

# E-Privacy – Privacy in the Electronic Society

---



Jan Camenisch  
Günter Karjoth

IBM Zurich Research Laboratory  
Rüschlikon

Spring term 2009

# Tentative Schedule

---

- Introduction
- Environment
  - Laws & Regulations
  - Privacy Seals
  - Privacy Policy Languages
- Applications
  - Privacy in Databases
  - Ubiquitous Computing (RFID)
- Foundations
  - Identity and Trust Management
  - Anonymous Credentials
  - Encryption, verifiable encryption, anonymous communication
  
- Guest speaker(s): Tbd.

# What is privacy ?

*The right of individuals to determine for themselves when, how and to what extent information about them is communicated to others. [Alan Westin, 1967]*

*Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf „**informationelle Selbstbestimmung**“ sind nur im überwiegenden Allgemeininteresse zulässig. [Volkszählungsurteil des Deutschen Bundesverfassungsgerichts, 1983]*

## *Internationally agreed privacy principles*

- No covert / secret collections of personal information*
- Informed consent to purpose prior to collection*
- Use, retention only according to agreed purpose*
- Individual must get access to own data, can correct/comment own data*

*LDSG Hessen (1970)  
US Fair Information Practices (1973)  
OECD Guidelines (1980)  
EU Privacy Directive (1995) ...*

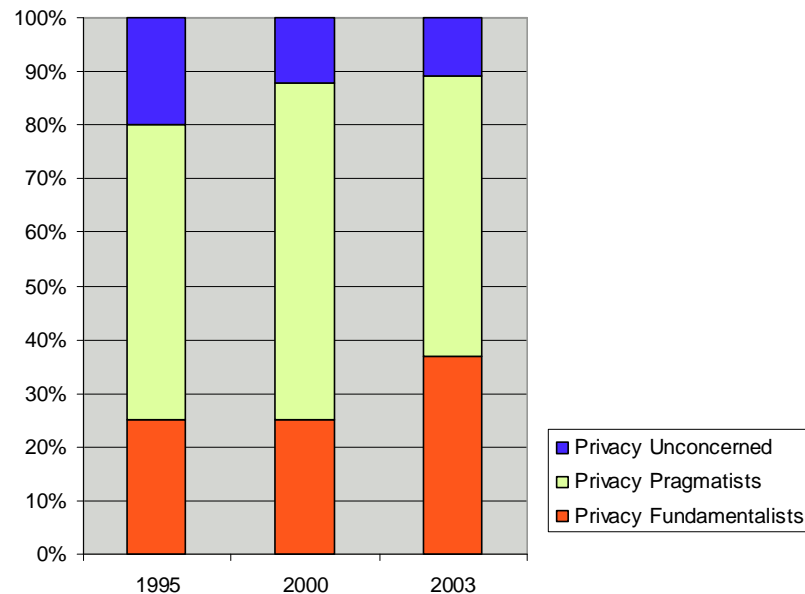
# Do you care about privacy ?

---

- Elektronischer Auto-index
  - <http://www.autoindex.zh.ch/>
    - 800'000 entries
  
- Datenschutzbeauftragter Kanton Zürich
  - <http://www.datenschutz.ch/home.php>

# Do people care about their privacy? – YES!

---



Representative survey among US citizens [Alan Westin, 2003]

- Only 6% consider sharing personal data worth the loss of privacy
- No party gets trust of 5 on 1-7 scale for data like address and credit card info
- More people than ever are concerned about their privacy [Harris 2003]
- Similar to other fundamental rights
- Consumers have clear preferences [Harris 2002]
  - Security procedures [90%], access control [84%], enforcement [>80% ]
  - Assurance of real privacy practices (i.e., not just promises) [91%]

# What is (your) identity ?

---

OSCON 2005 Keynote – identity 2.0

Dick Hardt | Founder & CEO, Sxip identity

[http://identity20.com/media/OSCON2005/oscon\\_videos/oscon\\_lg.html](http://identity20.com/media/OSCON2005/oscon_videos/oscon_lg.html)

# The Information Explosion Continues... (Actually, it's accelerating)

---

## Technology Trends

### COMPUTING:

- Chips/\$ 10x in 5 years
- Computing power/\$ 10x in 4 years

### STORAGE:

- Storage/\$ 10x in 6 years

### COMMUNICATIONS:

- Backbone 100x in 5 years
- Local loop 100x in next 5 years

# Total Amount of Data Connected to The Internet

---

2001	1 petabyte	( $10^{15}$ bytes)
2006	1 exabyte	( $10^{18}$ bytes)
2010	1 zettabyte	( $10^{21}$ bytes)

The result of:

- More people spending
- More time using
- More data-rich applications
- More replication and caching of data

# Much More to Come...

---

The Internet Revolution is <5% complete

- Number of users
- Number of devices
- Speed/bandwidth
- Amount of content
- Number of applications

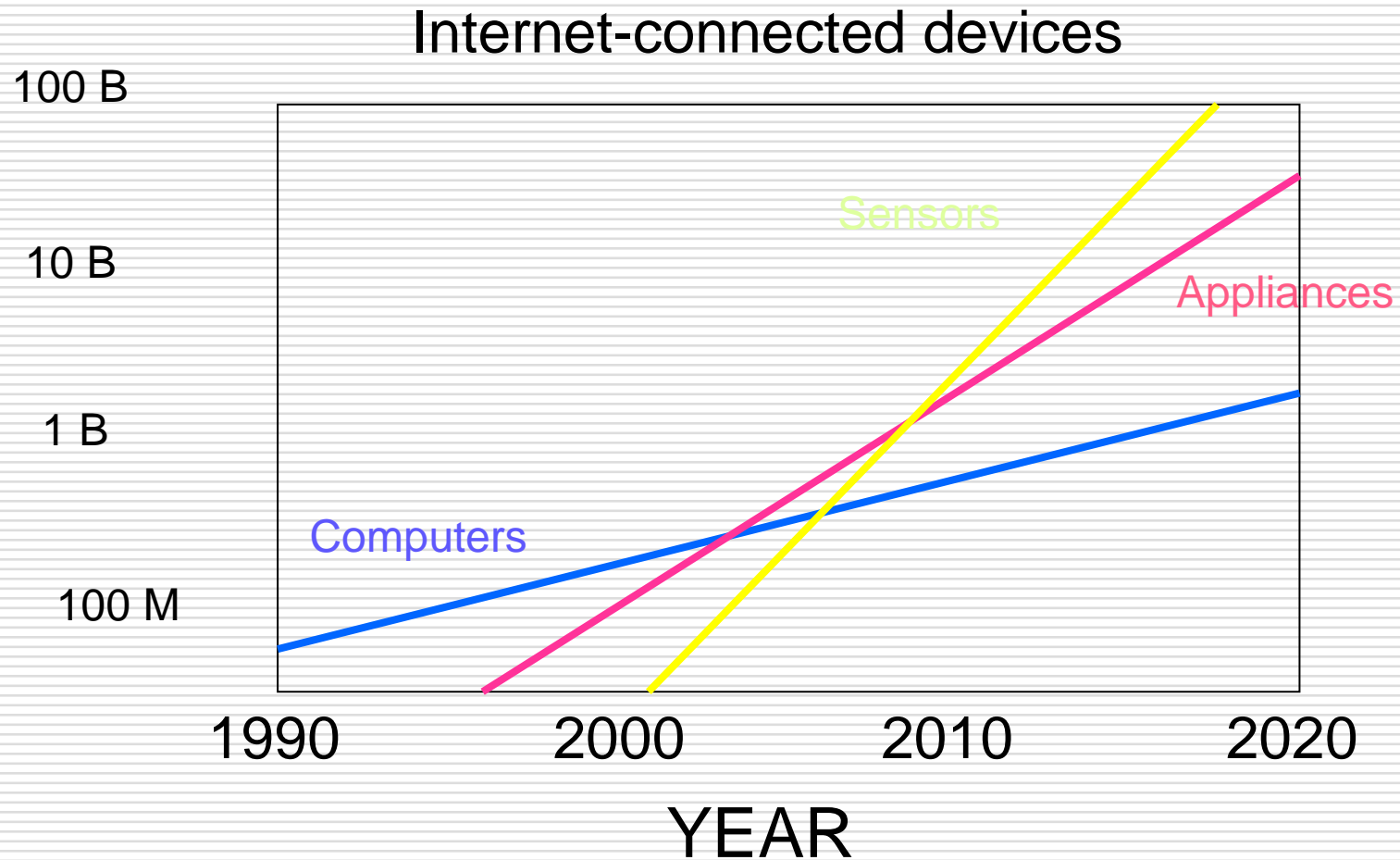
# Data, Data Everywhere...

---

- ❑ Video surveillance
- ❑ E-commerce
- ❑ Location-dependent services
- ❑ Customized video on-demand
- ❑ Video-conferencing
- ❑ Networked devices
- ❑ Embedded sensors
- ❑ Data mining

# Sensors Will Predominate...

---



Harriet Pearson  
Privacy and Security in an On Demand World

# The Data Can Be Combined And Analyzed

---

Data mining and data matching can give governments and businesses powerful, useful, and sometimes disturbing new capabilities:

- Total Information Awareness
- CAPPs II
- New digital video surveillance systems
- Identity theft detection

# Fiction or reality ?

---



Loading....

<http://www.aclu.org/pizza>

# You are what you say

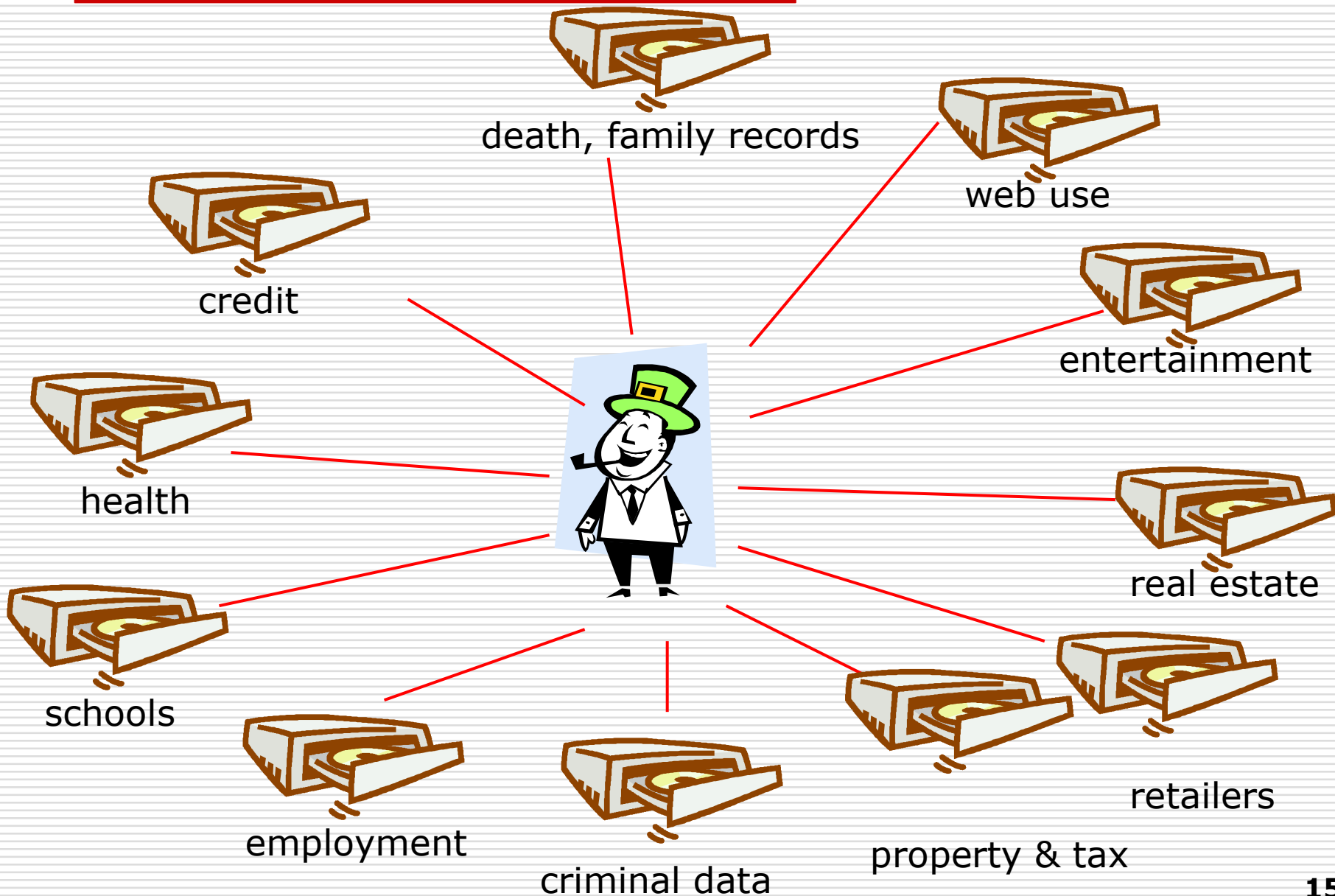
---

## Privacy risks of public mentions

- Wrote a blog
  - Published some pictures on Flickr
  - Posted a movie on YouTube
  - ...
- 
- People are judged by their preferences

# Sources of data on individuals

---



# Trends in Data Collection Behaviors

---

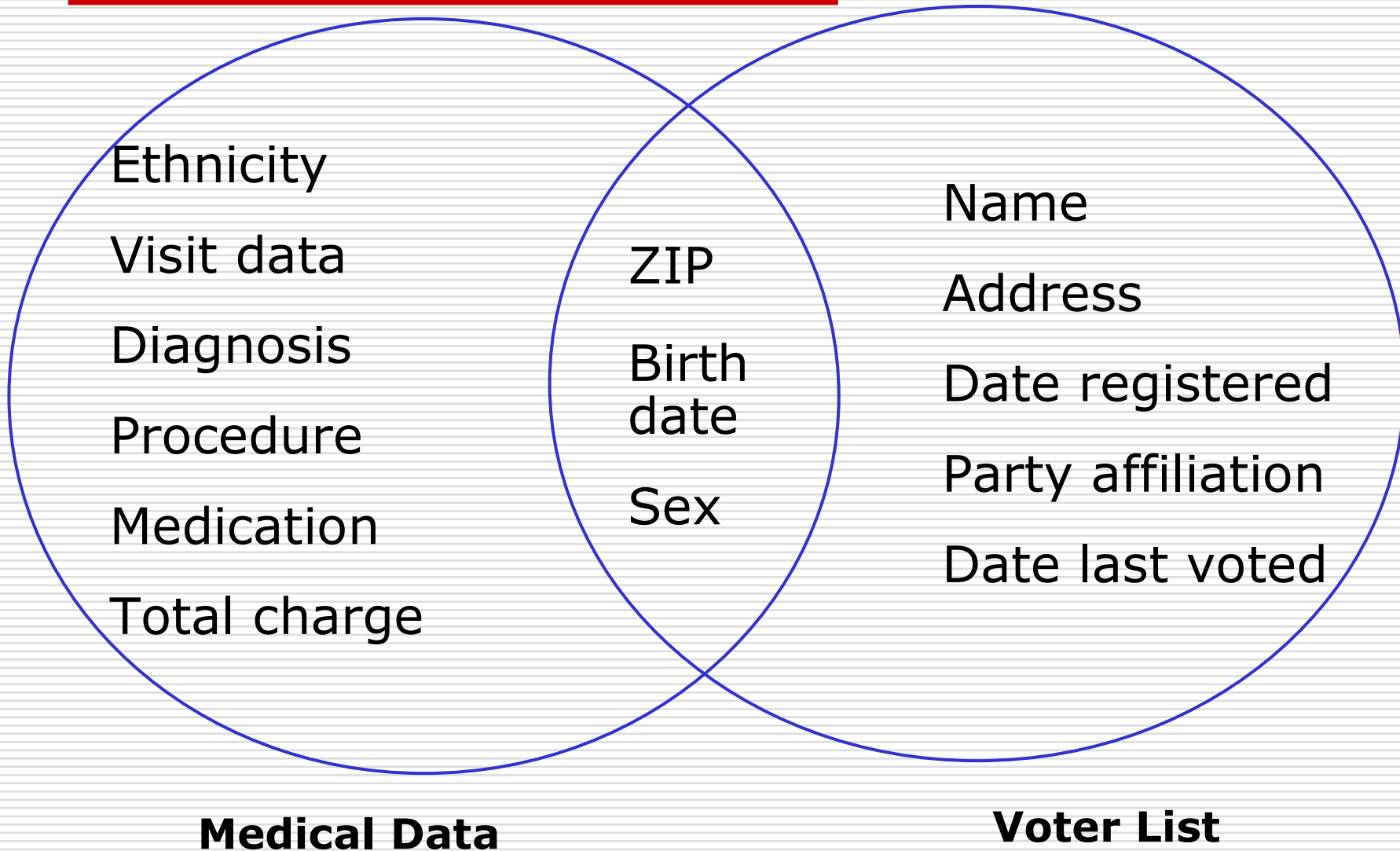
- **Collect more**  
Expand an existing person-specific data collection.
- **Collect specifically**  
Replace an existing aggregate data collection with a person-specific one.
- **Collect if you can**

Examples (#fields)	1983	1996
Each birth	15	226
Each hospital visit	0	50
Each grocery visit	0	1,272

[Source: Sweeney, 2004]

# Linking to re-identify data

---



# A new company in 2005 ...

ZoomInfo.com - Mozilla Firefox  
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe  
http://www.zoominfo.com/ Wikipedia (de)  
zoominfo  
People, Companies, Relationships  
“ It basically increases the chances of being found by an employer. ”  
- Gino S  
Find BeFound PowerSearch About Us  
The search engine for discovering people, companies, and relationships  
Person Company Find Jobs  
Zoom  
Ex: "Jonathan Stern" or "Bryan Burdick at Reuters" Advanced Search  
BeFound Create your own Web Summary  
Join the largest index of people in business in the world.  
Register for free to create a ZoomInfo Web Summary today!  
Already registered? [Update Your Summary](#)  
Get more search capabilities with PowerSearch  
Join the thousands using our flagship product [PowerSearch](#). Search by title, industry, location and over 15 other characteristics.  
Current PowerSearch customer? [PowerSearch Login](#)  
Use ZoomInfo on your desktop! [Download AOL's AIM Pro or the Watson search tool](#) »  
FAQ | Tools & Developer Resources | Terms of Service | Privacy Policy | Help | Contact ZoomInfo  
Copyright © 2007 Zoom Information Inc. All rights reserved.

# Summary: Digital World & Privacy

---

- Once personal data is released, it can no longer be controlled
  - can be distributed
  - different pieces can be linked and profiles be make
- Digital World makes this even worse
  - storage is becoming increasingly cheaper
  - data mining more efficient, e.g., Google
- Basic protection techniques:
  - release only necessary data
  - use cryptography to control and minimize the release of data
  - require from recipient that data be protected

# References & Links

---

- IBM Almaden Institute 2003: Privacy  
<http://www.almaden.ibm.com/institute/2003/agenda.shtml>
- Harriet Pearson: Privacy and Security in an On Demand World.  
<http://www.almaden.ibm.com/institute/pdf/2003/HarrietPearson.pdf>
- Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems  
<http://theory.lcs.mit.edu/~sweis/spc-rfid.pdf>
- J. Biskup, P.A. Bonatti. Lying versus refusal for known potential secrets. Data and Knowledge Engineering, 38(2):199-222, 2001
- Comic strip  
<http://ars.userfriendly.org/cartoons/?id=20030521>