# Data protection in a global economy, The IBM Experience and IBM PET Research

**Jan Camenisch, Matthias Schunter**
IBM Zurich Research Lab

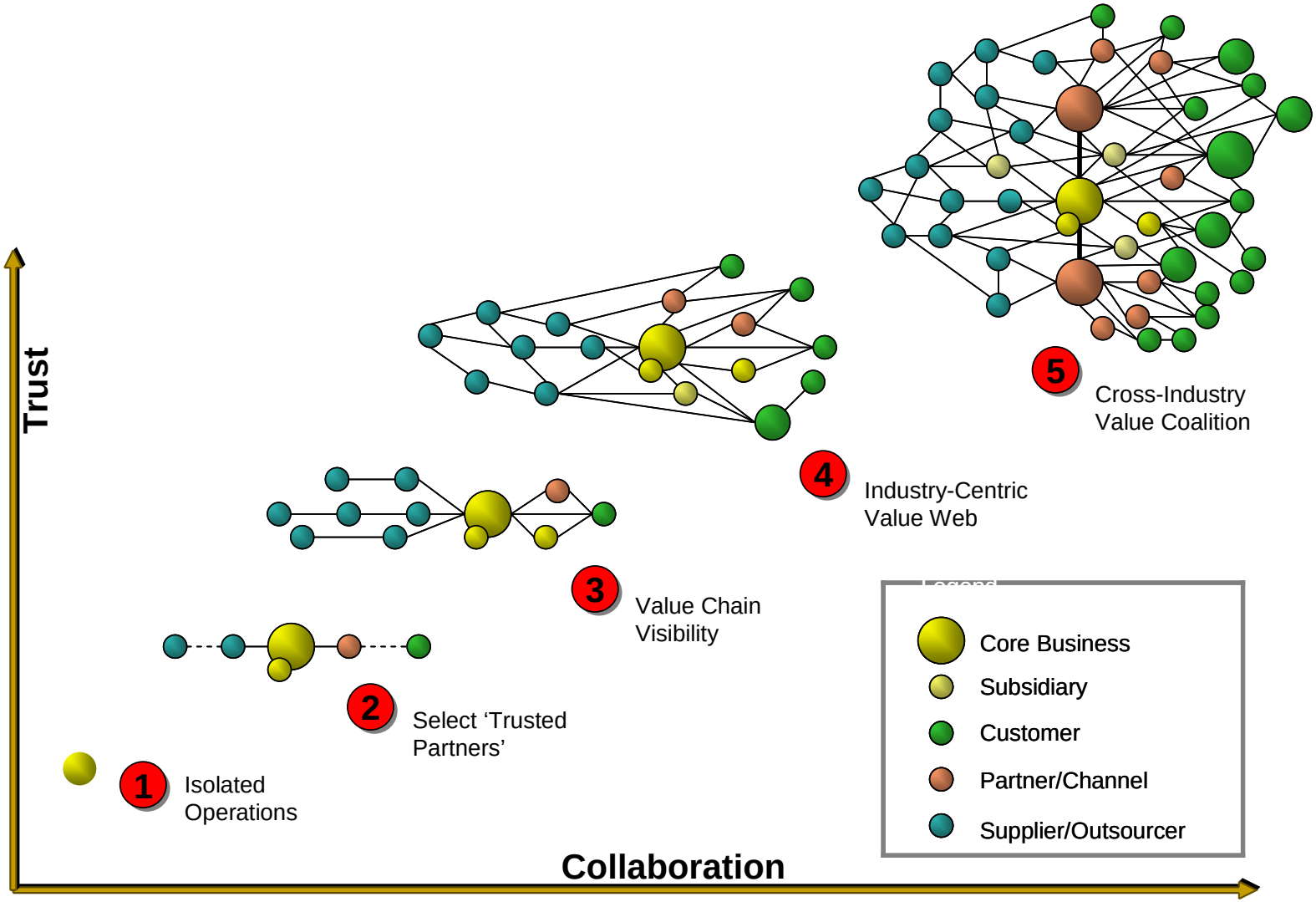
**Armgard Von Reden**
IBM Deutschland GmbH

Presented by Phil Janson, IBM Zurich Research Lab

# Outline

- **Introduction:**
  - **IBM's Privacy Challenges**
  - **IBM's Privacy Framework**
- **Privacy-enabling Technologies**
  - **Changing Landscape**
  - **IBM Technologies**
- **Suggestions for Privacy Criteria**
  - **Consumer Perspective**
  - **Enterprise Perspective**

# On demand business



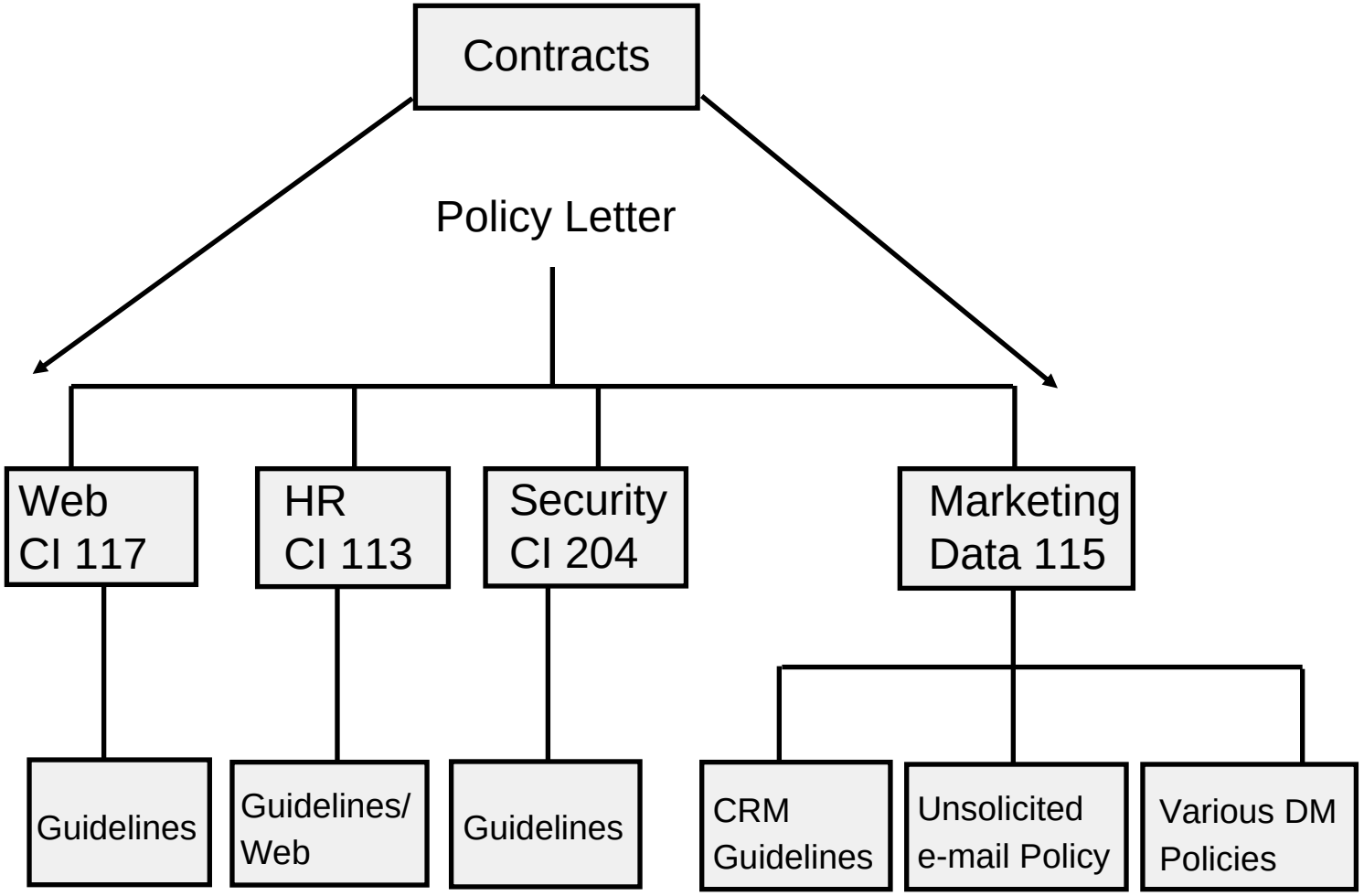
# IBM's Infrastructure and governance were simplified
# 380 000 Employees in 170+ countries
# => Increased Privacy Threat

| | BEFORE | AFTER |
|---|---|---|
| CIO | 128 | 1 |
| Host Datacenters | 155 | 11 |
| Web hosting Centers | 80 | 7 |
| Networks | 31 | 1 |

# Privacy challenges in the on demand world

- **Who can have access to the personal data in the on demand business processes**
- **How to protect the data in transfer and storage**
- **How to ensure respect of customer preferences respected in the on demand business chain**
- **How to track who has done what with the data when**
- **How to minimize / anonymize (video)data**
- **Education, awareness and compliance**

# IBM data protection framework



# Outline

- **Introduction:**
  - **IBM's Privacy Challenges**
  - **IBM's Privacy Framework**
- **Privacy-enabling Technologies**
  - **Changing Landscape**
  - **IBM Technologies**
- **Suggestions for Privacy Criteria**
  - **Consumer Perspective**
  - **Enterprise Perspective**

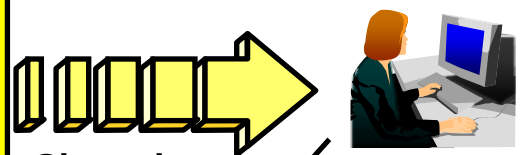
# Privacy Through Technology "Next Generation"

## What has changed?

- More, and more diverse sources of personal data
- Integration of physical and digital worlds
- Persistent storage about everything
- Easy to mine unstructured and real-time data
- Many recipients of personal information
  - Outsourcing, resource sharing, federation partners
  - Not necessarily all known to the individual
  - Not necessarily all trusted by the individual

# Global E-mail Cleansing Service

- Data owner uploads the e-mail campaign list to a secure website hosted by Harte Hanks.
- Within 24 hours the data owner is sent an e-mail message informing them to return to the website to collect the cleansed/suppressed files.
- Data owner collects cleansed file and sends to e-Engine for campaign execution
- Typically 35% reduction






GECS User ID & Password

Upload from PC to Web Site

e-List from User

Cleansed e-List from GECS

Suppr. e-Mail Address Found

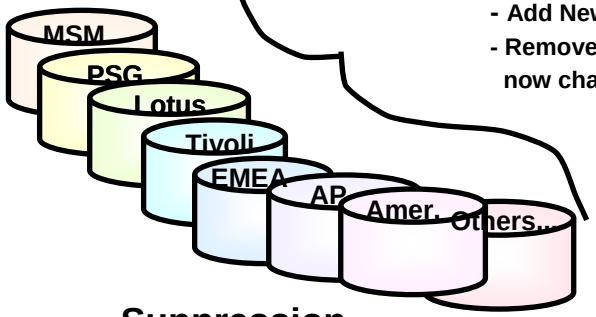
Download from Web Site to PC

Suppression Feed

Authorized Personnel Only

Website hosted by Harte Hanks

- Add New Suppressions
- Remove old Suppressions now changed to Permissions

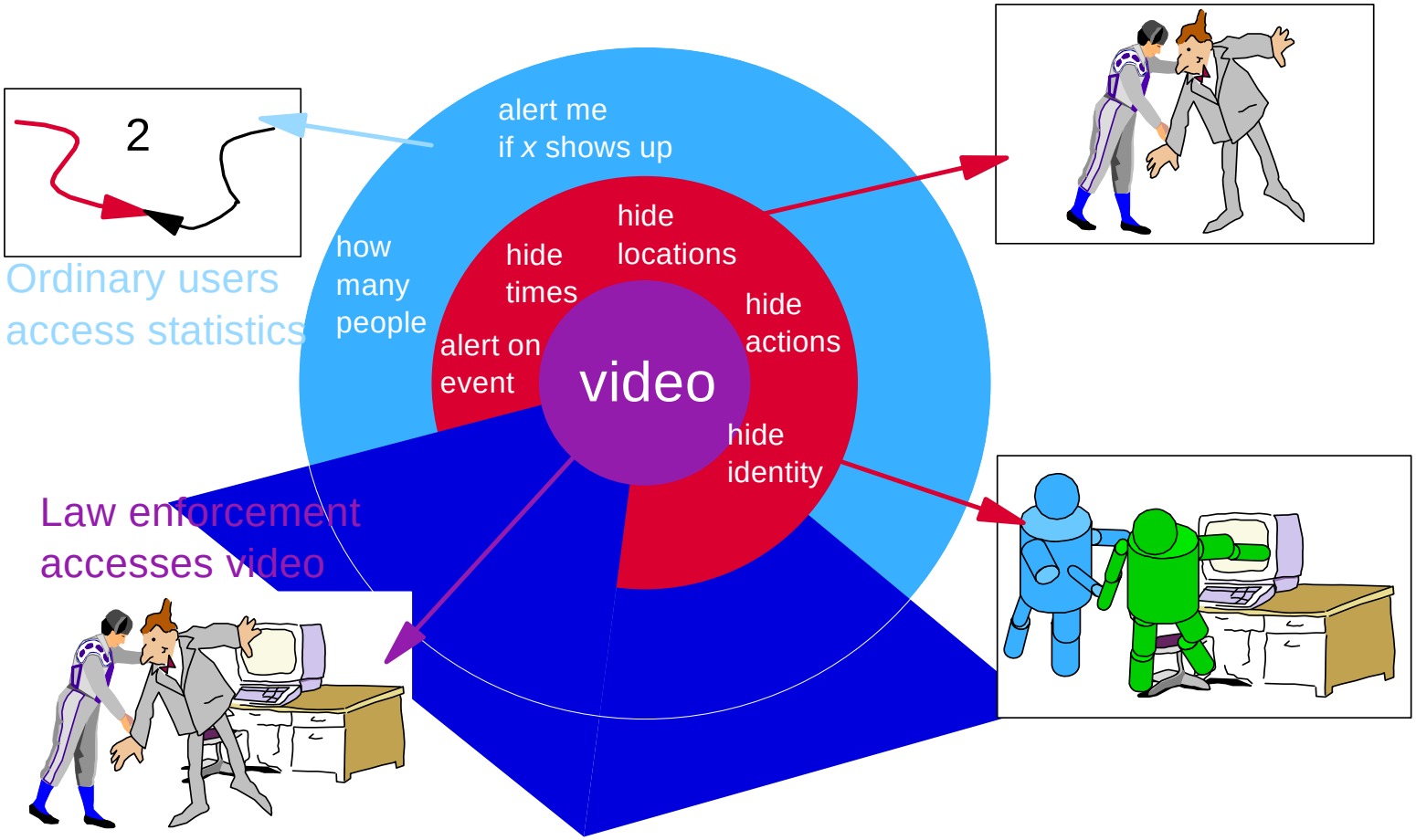



Suppression Sources

Database held in Belgium to avoid European Data Privacy Issues

Global e-Suppression Database held in Belgium

# Smart Surveillance System – Privacy-Enhancing Cameras

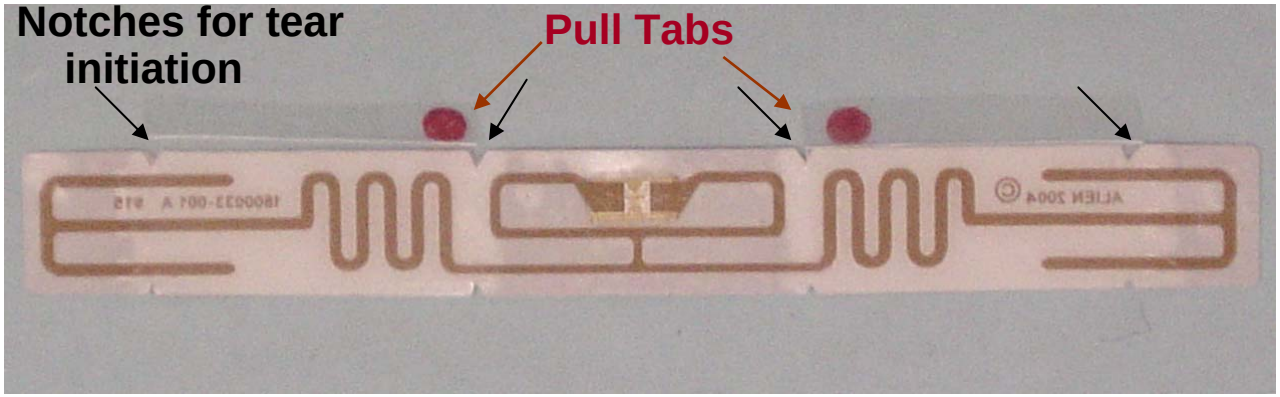


# Clipped RFID Tags

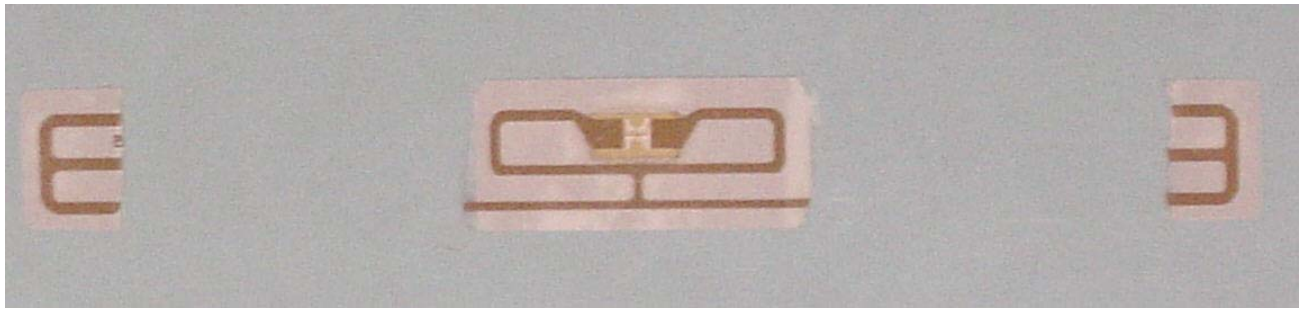
**Implementation for UHF tags – the tag substrate can be perforated or notched for tear initiation**

**Before: Range is over 2 meters with handheld reader**

Scale: Tag length ~ 10 cm (4 inches)

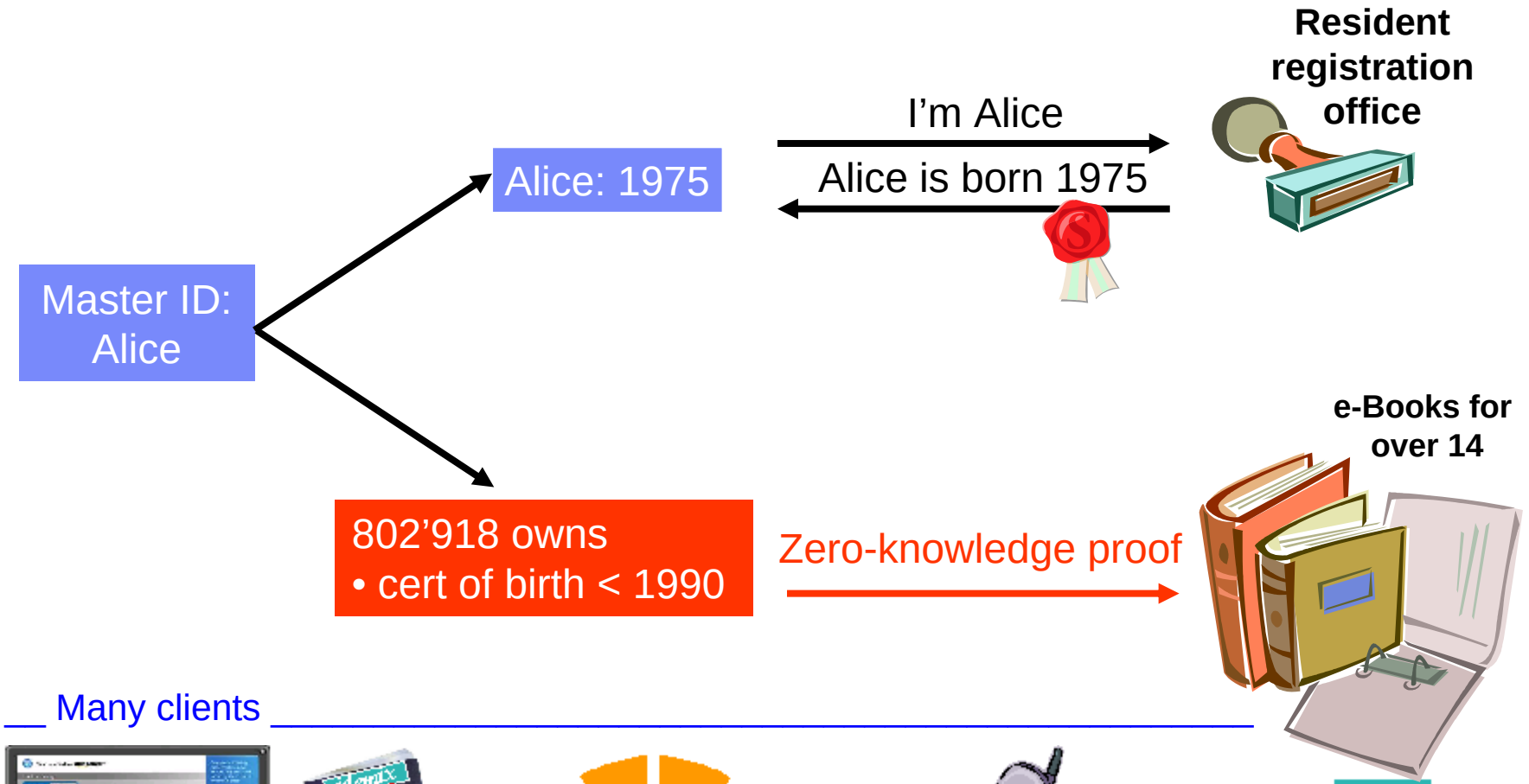



**After: Range is less than 5 cm with handheld reader**



Tags provided by Doug Martin, Alien Technology

# Identity Mixer – Anonymous Attribute-based Access



# Outline

- **Introduction:**
  - **IBM's Privacy Challenges**
  - **IBM's Privacy Framework**
- **Privacy-enabling Technologies**
  - **Changing Landscape**
  - **IBM Technologies**
- **Suggestions for Privacy Criteria**
  - **The Consumer Perspective**
  - **The Enterprise Perspective**

# The Consumer Perspective (EU PrimeLife)

- **Minimum Disclosure**
- **Ease of use – “Transparent Privacy”**
- **Sustainability – “Privacy for Life”**
- **Trustworthy Enforcement**
- **Multi-party Considerations**

# Benefits of PETs from an Enterprise Perspective

**Regulatory Compliance**

- **Simplified Compliance with Privacy Laws**
- **Reduced Risk of Privacy Breaches**

**Data Quality**

- **Better data quality from less data collection**
- **More essential information – better intelligence**
- **Avoids "Data Rich – Information Poor" effect**

**Business Focus**

- **Identity Provider owns "customers"**
- **Other Service Providers need not maintain registrations**
- **Customer buy-in**

# The Enterprise Perspective

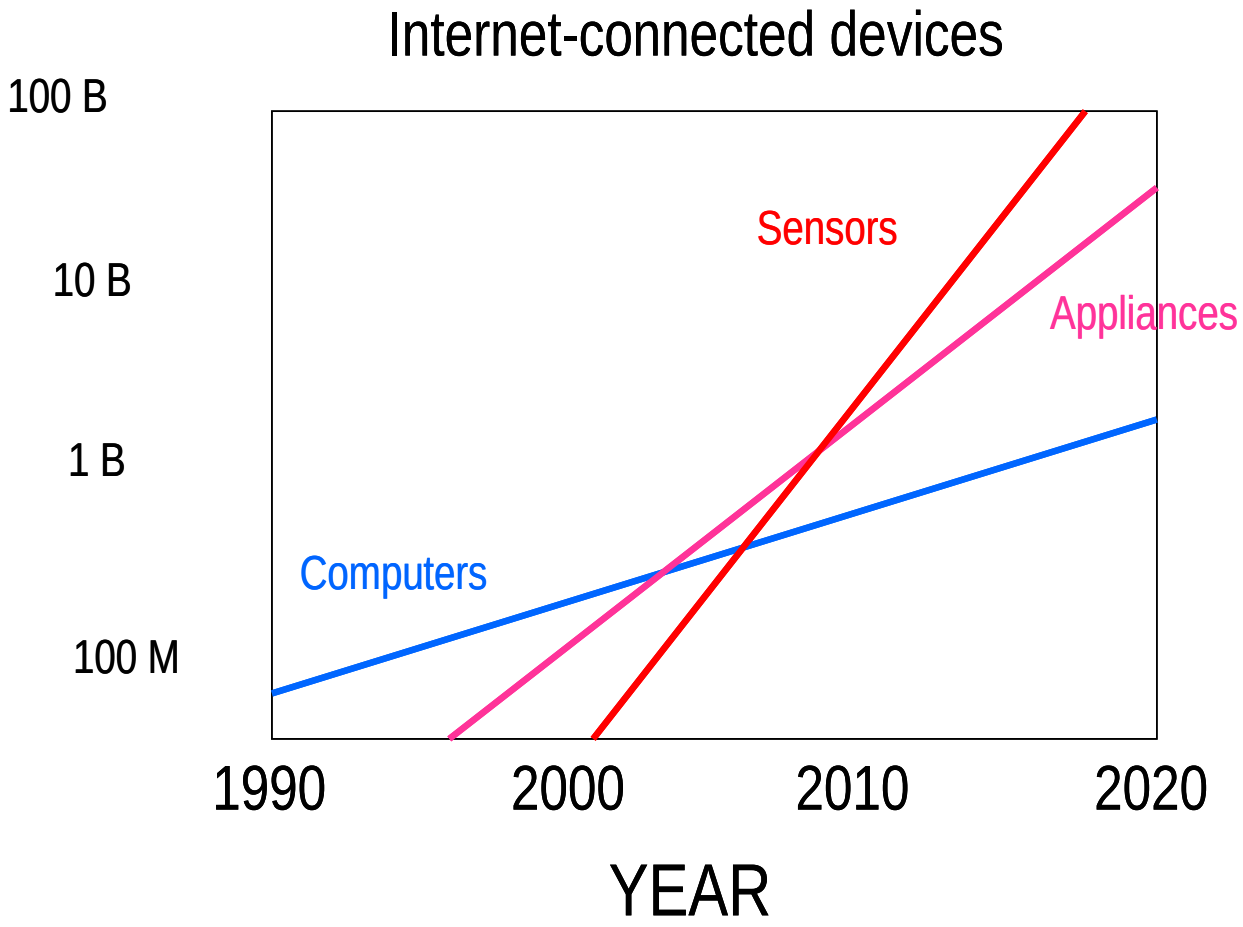
- **Incentives:**
  - **Benefit from compliance (competitive/reduced risk)**
  - **Safety from suing if follows rules (e.g. EU model clauses)**
- **Cost-effectiveness:**
  - **Requirement for newly built systems**
  - **Differentiator for products**
- **Performance-effectiveness:**
  - **Requires**
    - **Regular reassessment**
    - **Monitoring security / privacy tradeoff**
    - **Preserving customer experience through “Transparent Privacy”**

# Conclusion

- New Technologies – New Privacy Challenges
- Technology can also help!
- Privacy Criteria should
  - Aim at creating incentives
  - Aim at effective implementation

# The End…

# Data everywhere / Sensors Will Predominate / Metadata




# Hippocratic Database Technologies

**Create a new generation of information systems that protect the privacy, security, and ownership of data while not impeding the flow of information.**

## Policy-Based Private Data Management

**Active Enforcement**
Database-level enforcement of disclosure policies and patient preferences

**Privacy Preserving Data Mining**
Preserves privacy at the individual level, while still building accurate data mining models at the aggregate level

## Secure Information Exchange

**Optimal *k*-anonymization**
De-identifies records in a way that maintains truthful data but is not prone to data linkage attacks

**Sovereign Information Sharing**
Selective, minimal sharing across autonomous data sources, without trusted third party

## Efficient Data Access Tracking

**Compliance Auditing**
Determine whether data has been disclosed in violation of specified policies

**Database Watermarking**
Tracks origin of leaked data by tracing hidden bit pattern embedded in the data

# New CDT RFID/Privacy Best Practices

- **Center for Democracy and Technology has drafted best practices**
- **CDT's goal is to increase transparency about the use of RFID technology involving consumers**
  - **Strong focus on: protecting Personally Identifiable Information (PII) and "clear, and concise" notification**
- **Aim is to promote industry self-regulation over legislation/regulation**
- **Working group includes IBM, P&G, GM, Microsoft, HP, Cisco, Intel, Electronic Frontier Foundation, National Library Assn, National Retail Federation, National Consumers League**