A Privacy Awareness System for Ubicomp

Marc Langheinrich
ETH Zurich, Switzerland

RESEARCH GROUP FOR
Distributed Systems

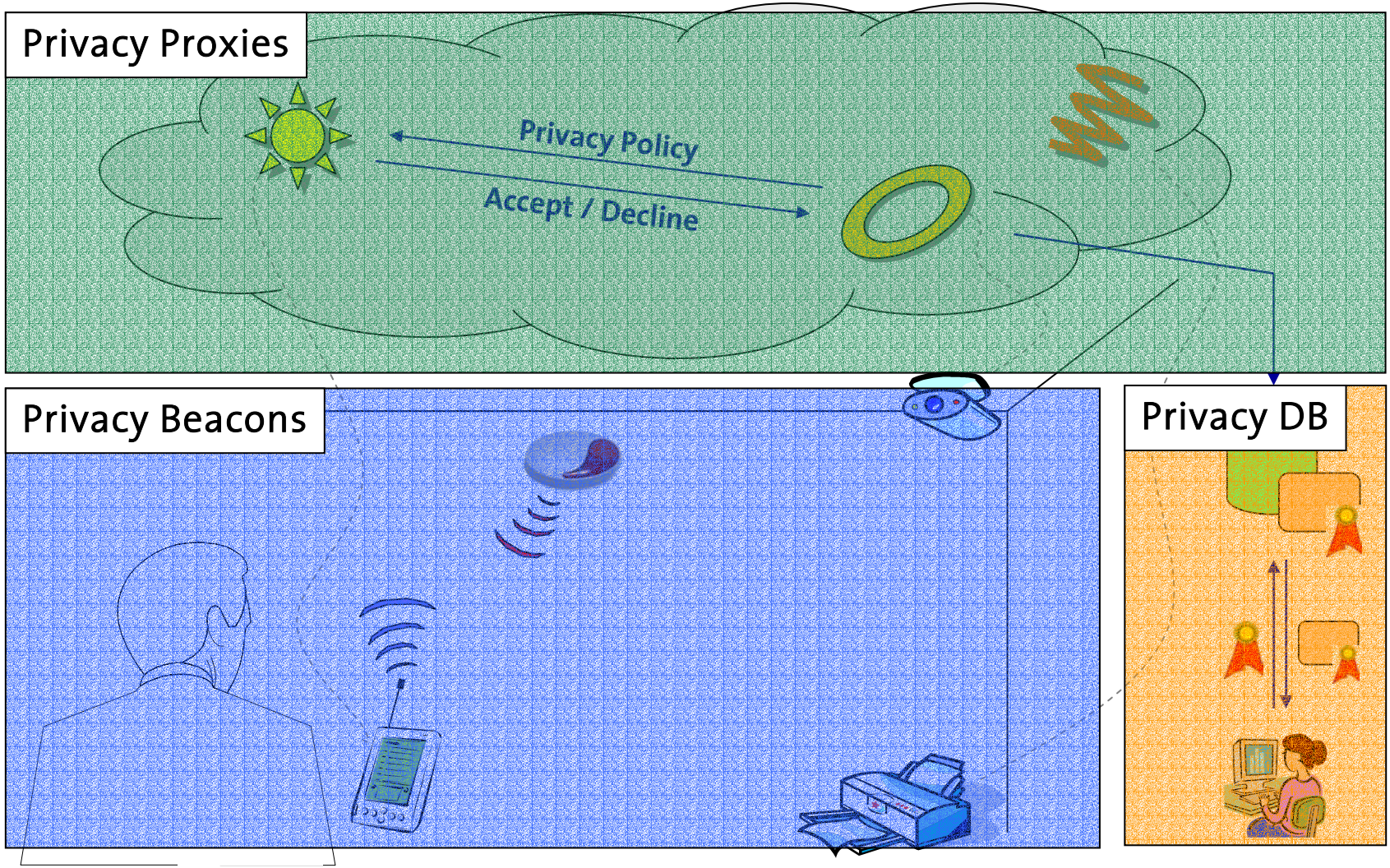
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Motivation

- Ubicomp features real-world electronic services, often without user interface
- Automated data transfer facilitates interaction with such services
- Anonymous usage not always possible
- User should stay in control of data flow

Control and Transparency Tools

Privacy Awareness System

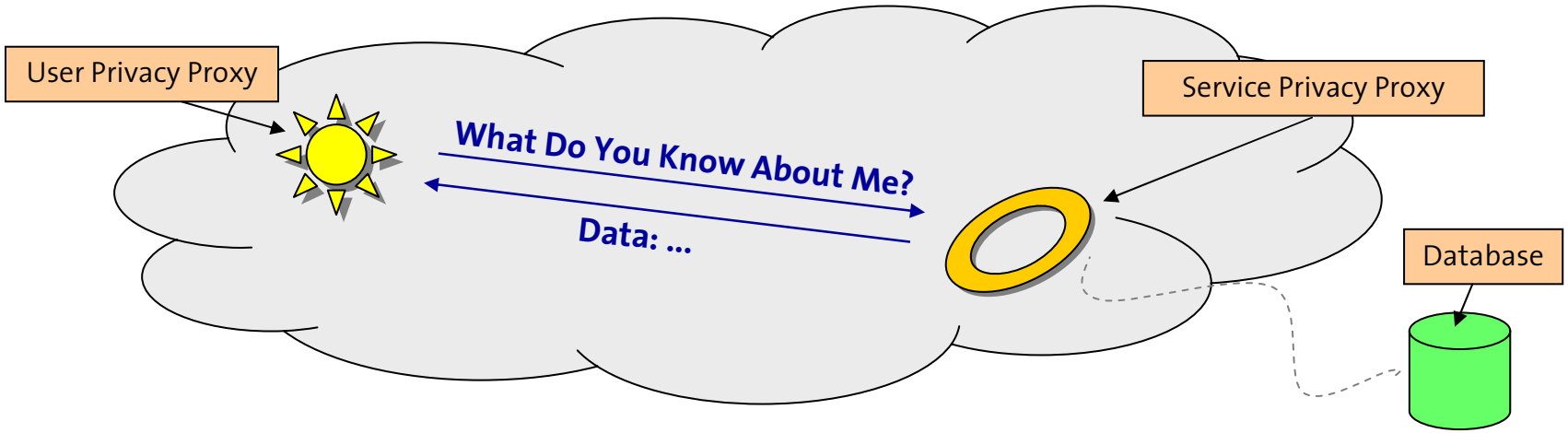


1. Privacy Beacons

- Let people (data subjects) know about collection
  - "Software" beacons as part of service discovery
  - "Stand-alone" beacons for video, audio rec.
- Beacons describe data to be collected, purpose
  - Machine-readable privacy policies (P3P)
  - Extended with ubicomp-specific fields

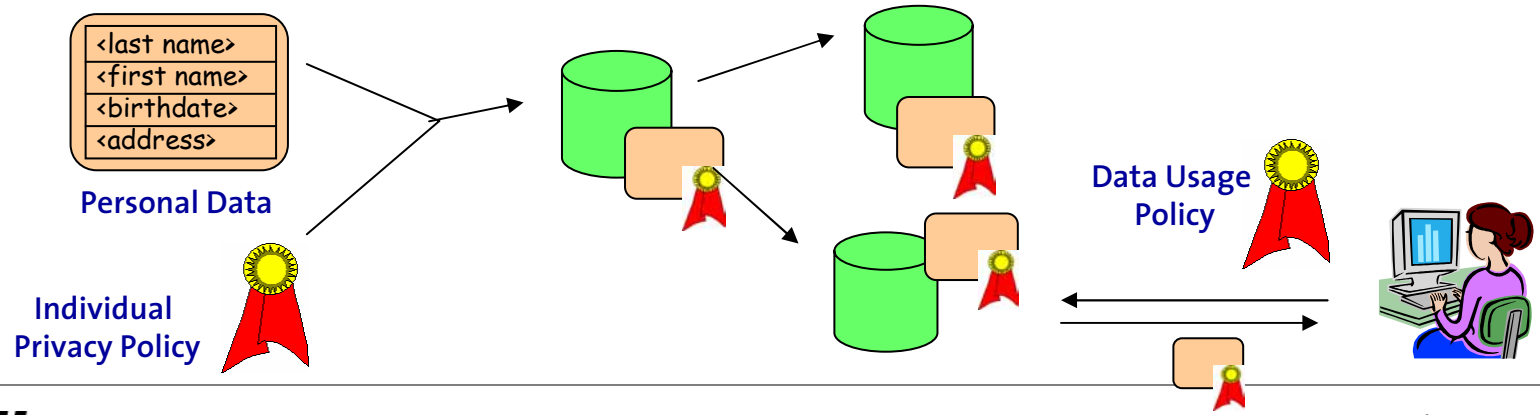
2. Privacy Proxies

- Service proxy solicits data subject's consent
  - User proxy compares preferences (APPEL) with policy obtained from service proxy
- Provide single entry point for data exchange
  - Allows automated data inspection, update, deletion

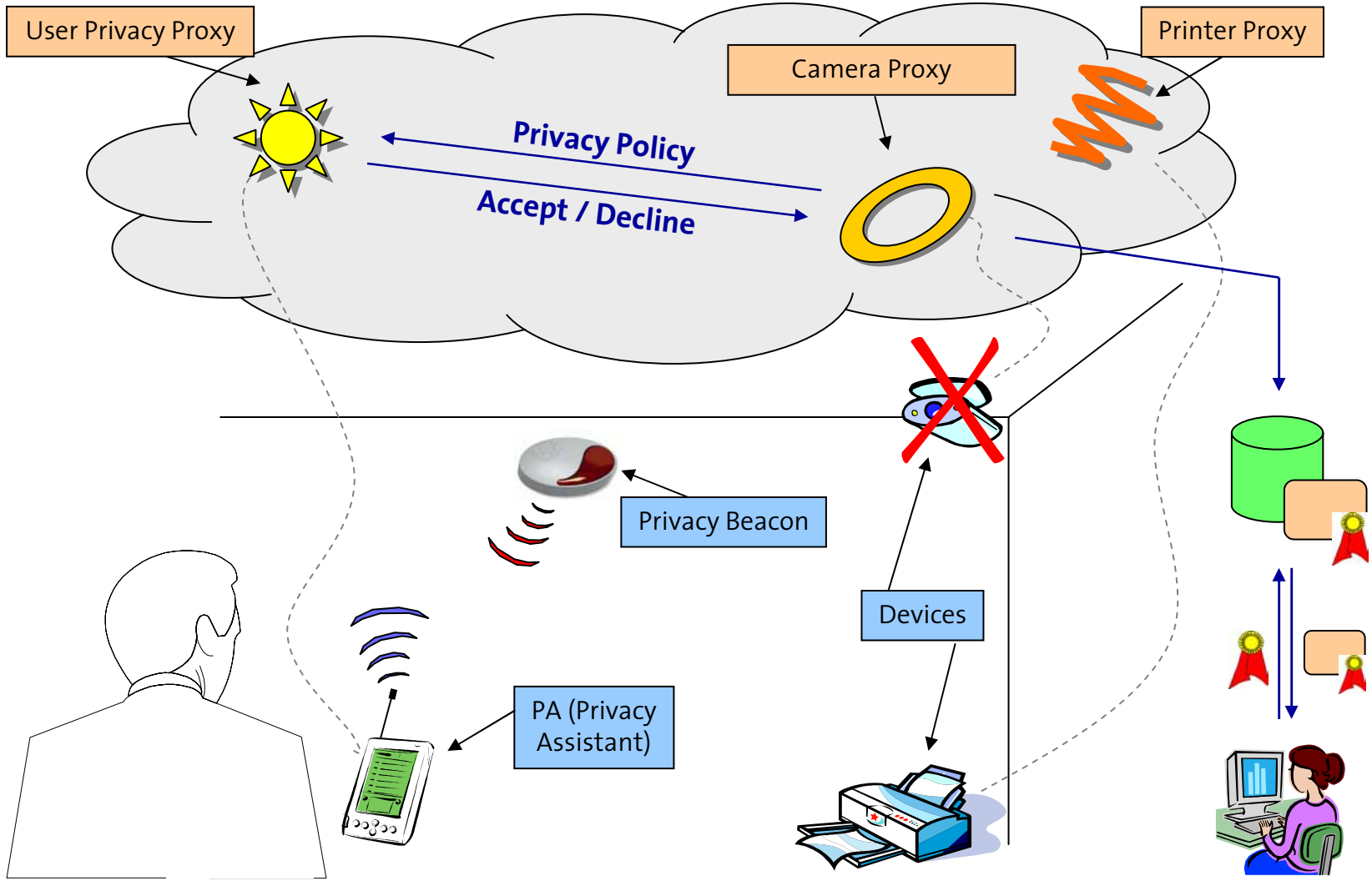


3. Privacy Aware Database

- Store personal info together with P3P policy
  - Data and policy (metadata) form single logical unit
- Requires usage policy for each data access
  - DB compares policies for data subject and data user and only releases records w/ matching policies
  - Each data usage recorded in usage log (auditing)

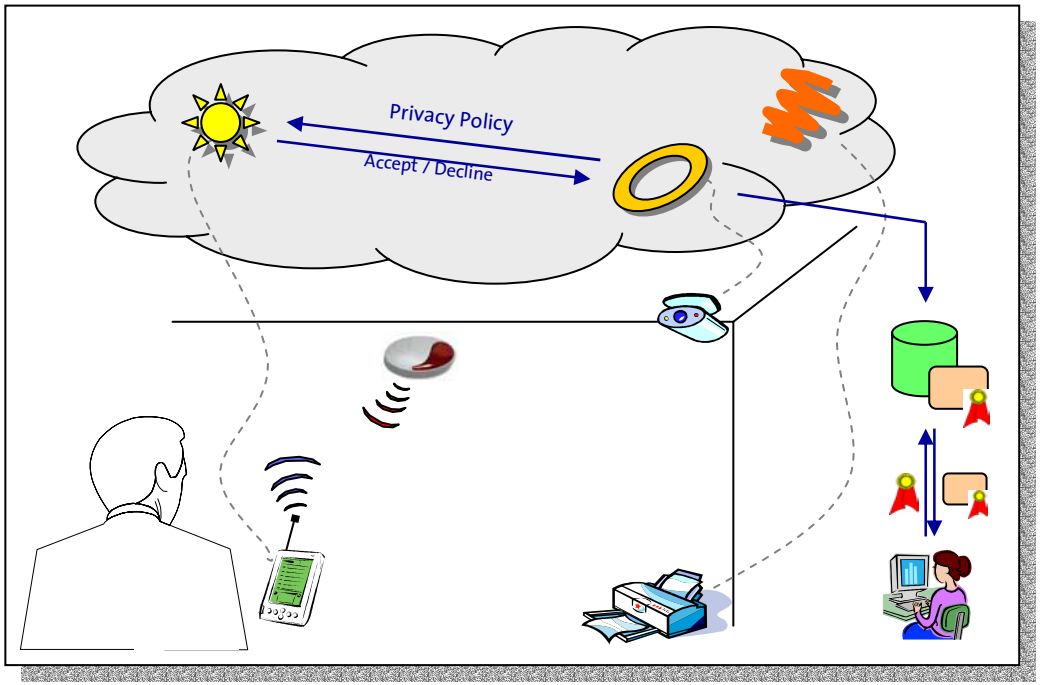


Privacy Awareness System



Privacy Awareness System

- Privacy Database
  - Oracle 8i, Java interface (no direct table access)
  - P3P policies cached for speed
- Privacy Proxies
  - Web service (Apache Tomcat)
  - SOAP, SSH
  - Extended P3P
- Privacy Beacons
  - In the works
  - BT/IR, iPAQ



The Take Home Message

- Privacy is Possible in Ubiquitous Computing
  - Let people know about collections (beacons)
  - Let people query, update, delete own data (proxies)
  - Let people know about (each) usage (database)
- Solutions Need Not be Perfect to be Useful
  - Trusting fair information practices
  - Trusting collectors to keep their promises
  - Trusting the legal system (rouge collectors)

Open Issues

- User Issues (Data Subject)
  - Can the average user specify preferences?
  - How are multiple preferences merged?
- Service Issues (Data Collector)
  - Does anybody need that fine-grained control?
  - Efficiency, efficiency, efficiency
- Enforcement and trust
  - Incorporating anonymity, pseudonymity
  - How can we catch the bad guys?