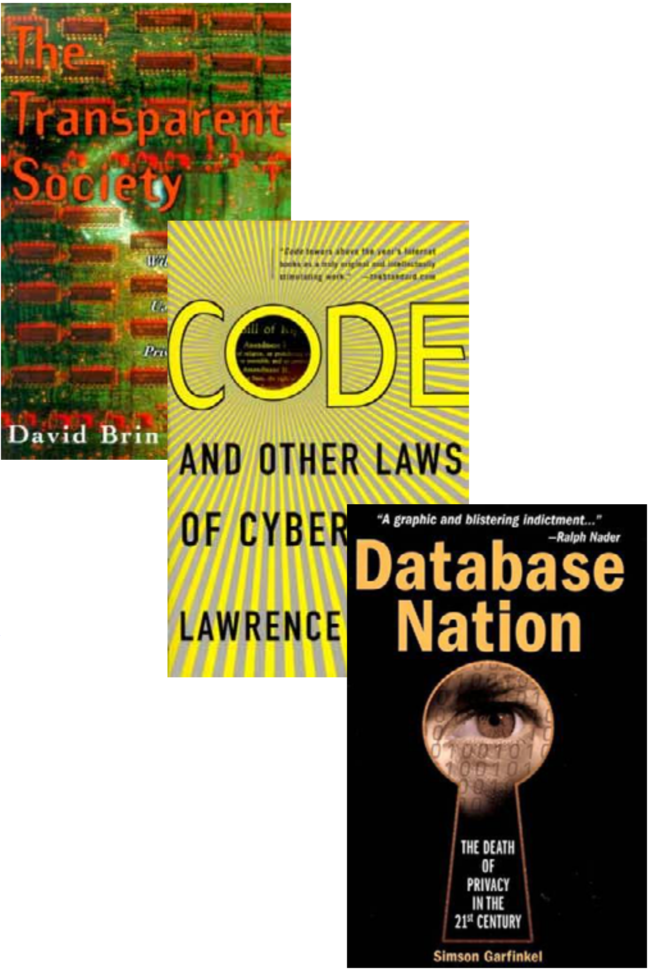
- Privacy is Complex Legal and Social Problem
  - Different Facets, Extend, Borders, Motivations
  - Not Limitless
- Impact on System Design
  - Not “Just” Security!
  - What Data to Collect? How to Use? How to Communicate?

Privacy Web Sites

- http://www.privacyinternational.org
- http://www.privacyfoundation.org
- http://www.privacyexchange.org
- http://www.privacycouncil.com
- http://www.privacyplace.com
- http://www.junkbusters.com
- http://www.privacilla.org
- http://www.statewatch.org
- http://www.privacy.org
- http://www.pandab.org
- http://www.epic.org
- http://www.cdt.org

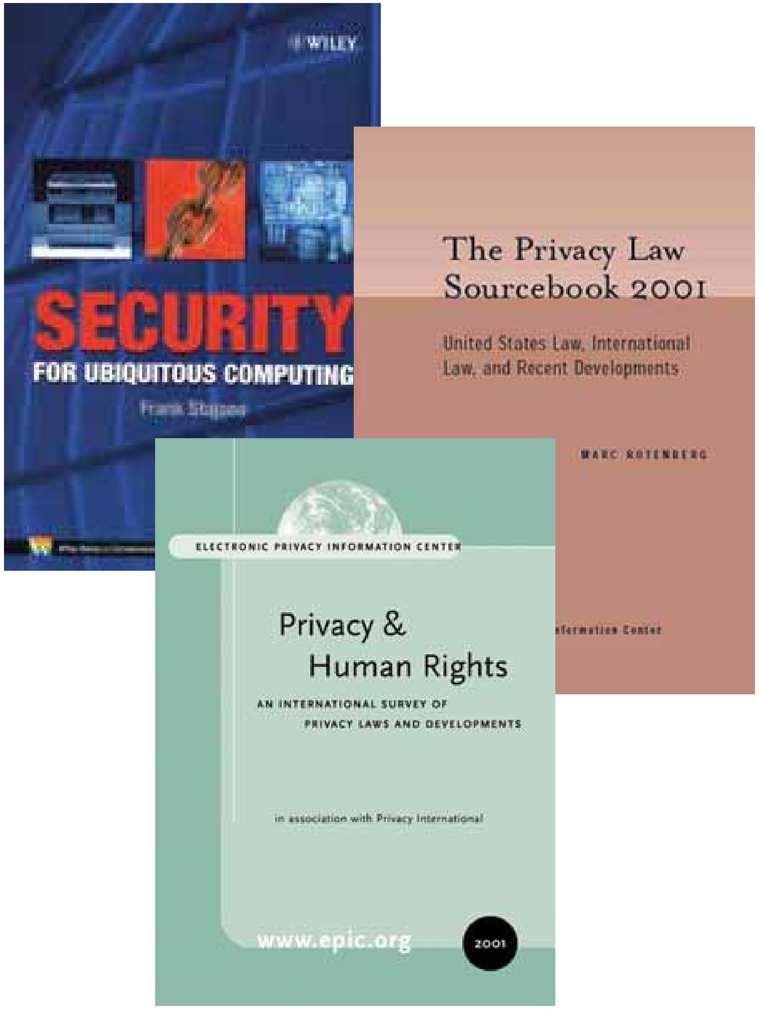
Recommended Reading

- 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


WILEY
SECURITY
FOR UBIQUITOUS COMPUTING
Frank Stajano
The Privacy Law
Sourcebook 2001
United States Law, International
Law, and Recent Developments
MARC ROTENBERG
Information Center
ELECTRONIC PRIVACY INFORMATION CENTER
Privacy &
Human Rights
AN INTERNATIONAL SURVEY OF
PRIVACY LAWS AND DEVELOPMENTS
in association with Privacy International
www.epic.org
2001