Privacy by Design

Privacy by Design

Principles of Privacy-Aware Ubiquitous Systems

Marc Langheinrich
ETH Zurich, Switzerland

www.inf.ethz.ch/~langhein

RESEARCH GROUP FOR
Distributed Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Ubicomp 2001, Atlanta

Contents

- Privacy primer
  - Does privacy matter?
- Privacy in ubiquitous systems
  - What's so different about it?
- Challenges
  - Issues to address in ubicomp systems
- Privacy-aware infrastructures
  - A first attempt

Just a Modern Fad?

- "All this secrecy is making life harder, more expensive, dangerous..."
  - Peter Cochran, former head of BT Research
- "You have zero privacy anyway"
  - Scott McNealy, CEO Sun Microsystems
- "By 2010, privacy will become a meaningless concept in western society"
  - Gartner Report

Privacy – a Human Need?

- References in the Bible
- Jewish law ("...free from being watched")
- Justice of Peace act (England 1361)
- Privacy is a human right
  - Universal declaration of human rights, article 12 (1948)
  - European convention on human rights, article 8 (1970)

Legal Realities Today

- Legislation varies around the world
  - Mostly self-regulatory approach in US
  - Comprehensive laws for government and industry in EU
- EU Directive 95/46/EC
  - Limits data collection
  - Requires comprehensive disclosures
  - Prohibits data export to „unsafe“ countries
    - Prompted legislative updates worldwide

Contents

- Privacy primer
  - Does privacy matter?
- Privacy in ubiquitous systems
  - What's so different about it?
- Challenges
  - Issues to address in ubicomp systems
- Privacy-aware infrastructures
  - A first attempt

Aspects of Privacy

- Anonymity
  - Authentication & Routing
- Security
  - Encryption & Communication Hiding
- Transparency
  - Trust-Labels, Signatures, Protocols (P3P)

How much of this works in ubicomp?

Unlimited Coverage

- The Web: covers our *digital* life
  - Shopping, chatting, news reading
- Ubicomp: *real-world* deployment!
  - Home, School, Office, Public Spaces, ...
- Covers *all* of our life, comprehensively!
  - Day in, day out – from cradle to grave
- No switch to turn it off?
  - Constant, seamless surveillance possible

Loss of Awareness

- Surveillance and data collection today
  - Stores, credit card applications, sweepstakes
- Ubicomp: invisible computing
  - Computers *disappear* into the environment
- When am I giving out data?
  - Fingerprint could be taken without notice
- When am I under surveillance?
  - Life recorders, room computers, smart cups

New Types of Data

- Last 50 years of data collection
  - Identity, contact info, preferences, ...
- Ubicomp: advanced sensors
  - New data (location, health, habits, ...)
  - More detailed & precise (24/7)
- Does the system know more than I?
  - Body sensors detect moods
  - Nervous? Floor & seat sensors, eye tracker

More Data, More Knowledge

Ubicomp 2001, Atlanta

- Traditional data, traditional use
  - Compiling mailing lists, predicting trends, …
- Ubicomp: smartness through context
  - Context is distilled sensory information
- Encourages increased data collection
  - More data means more, better context
- Innocuous data can lead to new knowledge
  - Data mining: more than the sum of its parts

Contents

- Privacy primer
  - Does privacy matter?
- Privacy in ubiquitous systems
  - What's so different about it?
- Challenges
  - Issues to address in ubicomp systems
- Privacy-aware infrastructures
  - A first attempt

1. Notice

- 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

- Laws require *explicit consent* by user
  - 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. 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)

5. 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

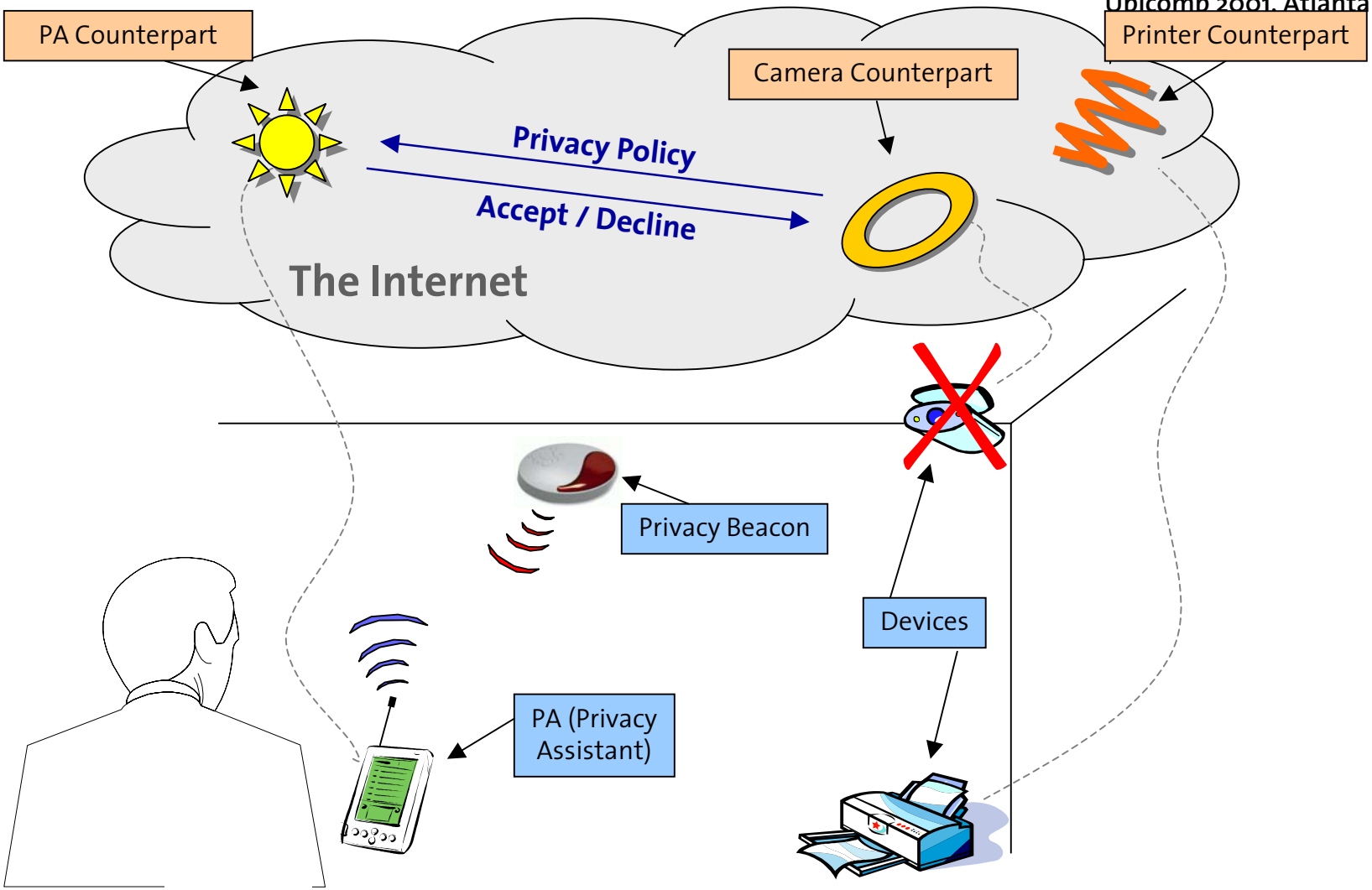
6. Access & Recourse

- 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?

Contents

- Privacy primer
  - Does privacy matter?
- Privacy in ubiquitous systems
  - What's so different about it?
- Challenges
  - Issues to address in ubicomp systems
- Privacy-aware infrastructures
  - A first attempt

Privacy Infrastructures



Privacy Infrastructure

- Project Status
  - Started Aug 2001
  - Currently devising architecture
- Challenges
  - Policy broadcasts, privacy services, user interface, ...
- Goals
  - Operational prototype for trying out new concepts

The Take Home Message

- Many questions, few answers
  - Technology, laws still to evolve
- Ubicomp adds a new quality to privacy
  - Invisible, real-world coverage, comprehensive collection, inconspicuous
- Ubicomp (privacy) challenges
  - User interface (notice, choice, consent)
  - Protocols (anonymity, security, access)
  - Social acceptance (user expectations)