“What Do You Want to Share Today?”
Building Privacy-Aware AmI-Systems
Marc Langheinrich
Institute for Pervasive Computing
ETH Zürich
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. Collection Limitation
  5. Data subject’s consent

- Core principles of most modern privacy laws
  - Implication: Technical solutions must support FIP
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. Collection Limitation
  5. Data subject’s consent

**Core Question**: Can (user interface) technology support those principles that need user involvement? Can we put the user “into the loop“ of privacy protection?
Openness in AmI

- No hidden data collection!
  - Legal requirement in many countries
- Established means: privacy policies
  - Who, what, why, how long, etc. ...
Openness in AmI

- 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?
- Too many devices?
  - Countless announcements an annoyance
  - Notices “get in the way” – Background vs Foreground
Openness in Aml

- No hidden data collection!
  - Legal requirement in many countries
- Established means: privacy policies
  - How many people read SSL certificate warnings?
  - Cookie warnings? Do you want to proceed, yes or no?
  - Periodic broadcasts?
- Too many devices?
  - Countless announcements an annoyance
  - Notices “get in the way” – Background vs Foreground
Access & Control in AmI

- Identifiable data must be accessible
  - Users can review, change, sometimes delete
- Collectors must be accountable
  - Privacy-aware storage technology?
Access & Control in AmI

- Identifiable data must be accessible
  - Users can review, change, sometimes delete
- Collectors must be accountable
  - Privacy-aware storage technology?
- Whom should I ask?
  - Countless, often unknown interactions. Centralized?!
- How to check for correctness?
  - Is this really my walking pattern?
Consent in AmI

- Participation requires explicit consent
  - Usually a signature or pressing a button
- True consent requires true choice
  - More than „take it or leave it“
Consent in AmI

- 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?)

Consenting to what?
- Do I understand the implications?
Consent in AmI

- 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?)
- Consenting to what?
  - Do I understand the implications?
Example: Convenience

- **Emnid survey Germany (03/2002)**
  - 50% have at least one loyalty card
  - 72% welcome such offers
- **70 million cards in circulation (12/2003)**
  - 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 – 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)
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)

Informed Consent?
Who Would Think of Such Things When Buying a Screwdriver?!
“Do-the-right-thing” Privacy

- No one **wants** to manage their privacy!
  - Anonymizer (Zero-Knowledge.com)? Infomediaries?
  - Privacy interface? Identity managers?
“Do-the-right-thing” Privacy

- No one wants to manage their privacy!
  - Anonymizer (Zero-Knowledge.com)? Infomediaries?
  - Privacy interface? Identity managers?

- Challenge: When to share what with whom?
  - Simple command (touch, shake, press) for paying, etc.
  - System knows what to share (not too much!)

- Challenge: Something wrong?
  - Simple to check
  - Simple to fix or get help
„Pervasive Privacy“ (Rossnagel)
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
„Pervasive Privacy“ (Rossnagel)
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?