

# Privacy, Data Protection Law, and RFID Irreconcilable Differences?

Marc Langheinrich

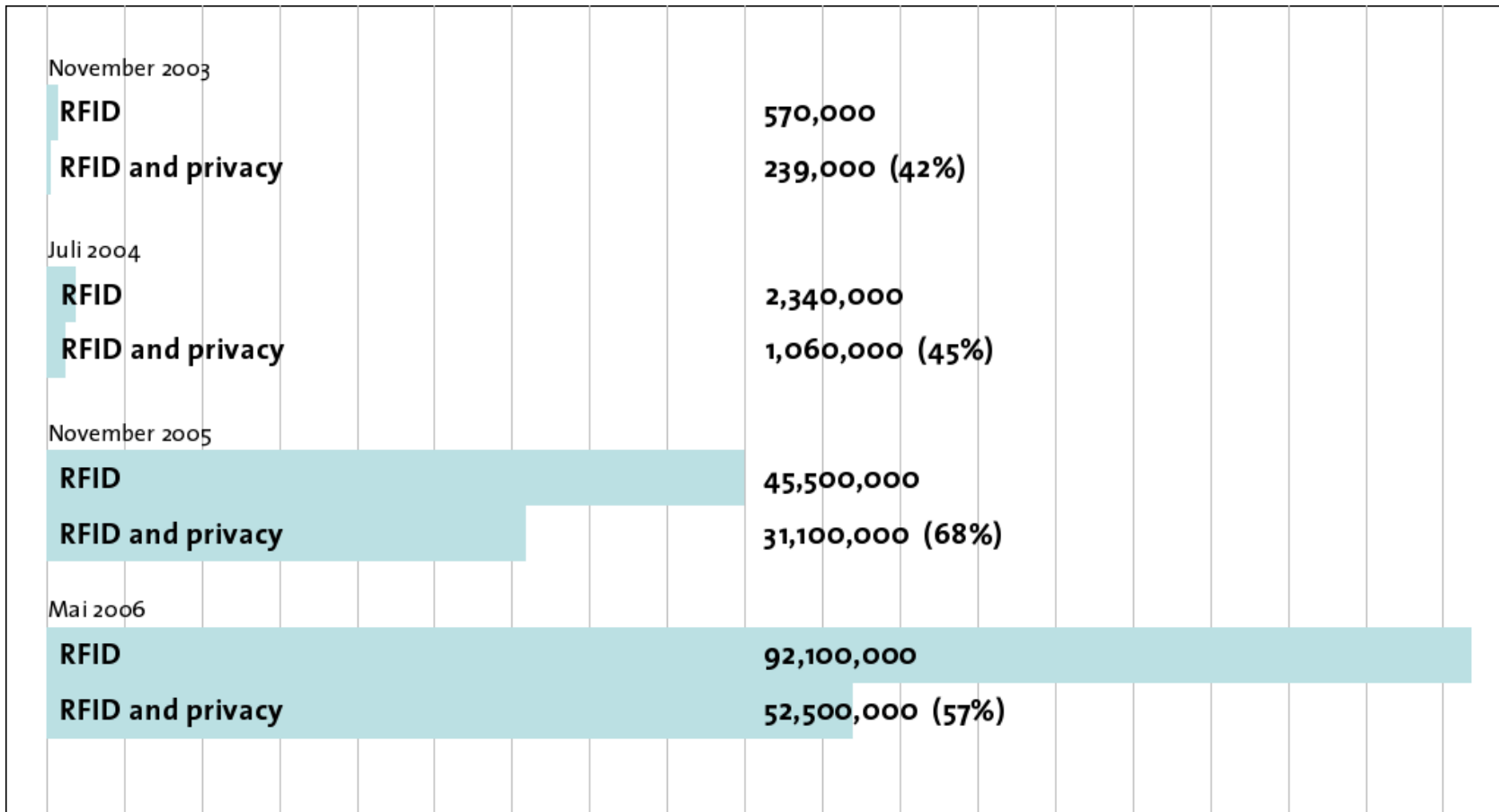
Institute for Pervasive Computing  
ETH Zurich, Switzerland



# Public Concern (as seen on TV)



# Public Concern (as measured by Google)



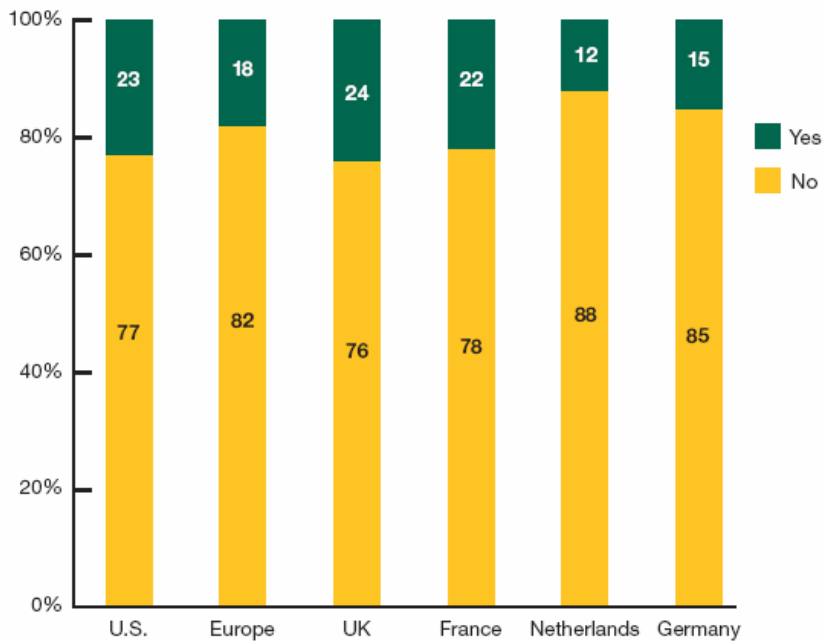
Original numbers by Ravi Pappu, RFID Privacy Workshop @ MIT: November 15, 2003

# Public Concern (as seen by Aml-Experts)

- **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.”
- **Hindrance:** “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”

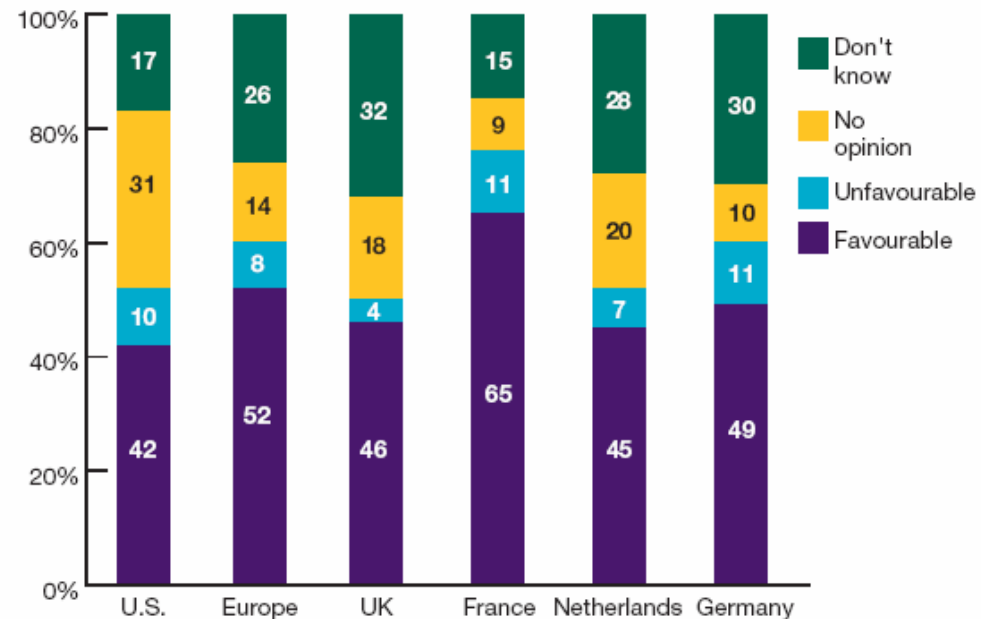
# Public Concern (as measured by Capgemini)

Have You Heard of RFID Technology? (% consumers saying)



Source: Capgemini

What Is Your Perception of RFID Technology? (% consumers saying)



Base: All who have heard of RFID

Source: Capgemini

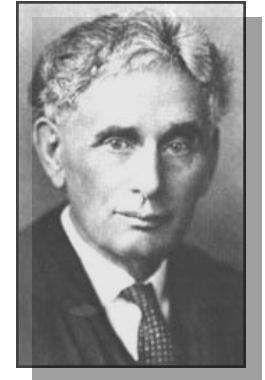
Capgemini: RFID and Consumers – what European Consumers Think About Radio Frequency Identification and the Implications for Business. Survey, **February 2005**. Available from: [www.capgemini.com/news/2005/Capgemini\\_European\\_RFID\\_report.pdf](http://www.capgemini.com/news/2005/Capgemini_European_RFID_report.pdf).

A blue-tinted photograph of a large, classical-style building with a prominent dome and arched windows, likely a part of the ETH Zurich campus. The image is positioned at the top of the slide.

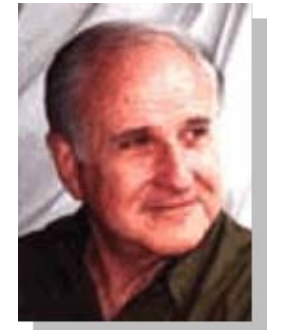
Should **we** be concerned about privacy?

# What is Privacy?

- **„The right to be let alone.“**
  - Louis Brandeis, 1890 (Harvard Law Review)
- **„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 („Privacy And Freedom“, 1967)  
Prof. Emeritus, Columbia University



Louis D. Brandeis, 1856 - 1941



Alan Westin

# Why Privacy?

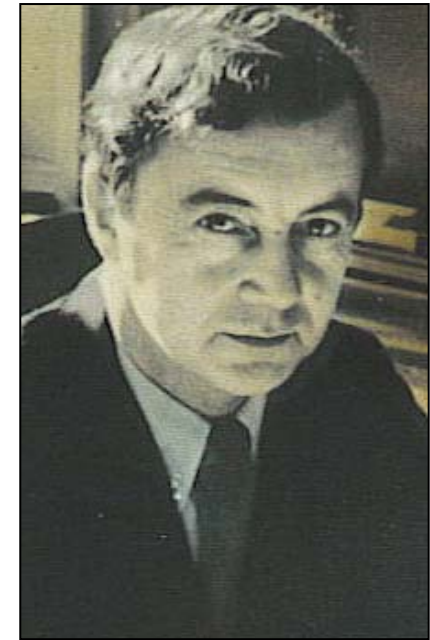
- **Reasons for Privacy**
  - Free from Nuisance



Louis D. Brandeis, 1856 – 1941  
„The right to be let alone“ (1890)

# Why Privacy?

- **Reasons for Privacy**
  - Free from Nuisance
  - Intimacy

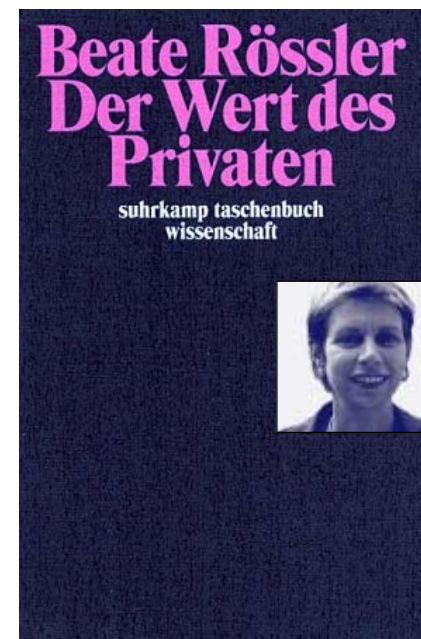


Erving M. Goffman, 1922 – 1982

The Presentation of Self in Everyday Life (1959)

# Why Privacy?

- Reasons for Privacy
  - Free from Nuisance
  - Intimacy
  - Free to Decide for Oneself



Beate Rössler

Protecting the decisional autonomy in one's life (2001)

# Why Privacy?

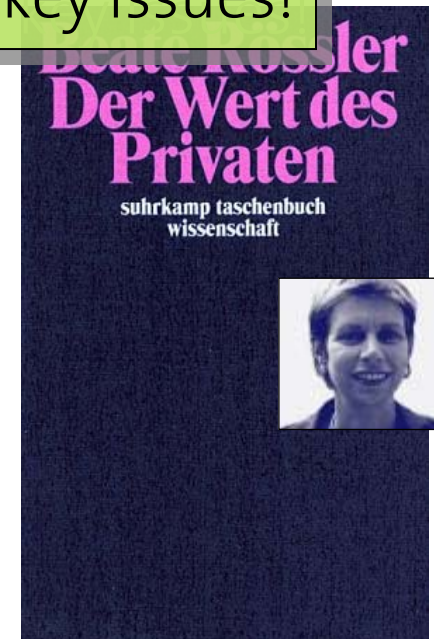
Privacy isn't just about keeping secrets – data **exchange** and **transparency** are key issues!

## ■ Reasons for Privacy

- Free from Nuisance
- Intimacy
- Free to Decide for Oneself

## ■ By Another Name...

- Data Protection
- Informational Self-Determination



Beate Rössler

Protecting the decisional autonomy in one's life (2001)

# Privacy Violations?

- **Violations Due to Crossings of “Privacy” Borders**
  - Prof. Emeritus Gary T. Marx, MIT
- **“Privacy” Borders**
  - Natural Borders
  - Social Borders
  - Spatial/Temporal Borders
  - Ephemeral Borders



RFID-technology makes some of those borders easier to cross

# Privacy Implications of Smart Environments

## ■ Data Collection

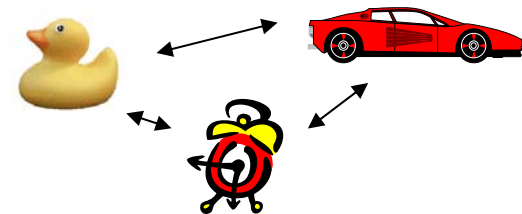
- Scale (everywhere, anytime)
- Manner (inconspicuous, invisible)
- Motivation (unspecified, e.g., context)

## ■ Data Types

- Observational instead of factual data

## ■ Data Access

- “The Internet of Things”



# Should we be concerned about **RFID**?

# Societal Drivers for RFID Acceptance – Collection and Use

- **Higher Efficiency (Cheaper Stuff!)**
  - Rebates! (Loyalty Cards)
  - Targeted Sales (1-1 Marketing)
- **More Convenience**
  - Getting shopping advice (e.g., allergies)
  - Simplified handling (return, repairs, access)
- **Increased Safety**
  - Crime prevention (Ticketing, counterfeiting, CCTV, ...)
  - Homeland security (terrorism, child molesters, ...)



# Example: Loyalty Cards

- **Emnid Survey Germany (03/2002)**
  - 50% have at least one loyalty card
  - 72% welcome such offers
- **70 Million Cards in Circulation (DE, 12/03)**
  - Average rebate: 1.0-0.5%
  - 15% of consumers estimate rebate being 5-10%
- **Minding the Fine Print?**
  - Explicit signature allows detailed data mining
  - Consequences?



# Consumer Loyalty Cards – The Dark Side

- **The Story of Robert Riveras (1998)**
  - Slipped on spilled yoghurt and hurt kneecap. Sued.
  - Consumer card showed high volume licqour purchases
  - Settled out of court
- **Or: Divorce Case**
  - Liking of expensive wines increased alimony payments



# Consumer Loyalty Cards – Legal Implications

- **Arson Near Youth House Niederwangen (Berne)**
  - At scene of crime: Migros-tools
  - Court ordered disclosure of all 133 consumers who bought items on their supermarket card (8/2004)
  - Arsonist not yet found (11/2005)



Aren't there **laws** against this stuff?

# A (Very) Brief History of Privacy Legislation

- **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; ... – 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
- **First Data Protection Law in the World in Hesse**
  - 1970



# Privacy 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)

- 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 (Federal)

- 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
- **Applies to both Public and Private Sector**
  - Data collection illegal, unless consented or authorized
  - Follows OECD Fair Information Principles (1980)

# 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)
- **Six Principles (simplified)**
  1. Openness
  2. Data access and control
  3. Data security
  4. Collection Limitation
  5. Data subject’s consent
  6. Use Limitation
- **Core Principles of Most Modern Privacy Laws**
  - Implication: Technical solutions must support FIP

# Data Protection Law and RFID

25th Intl. Conf. of Data Protection and Privacy Commissioners, 11/03

- All basic principles of data protection law have to be observed when designing, implementing and using RFID technology. In particular
  - any controller – before introducing RFID tags linked to personal information or leading to customer profiles – should **first consider alternatives** which achieve the same goal without collecting personal information or profiling customers; **(Collection Limitation)**
  - if the controller can show that personal data are indispensable, they must be collected in an **open and transparent** way ; **(Openness, Consent)**
  - personal data may only be used for the **specific purpose** for which they were first collected and only retained for as long as is necessary to achieve (or carry out) this purpose, and **(Use Limitation)**
  - whenever RFID tags are in the possession of individuals, they should have the possibility to **delete** data and to **disable** or **destroy** the tags. **(Access and Control)**


A blue-tinted photograph of a large, classical-style building with a prominent dome and arched windows, likely a part of the ETH Zurich campus. The image is positioned at the top of the slide.

Let's just build **privacy-law compliant** RFID-Systems

# 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)
- **Six Principles (simplified)**

|   |  |
|---|--|
| <ol style="list-style-type: none"><li>1. Openness</li><li>2. Data access and control</li><li>3. Data security </li></ol> | <ol style="list-style-type: none"><li>4. Collection Limitation</li><li>5. Data subject's consent</li><li>6. Use Limitation</li></ol> |
|---|--|
- **Core Principles of Most Modern Privacy Laws**
  - Implication: Technical solutions must support FIP

# Openness with RFID



- **No Hidden Data Collection!**
  - Legal requirement in many countries
- **Established Means: Privacy Policies**
  - Who, what, why, how long, etc. ...
- **How to Publish RFID Policies?**
  - Is a poster enough? A paragraph of fine print?
- **Too Many Transactions?**
  - Countless announcements an annoyance
  - Notices “get in the way” – Background vs Foreground

# Openness with RFID



- **No Hidden Data Collection!**
  - Legal requirement in many countries
- **Established Means: Privacy Policies**
  - Who, what, why, how long, etc. ...
- **How to Publish RFID Policies?**
  - Is a poster enough? A paragraph of fine print?
- **Too Many Transactions?**

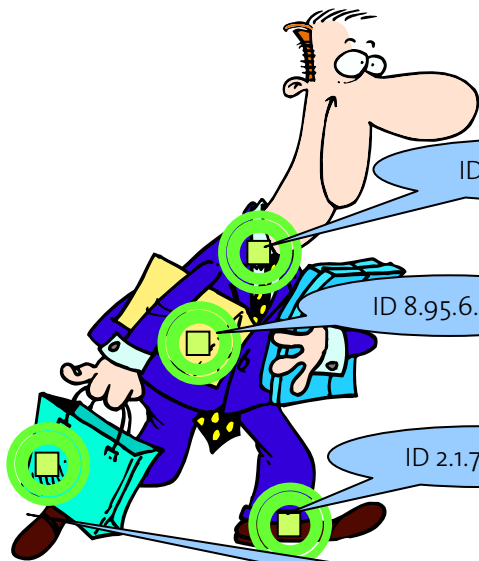
Countless announcements and approvals  
Noises "going by" Background vs Foreground

How many people read SSL certificate warnings?  
Cookie warnings? Do you want to proceed, yes or no?

# Today's RFID Systems

**Privacy Policy**  
The information we learn from customers helps us personalize and continually improve your shopping experience.

All tags respond, please!



ID 1.82.221.3

ID 8.95.6.086

ID 2.1.741.850

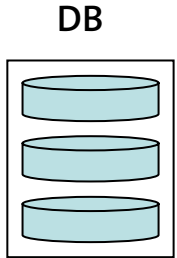
ID 9.23.114.63

ID 9.834.12.30

ID 9.834.12.31

ID 9.834.59.01

ID 8.75.03.914



- ID 1.82.221.3
- ID 8.95.6.086
- ID 2.1.741.850
- ID 9.834.12.30
- ID 9.834.12.31
- ...
- ...
- ...

Clipart Courtesy of Ari Juels

Slide Courtesy of Roland Schneider

# Example: Openness in RFID Protocols

| Protocol extension | Init round all | SUID flag | Round size | CRC-5  | RPID    | Purpose | Collection type | CRC-16  |
|--------------------|----------------|-----------|------------|--------|---------|---------|-----------------|---------|
| 1 bit              | 6 bits         | 1 bit     | 3 bits     | 5 bits | 96 bits | 16 bits | 2 bits          | 16 bits |

- **Init\_Round Command in ISO 18000 Part 6**
  - Defines start of reading cycle (Aloha-based anti-collision)
  - Defines Anti-collision protocol parameters
- **New: 130 Bits „Privacy-Header“ Extension**

# Openness using the ReaderPolicyID

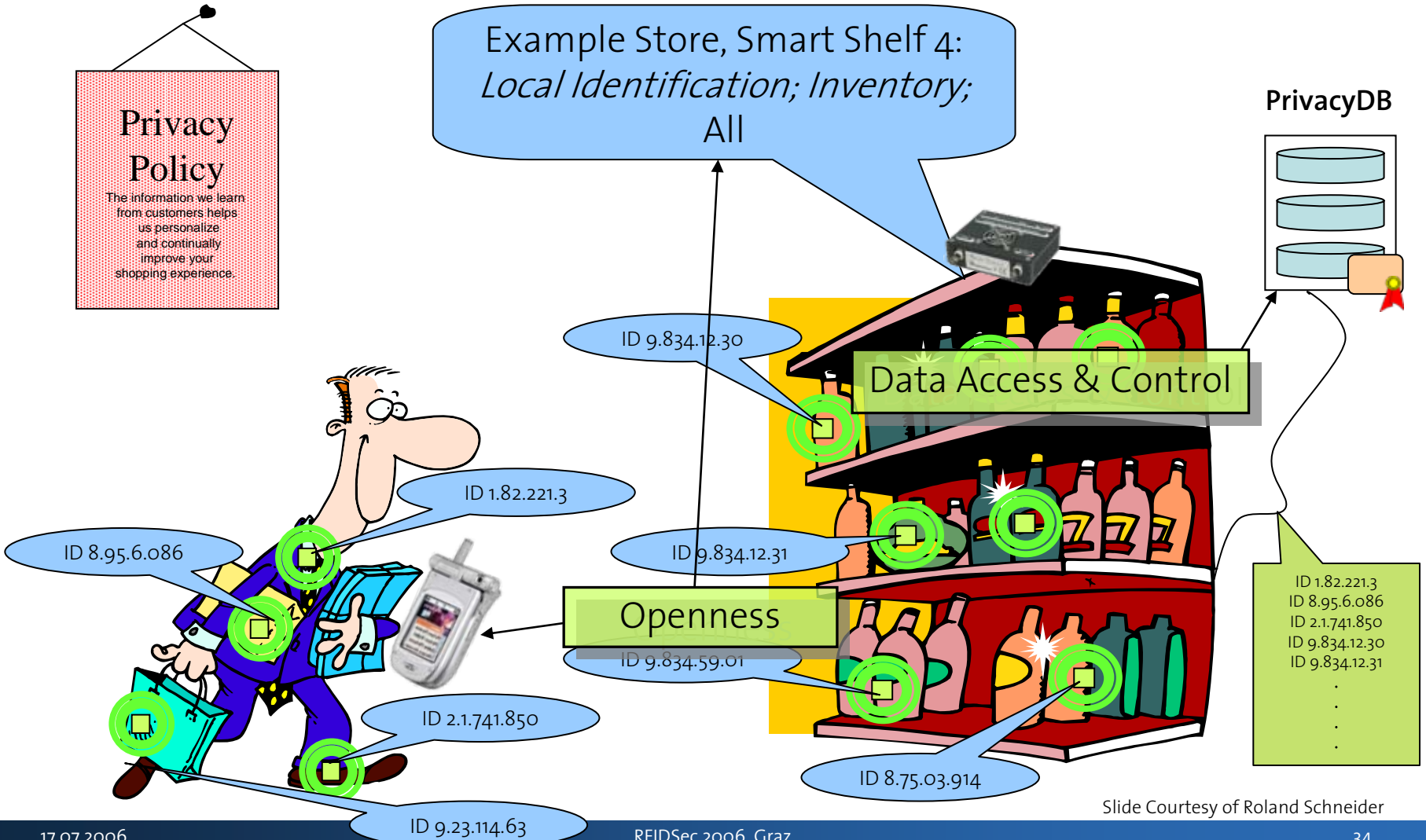
| Protocol extension | Init round all | SUID flag | Round size | CRC-5  | RPID    | Purpose | Collection type | CRC-16  |
|--------------------|----------------|-----------|------------|--------|---------|---------|-----------------|---------|
| 1 bit              | 6 bits         | 1 bit     | 3 bits     | 5 bits | 96 bits | 16 bits | 2 bits          | 16 bits |

| Header | Data Collector | Policy  | Reader  |
|--------|----------------|---------|---------|
| 8 bits | 28 bit         | 24 bits | 36 bits |

5F.4A886EC.8EC947.24A68E4F6

- **Each Read Request can be Associated with Data Collector**
  - Data collector, reader, and privacy policy identifiable
  - Format follows EPC standard (facilitates implementation)

# Today's RFID Systems (with „Watchdog“-Tag)



Clipart Courtesy of Ari Juels

Slide Courtesy of Roland Schneider

# Access & Control with RFID



- **Identifiable Data Must be Accessible**
  - Users can review, change, sometimes delete
- **Collectors Must be Accountable**
  - Privacy-aware storage technology
- **When Does RFID Data Become Identifiable?**
  - Even product-level IDs identify people (constellations)
- **Who to Ask? How to Verify? How to Display?**
  - Who was reading me when? Is this really my trace?



# Consent with RFID



- **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 “On The Fly”?**
  - Pen&Paper? Automating consent (is this legal)?
  - The mobile phone as a „Vindictive Sentinel“ (Sanja)?
- **Consenting to What?**
  - Do I understand the implications?

# Consent with RFID



- P
- T
- H

## ■ Consenting to What?

- Do I understand the implications?

A blue-tinted photograph of a large, classical-style building with a prominent dome, likely a part of the ETH Zurich campus, set against a light sky.

**Well, RFID won't get accepted otherwise...**

# Societal Drivers for RFID Acceptance – Collection and Use

## ■ Higher Efficiency (Cheaper Stuff!)

- 70 Million Cards! 72% Like it!



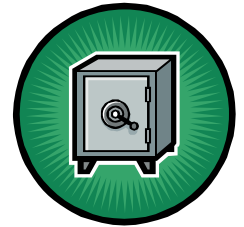
## ■ More Convenience

- Automated Toll-Roads! Skipasses! Remote Car-Keys!

## ■ Increased Safety

- Survey DE (05/06): 80+% like more CCTV surveillance
- Survey US (08/04): 70+% accept air travel surveillance

# “Don’t-get-in-my-way” Privacy



- **No One *Wants* to (Explicitly) Manage their Privacy!**
  - Anonymizer (Zero-Knowledge.com)? Infomediaries?
  - No one wants to pay extra, either (does privacy pay?)
- **Challenge: When to Share What With Whom?**
  - Simple command (touch, shake, press) for transfers
  - System knows what to share (not too much!)
- **Challenge: Designing for Mistakes**
  - Collected data should be simple to check
  - False data should be simple to fix, or to get help

# „Pervasive Privacy“ (Prof. Rossnagel, Kassel Univ.)

## Anytime, Anywhere, Automatic, Pro-Active

„The most profound technologies are those that **disappear**. They weave themselves into the fabric of **everyday life** until they are indistinguishable from it.“



Mark Weiser (1952 – 1999)

- Let Technology **Disappear into** Laws, Social Habits
  - Not through interfaces, but operate in the background
  - Can we make privacy laws „automatable“?
  - Can we know/predict what the user wants (no AI, pls)?
  - What do we need to „fix“ disclosure problems?

# Privacy Affordances

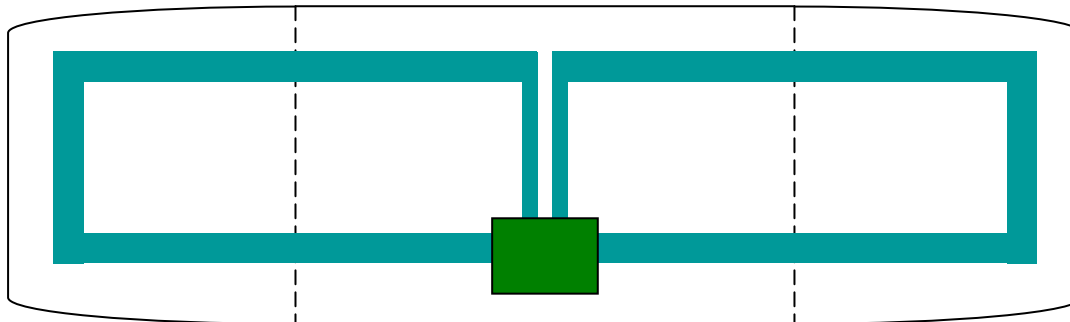
”Physics is our best friend” (Sanjay Sarma, RFIDSec’06)



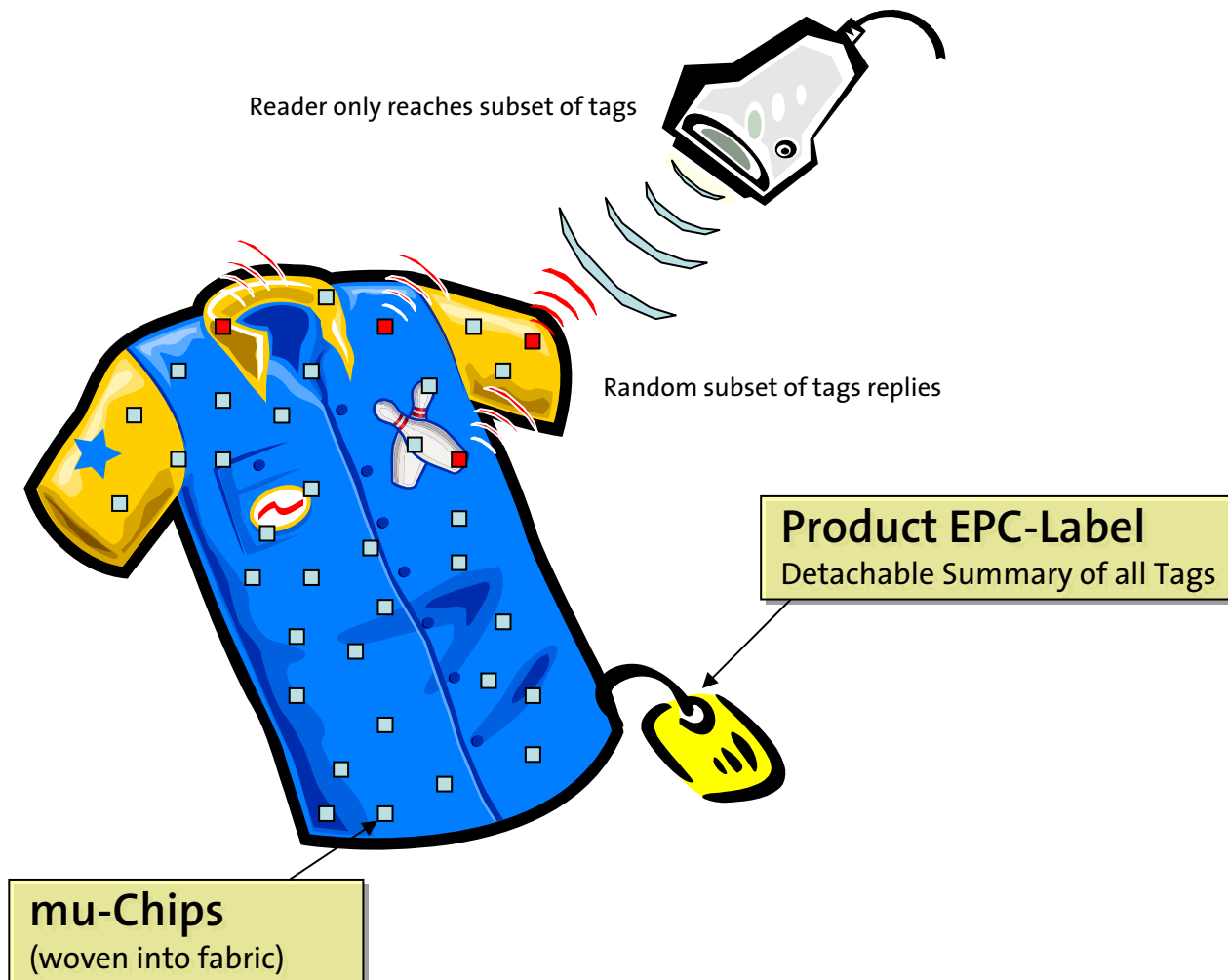
- **Privacy within Marx’s “Personal Borders”**
  - Natural borders: alone == privacy
  - Social borders: strangers don’t know me
- **“Proximity Affordance”**
  - No remote reading – access requires closeness
- **“Acquaintance Affordance”**
  - No rush-jobs – tag reading takes time, effort
- **„Locality Affordance“**
  - Collected data bound to place/owner/reader

# Example: Proximity Affordance

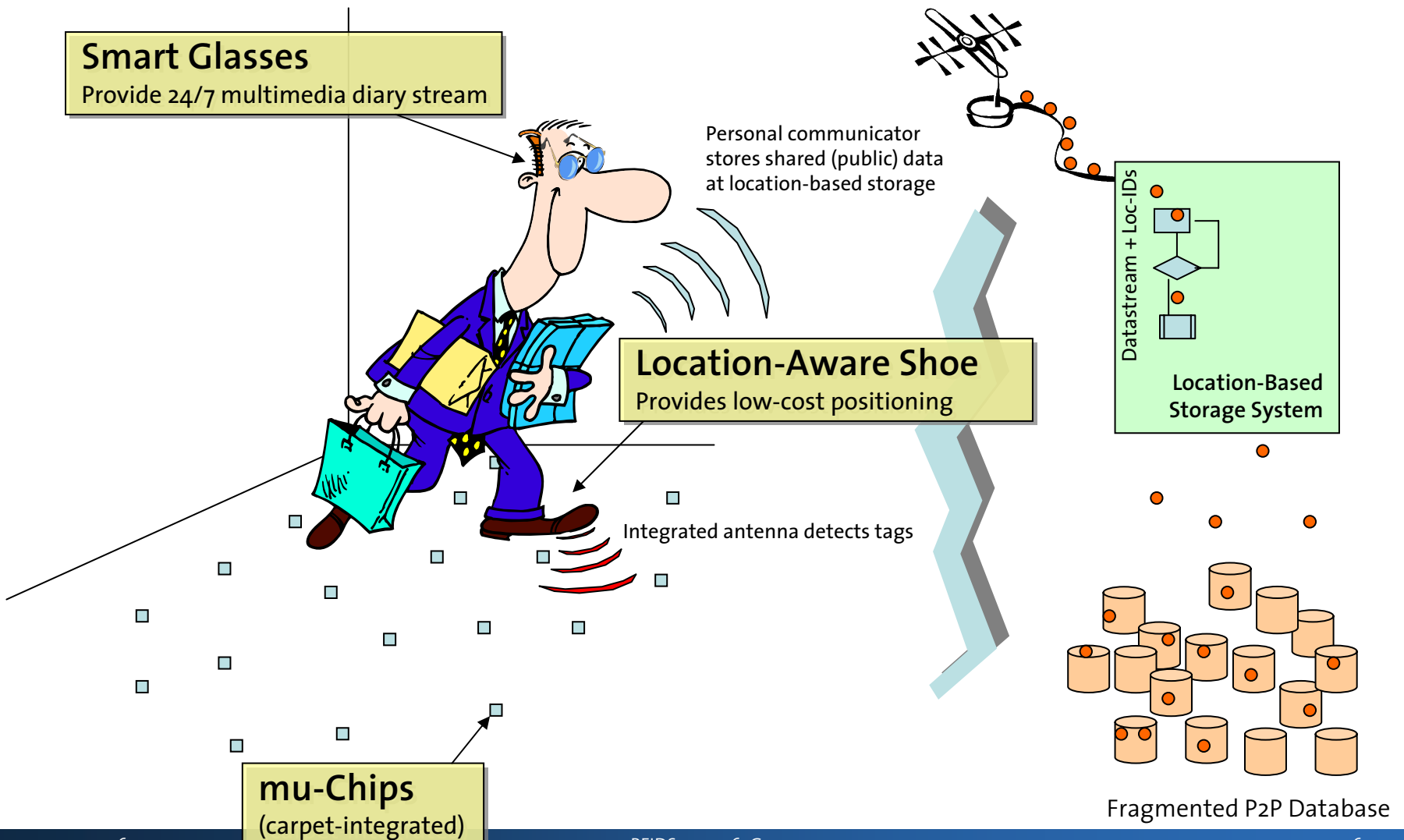
- **Clipped Tags (IBM Patent Pending)**
  - Manually disable (and inspect) tags after purchase
  - Still readable from very close distance



# Example: Acquaintance Affordances



# Example: Locality Affordance



Clipart Courtesy of Ari Juels

# Privacy Affordances

”Physics is our best friend” (Sanjay Sarma, RFIDSec’06)



- **Privacy within Marx’s “Personal Borders”**
  - Natural borders: alone == privacy
  - Social borders: strangers don’t know me
- **“Proximity Affordance”**
  - No remote reading – access requires closeness
- **“Acquaintance Affordance”**
  - No rush-jobs – tag reading takes time, effort
- **„Locality Affordance“**
  - Collected data bound to place/owner/reader

# Smart Environments Require Answers...

- **How Simple Do We Want Our Lives To Be?**
  - Smart systems need to know a lot about us
- **How Far Do We Want To Commercialize Our Life?**
  - Detailed profiles save money, add convenience
- **How Safe Do We Think We Can Make Our Life?**
  - Can total surveillance guarantee total safety?
- **Who Is To Give Those Answers, Sets the Rules?**

# (Some) Societal Implications of Unregulated Smart Environments

- “Decriminalizing Collection” (Gus Hosein, 2006)
  - Hosein observes shift in retention policy in UK courts
  - “*Collection* not privacy invasive, only *use*”

# Evolution of UK Policy

- Collected from those arrested and charged for sexual offences, unless acquitted.
- Collected from those arrested and charged for serious offences, unless acquitted.
- Collected from those arrested and charged for serious offences.
- Collected from those arrested for serious offences.
- Collected from those arrested for offences.

Gus Hosein: Combating Criminality in Aml, SWAMI-Workshop, Brussels, 05/2006

# (Some) Societal Implications of Unregulated Smart Environments

- **“Decriminalizing Collection” (Gus Hosein, 2006)**
  - Hosein observes shift in retention policy in UK courts
  - *“Collection not privacy invasive, only use”*
- **Techno Fallacies (G. Marx)**
  - *“Data is fast... but fallible”* (Sanjay Sarma, RFIDSec’06)
  - If it’s in the computer, it must be right!

# Sleepless in Seattle

1993



- Jessica: I am telling them you're twelve so you can fly unaccompanied and the stewardess won't carry you around and stuff like that.
- Jonah Baldwin: Are you crazy! Who'd believe I'm twelve?
- Jessica: **If it's in the computer, they believe anything.**
- Jonah Baldwin: Are you sure?
- Jessica: Do you want me to say that you are really really short for your age and they shouldn't say anything because it would hurt your feelings.
- Jonah Baldwin: Yea, that's a great idea!

# (Some) Societal Implications of Unregulated Smart Environments

- **“Decriminalizing Collection” (Gus Hosein, 2006)**
  - Hosein observes shift in retention policy in UK courts
  - *“Collection not privacy invasive, only use”*
- **Techno Fallacies (G. Marx)**
  - *“Data is fast... but fallible”* (Sanjay Sarma, RFIDSec’06)
  - If it’s in the computer, it must be right!
- **A Presumption of Guilt?**
  - If you have done nothing wrong, you got nothing to hide!

# Which Future Should We Want?

## Welche Zukunft sollen wir wollen?

(A. Roßnagel 1993)



# Which Future Should We Want?

## Welche Zukunft sollen wir wollen?

(A. Roßnagel 1993)



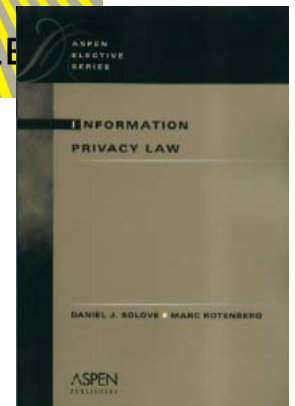
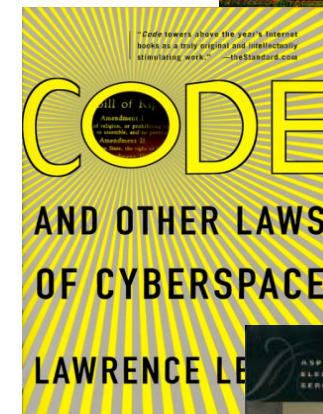
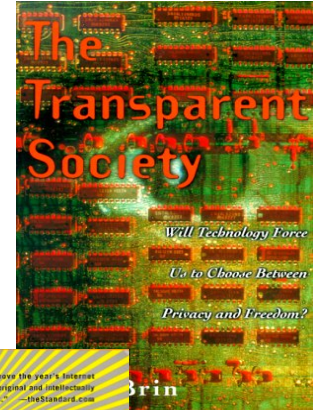
The wireless century will bring **an end to many crimes**. It will be a century of morality, since it is known that morality and fear are one and the same.

(Robert Sloss, "The World in 100 Years", 1910)



# Privacy Reads

- David Brin: **The Transparent Society**. Perseus Publishing, 1999
- Lawrence Lessig: **Code and Other Laws of Cyberspace**. Basic Books, 2000
- Daniel Solove and Marc Rotenberg: **Information Privacy Law**. Aspen Publ. 2003





May 13-16

# Pervasive 2007

The 5<sup>th</sup> International Conference on Pervasive Computing

Toronto, Ontario, Canada

- New **technologies** and **devices** for pervasive computing
- New **applications** of pervasive computing technologies
- New **interfaces** and **modes of interactions** between people and pervasive computing devices, apps or environments
- New **tools, infrastructures, architectures** and techniques for designing, implementing & deploying ubicomp apps
- **Evaluations** and evaluation methods, for assessing the impact of pervasive computing devices, applications or environments
- **Privacy, security, trust & social issues** and implications of pervasive computing



May 13-16

# Pervasive 2007

The 5<sup>th</sup> International Conference on Pervasive Computing

Toronto, Ontario, Canada

**October 13, 2006**

Deadline for Technical Paper submissions

**October 27, 2006**

Deadline for Workshop Proposals

**January 26, 2007**

Deadline for Late Breaking Results, Demos, Videos, Workshop Papers

**May 13-16, 2007**

[www.pervasive07.org](http://www.pervasive07.org)