



# Vorlesung

# Datenschutz und Privatheit in vernetzten Informationssystemen

Kapitel 8: Ubiquitous Computing  
*Teil 2: Smart Environments*

Erik Buchmann  
buchmann@ipd.uka.de



# Agenda für heute

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Smart Environments
  - Szenario, Rollen, Speicherorte
  - Anpassung der OECD-Datenschutzrichtlinien auf Smart Environments
- Privacy Middleware für Smart Environments
  - PawS
  - Confab Toolkit



# the AWARE HOME

A residential laboratory developing technology to solve the needs of home life now and in the future.



## Smart Environments

- das “Aware Home” vom Georgia Institute of Technology
  - Testbett für Anwendungen
    - Werkzeuge für den Alltag
    - Unterstützung für Personen mit eingeschränkten Fähigkeiten, z.B. Senioren oder Autismus-Patienten
  - Testbett für Technologien
    - Infrastruktur
    - Datenerfassung



# Technologiebeispiele

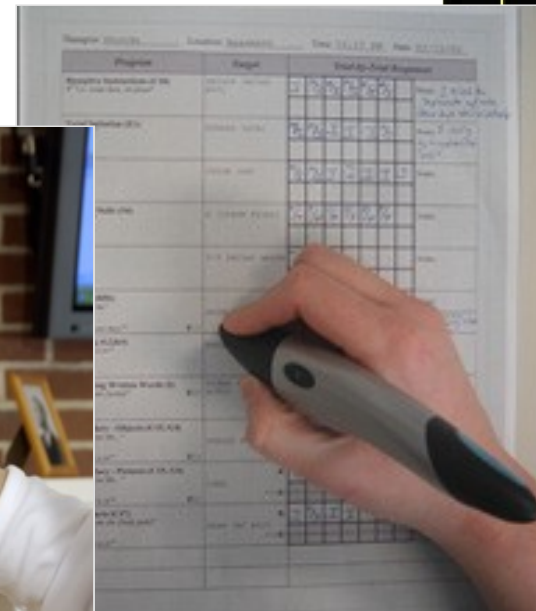
[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Optische Erfassung von Bewegungsdaten und Kontextinformationen
- Gesten, Touch-Screens, elektronische Stifte zur Steuerung von Abläufen



Quelle: <http://awarehome.imtc.gatech.edu>



# Prinzipien des Datenschutzes

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- OECD-Richtlinien (und geltendes Recht) fordern u.a.
  - Erforderlichkeit, Datensparsamkeit
  - Zweckbestimmung bei der Erhebung
  - Korrektheit
  - Nutzungsbegrenzung
  - Transparenz
  - Partizipation
- Schwer durchsetzbar im Ubiquitous Computing
  - viele Beteiligte mit unklaren Rollen
  - Erhebung und Verarbeitung im Hintergrund
  - riesige Zahl von adaptiven Datenverarbeitungsprozessen





# Datenschutz in Smart Environments

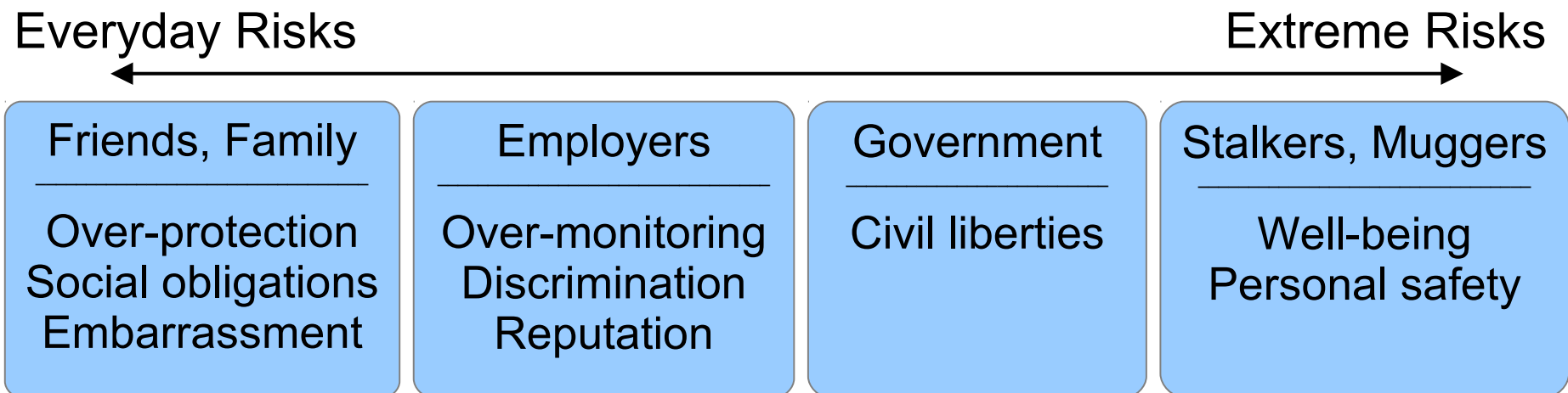
Einführung

[DS-Prinzipien](#)

PawS

Confab

- Anderer Ansatz als OECD-Richtlinien erforderlich
  - keine vollständige Sicherheit, vollständige Privatheit *nicht erzielbar* und/oder *nicht wünschenswert*
  - stattdessen: *Kompromiss* zwischen Nutzen und Aufwand beim Anwender



Quelle: [3]





# Principle of Minimum Asymmetry (1/2)

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Beobachtung: negative Auswirkungen entstehen oft durch Asymmetrie zwischen zwei Interaktionspartnern
    - Informations-Asymmetrie
    - “Macht”-Asymmetrie
  - **Principle of Minimum Asymmetry**
    - Informationsfluss vom Betroffenen zum Datensammler verringern
    - Informationsfluss vom Datensammler zum Betroffenen steigern
- *Wesentliches Grundprinzip aller Privacy-Ansätze im Ubiquitous Computing*



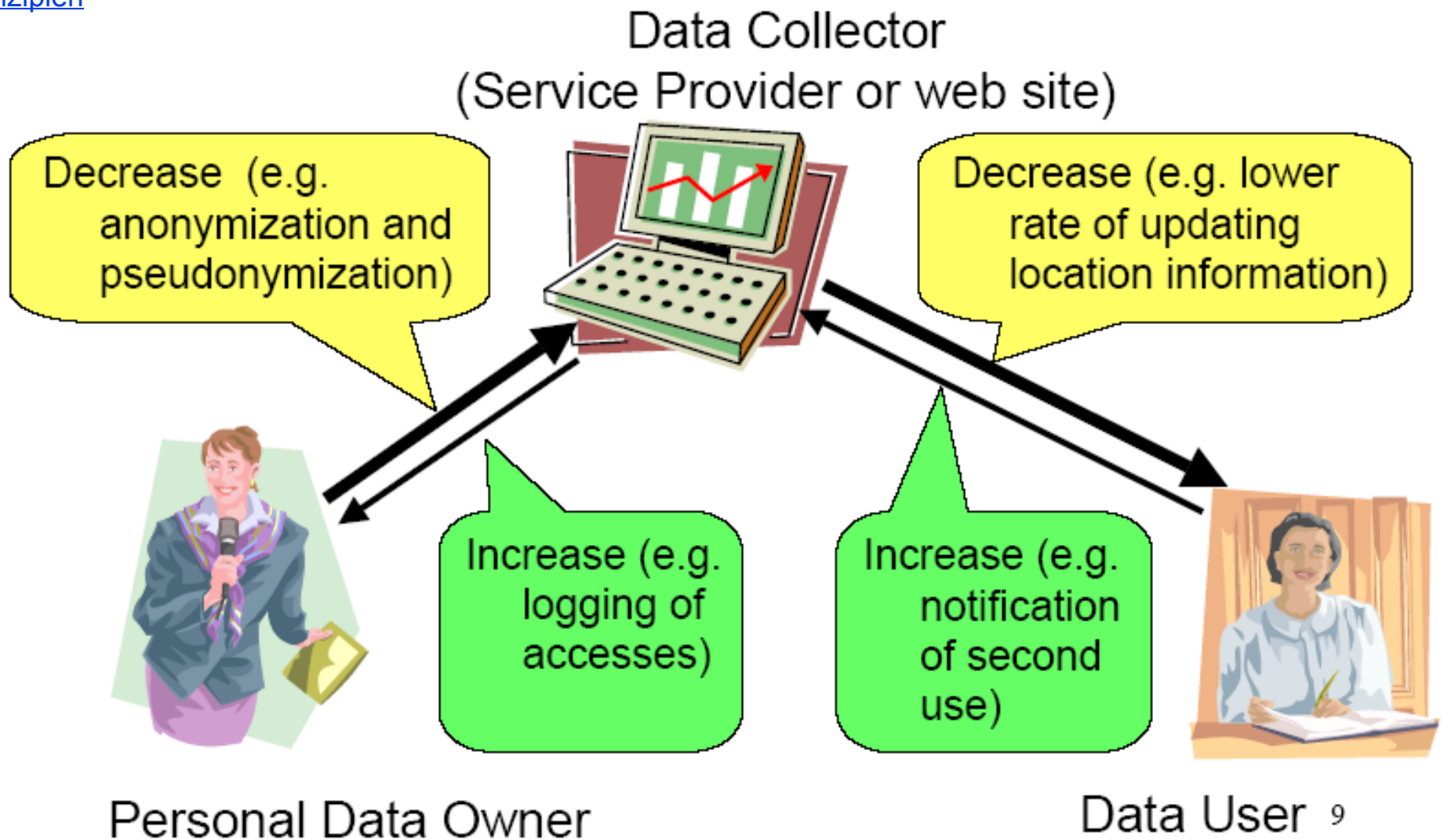
# Principle of Minimum Asymmetry (2/2)

Einführung

[DS-Prinzipien](#)

PawS

Confab



Quelle: S. Yamada, Presentation at APNOMS2003



# Datenschutzrichtlinien in Smart Environments

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Vorschlag für eine Adaptierung der OECD-Richtlinien auf Smart Environments [1]:
  - **Notice**
  - **Choice and Consent**
  - **Anonymity and Pseudonymity**
  - **Proximity and Locality**
  - **Adequate Security**
  - **Access and Recourse**





# Notice

Einführung

[DS-Prinzipien](#)

PawS

Confab

- Notice entspricht Transparenz
- Betroffener muss Datenerhebung bemerken können
  - es muss verhindert werden, dass Smart Items ihren Nutzer *unbemerkt* ausspähen können
- Umsetzung hängt von der Technologie ab
  - optische Markierungen
  - RFID-Tags mit elektronischen Warnungen an sensiblen Orten angebracht
  - Announcement-System, z.B. Funkbaken
- *Idealerweise sollte Notice elektronisch automatisch auswertbar sein (vgl. P3P)*





# Choice and Consent

Einführung

[DS-Prinzipien](#)

PawS

Confab

- Aufweichen der *expliziten* Einwilligung
  - Gesetz fordert explizite Zustimmung
    - nicht automatisierbar (Software-Agenten?)
    - erfordert eine Benutzerschnittstelle (RFID-Tags?)
  - in Smart Environments andere Einwilligungen möglich
    - z.B. implizit durch Dienstnutzung
- Auswahl (Choice) muss tatsächlich bestehen
  - Nutzung von Smart Environments auch dann, wenn Datenerhebung verweigert wird
  - es dürfen nur Dienste ausfallen, die auf die Daten tatsächlich angewiesen sind
  - ggf. Auswahl über Dienstgüteparameter





# Anonymity and Pseudonymity

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Daten so oft als möglich anonym oder pseudonym erheben
  - Personalisierung von Diensten durch ein Portfolio von vom Nutzer wählbaren Pseudonymen
    - z.B. ein Pseudonym für zu Hause, eines für die Arbeit, eines zum Einkaufen im Supermarkt etc.





# Proximity and Locality

Einführung

[DS-Prinzipien](#)

PawS

Confab

- Proximity
  - vergessene oder zurückgelassene Smart Items sind inaktiv; aktiv nur wenn Besitzer anwesend
  - kein unbemerktes Ausspähen durch vom Besitzer versteckte Sensoren
- Locality
  - Informationen bleiben (wenn möglich) an dem Platz, an dem sie aufgezeichnet wurden
    - z.B. verlassen Daten über die Bewegung am Arbeitsplatz nicht das Gebäude
  - physische Anwesenheit für Datenzugriff erforderlich
- *Solche Hürden behindern die meisten Dienste nicht, verhindern aber lückenlose Überwachung von Ferne*





# Adequate Security

Einführung

[DS-Prinzipien](#)

PawS

Confab

- das Problem liegt beim “Adequate”:
  - Sensornetze, RFID-Chips etc. haben nicht genug Rechenleistung für starke Kryptographie und ausgefeilte Algorithmen
  - Angemessenheit im Bezug auf Bedrohungspotential
    - Temperaturdaten müssen nicht so stark verschlüsselt werden wie Kontoinformationen
- Zusammenspiel von Security mit Proximity und Locality
  - Daten, die sowieso nicht den Raum verlassen können, müssen ggf. nicht stark verschlüsselt werden





# Access and Recourse

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Zugriff auf die eigenen Daten auf eine Art und Weise, die mit den Prinzipien des Ubicomp vereinbar ist
- automatische Mechanismen zum Aufspüren von Datenmißbrauch
- 'gerichtsfeste' Nachweise von Datenverarbeitungs- und Kommunikationsvorgängen
  - wenn tatsächlich ein Mißbrauch vorgelegen hat, soll dieser nachweisbar und schadensersatzpflichtig sein





# Kritik

Einführung

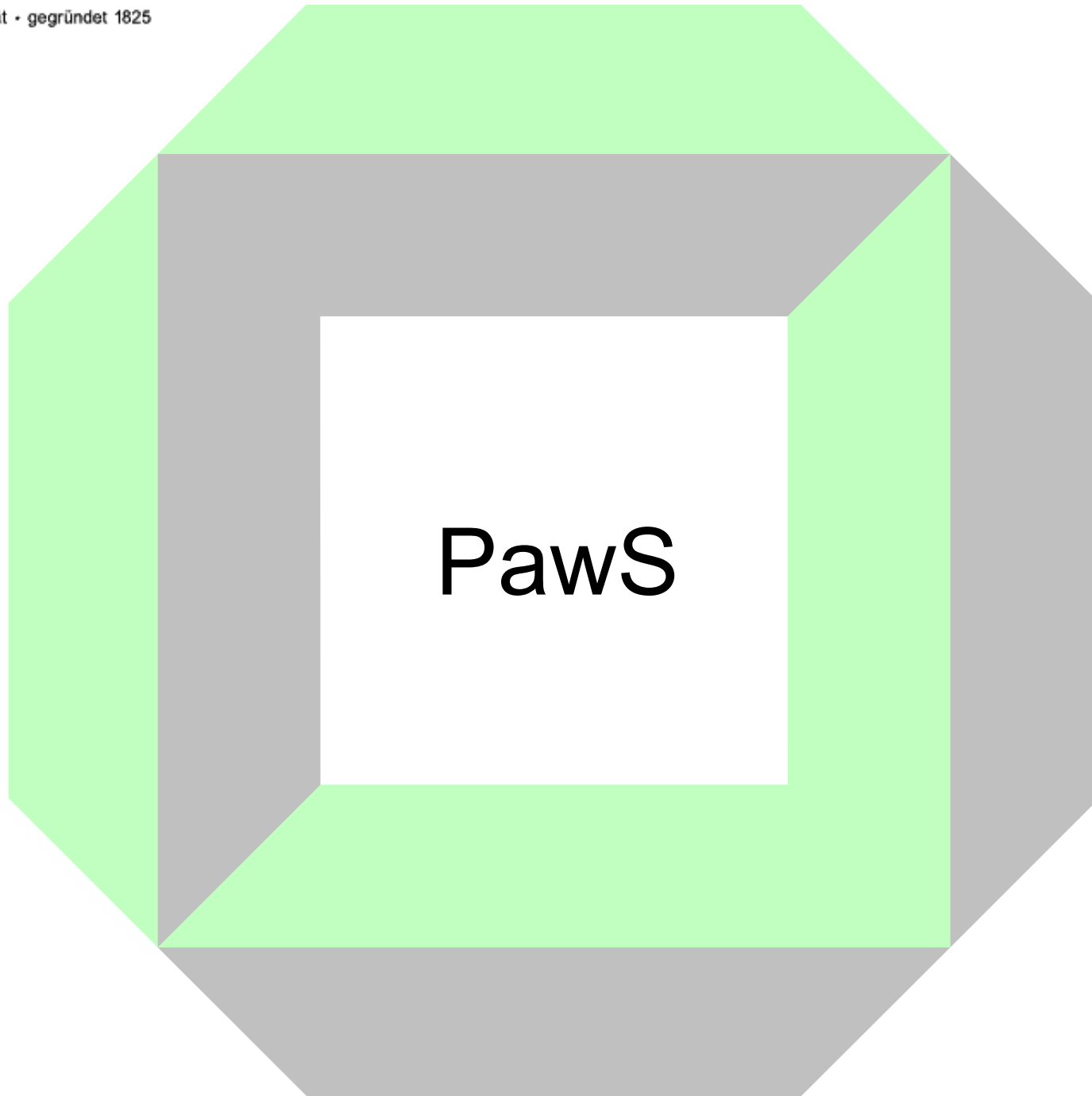
[DS-Prinzipien](#)

PawS

Confab

- die Prinzipien führen zu einem hochkomplexen System
  - Privacy abhängig von der Qualität der Implementierung von Privacy-Agenten?
  - Sinnvolle Konfiguration ohne tiefgehendes Technologieverständnis möglich?
- Daten sind unsichtbar
  - der Betroffene sieht nur die Anzeige seiner Geräte
  - wie überwachen, ob Datenschutz funktioniert?
- Beschränkt auf institutionelle Datenerhebung
  - Peer-to-Peer Modelle, Interaktionen von Freunden?
- Im folgenden: Ansätze, die diese Prinzipien umsetzen





PawS



# PawS

Einführung

DS-Prinzipien

PawS

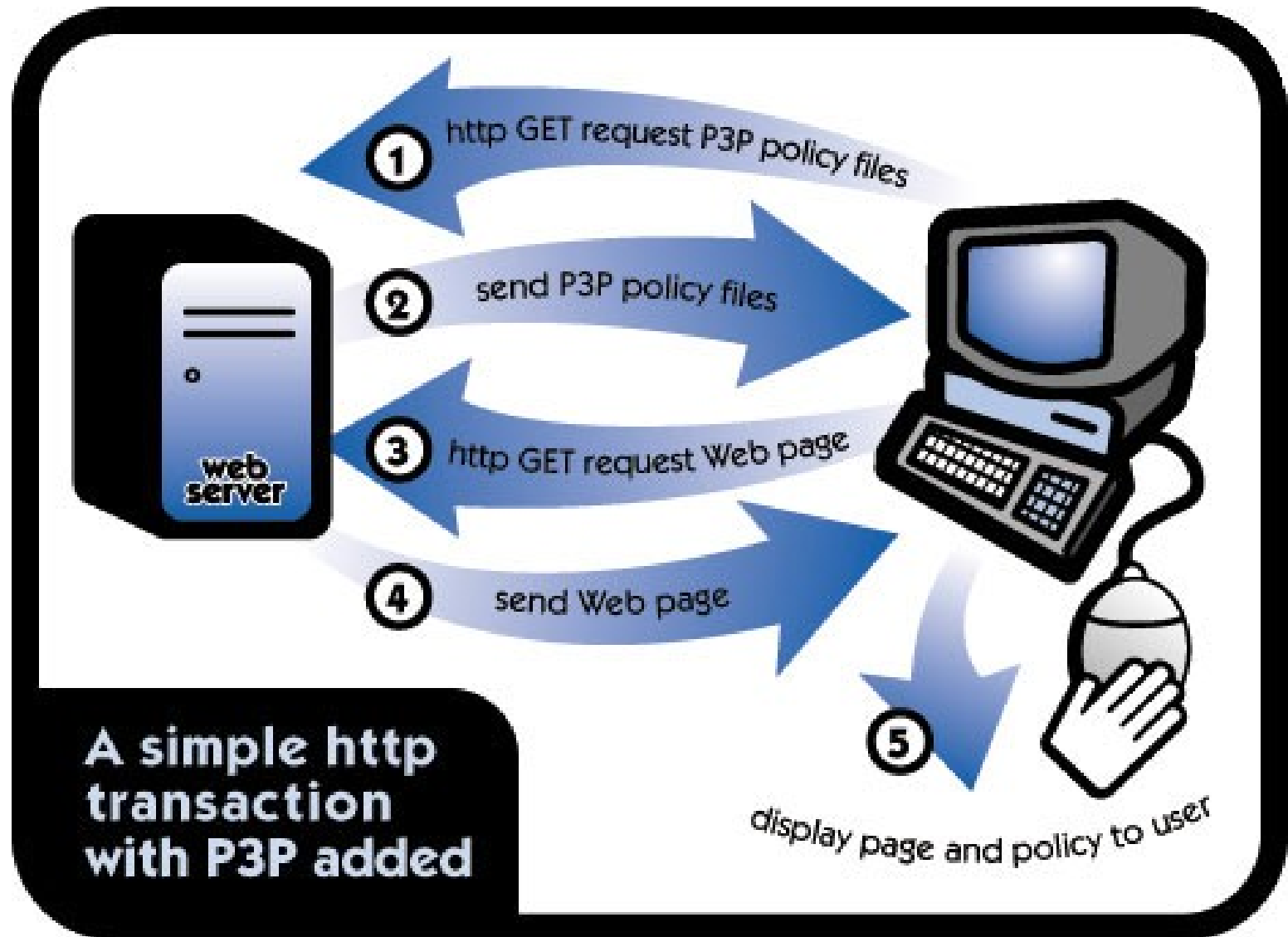
Confab

- PawS: a Privacy Awareness System [2]
    - Infrastruktur: Smart Items, Internet, Kommunikationsmedien (WLAN, Bluetooth etc.)
  - Idee: Umsetzung von P3P auf Smart Environments
    - Privacy Beacons melden Datenerhebungen
    - Nutzer trägt Privacy Assistant mit seinen Präferenzen bei sich
    - Geräte sind mit Service Proxies ausgestattet, die die Privacy Policies der Gerätebetreiber speichern
    - Privacy Proxies handeln anhand Nutzerpräferenzen aus, ob Datenerhebung stattfinden darf
- *Umsetzung von Notice, Choice and Consent, Proximity and Locality, Access and Recourse*



# Wiederholung: P3P

Einführung  
DS-Prinzipien  
PawS  
Confab

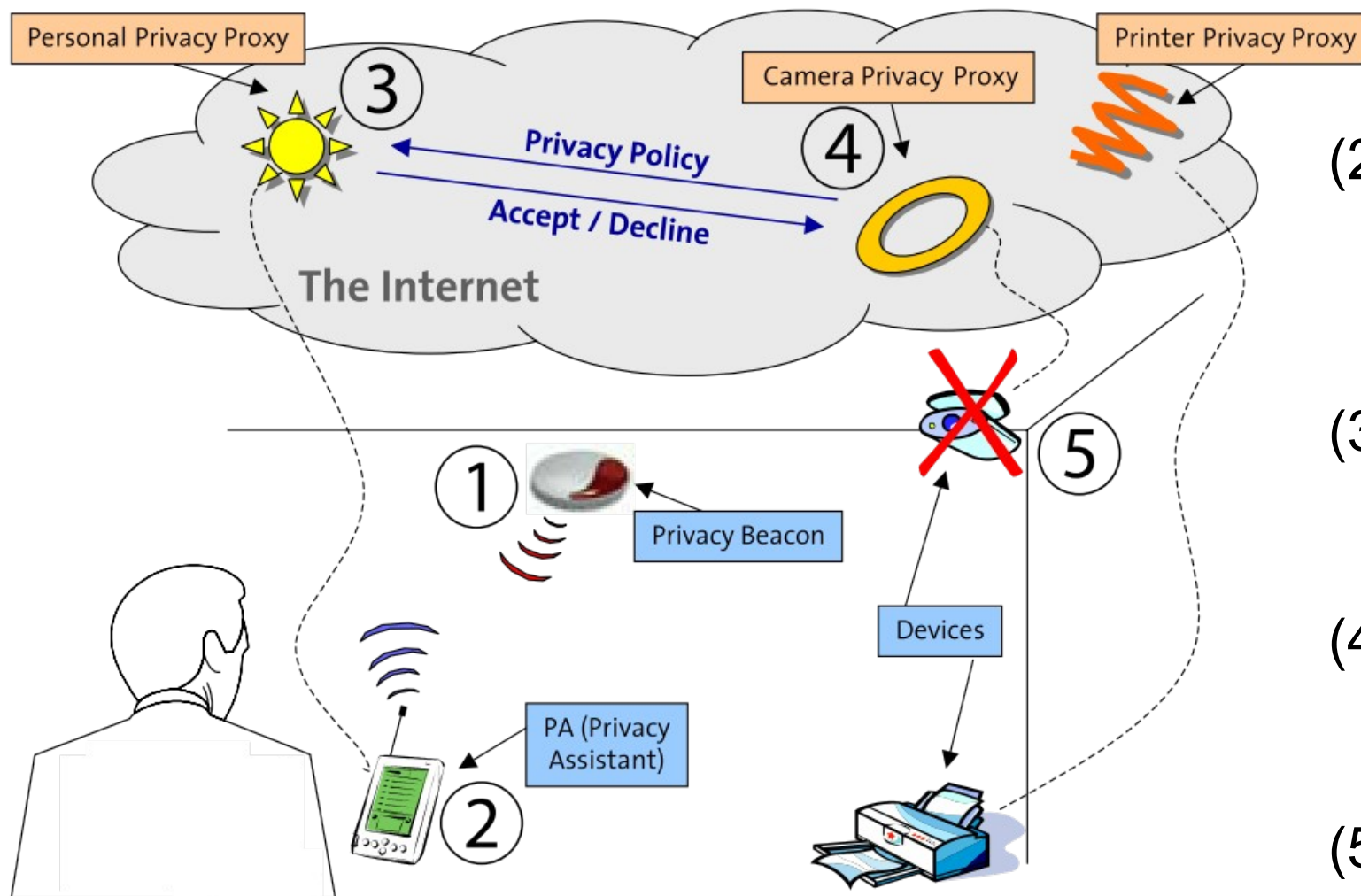


Quelle: <http://p3ptoolbox.org>

# Wiederholung: P3P Langformat

```
<POLICY name="forBrowsers"
discuri="http://www.catalogshop.example.com/PrivacyPracticeBrowsing.html">
<ENTITY><DATA-GROUP>
<DATA ref="#business.name">CatalogShop</DATA>
<DATA ref="#business.contact-info.postal.street">4000 Lincoln Ave.</DATA>
<DATA ref="#business.contact-info.postal.city">Birmingham</DATA>
<DATA ref="#business.contact-info.postal.stateprov">MI</DATA>
<DATA ref="#business.contact-info.postal.postalcode">48009</DATA>
<DATA ref="#business.contact-info.postal.country">USA</DATA>
</DATA-GROUP></ENTITY>
<DISPUTES-GROUP>
<DISPUTES resolution-type="independent"
service="http://www.PrivacySeal.example.org">
</DISPUTES>
</DISPUTES-GROUP>
<STATEMENT><br /> <PURPOSE><admin/><develop/></PURPOSE>
<RECIPIENT><ours/></RECIPIENT>
<RETENTION><stated-purpose/></RETENTION>
<DATA-GROUP>
<DATA ref="#dynamic.clickstream"/>
<DATA ref="#dynamic.http"/>
</DATA-GROUP>
</STATEMENT>
</POLICY>
```

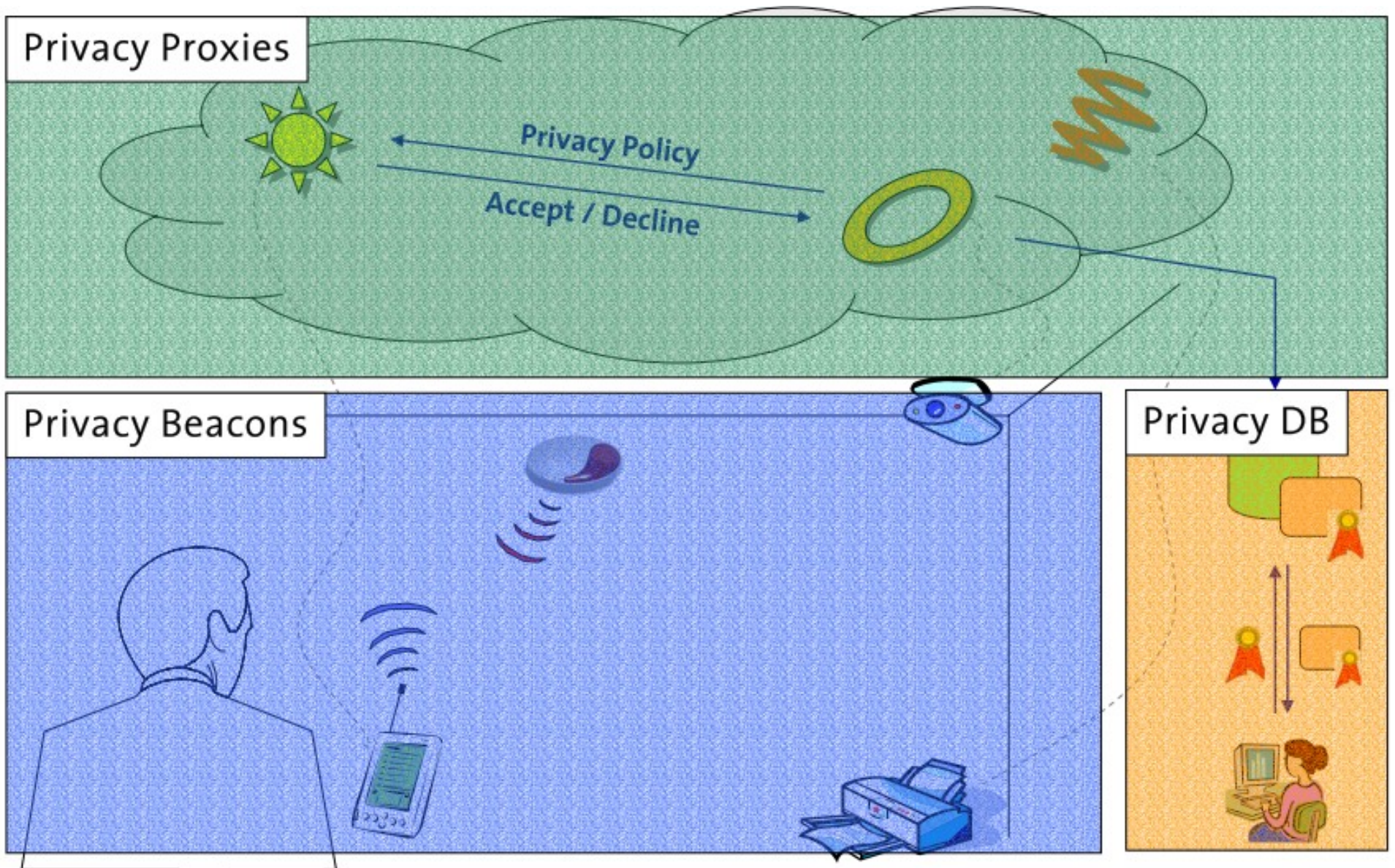
# Anwendungsszenario von PawS



- (1) Privacy Beacon meldet Erfassung.
- (2) Privacy Assistant sendet Nutzerpräferenzen an
- (3) Privacy Proxy, der Privacy Policies von
- (4) Service Proxies herunterlädt und anschließend
- (5) eine Kamera mit deaktiviert.

Quelle: [2]

# Bestandteile von Paws



Quelle: [2]



# Privacy Beacon

Einführung

DS-Prinzipien

PawS

Confab

- Kündigen sonst unbemerkte Datenerhebung
  - beschreibt die erhobenen Daten und den Erhebungszweck
  - sendet Adresse von maschinenlesbarer P3P-Policy mit UbiComp-Erweiterungen
- Zwei Arten des Announcements möglich
  - Aktives bekanntmachen
    - Funkbake, Infrarot etc.; Empfangsgerät beim Nutzer
  - Implizites bekanntmachen
    - Nutzer wird über Datenerhebung informiert, während er nach passenden Diensten in der Umgebung sucht
    - Bestandteil des Service Discovery-Protokolls





# Privacy Proxy

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Service Proxy
  - für jeden UbiComp-Dienst ist ein Proxy verantwortlich
  - speichert P3P-Policy
  - holt wenn nötig Einwilligung vom Personal Privacy Proxy ein
- Personal Privacy Proxy
  - für jeden Nutzer ist ein Proxy zuständig
  - handelt Parameter der Dienstnutzung und Datenerfassung im Namen des Nutzers mit den Service Proxies aus
    - automatisches generieren und löschen von Verträgen, Choice and Consent durch Softwareagenten
    - Basis: Präferenzen vom Privacy Assistant des Nutzers





# Privacy Database

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Speichert zwei Arten von Informationen:
  - alle persönlichen Daten des Nutzers
  - alle ausgehandelten Zustimmungen und Entscheidungen zwischen Personal Privacy Proxy und Service Proxy, P3P Policy Informationen
- Dadurch Überprüfbarkeit, ob sich der Service Provider an seine Policy hält oder gehalten hat (Recourse)
  - Agreement-ID für alle ausgehandelten “Verträge”
  - Daten mit unpassender Nutzung zurückhalten
  - Datenzugriffe vermerken





# Das Confab-Toolkit



# Das Confab-Toolkit

Einführung

DS-Prinzipien

PawS

Confab

- Toolkit für Privacy-sensitive Ubicomp-Anwendungen
- Auf folgende konkrete Anforderungen zugeschnitten:
  - klare Darstellung, wozu welche Daten gebraucht werden
  - Kontrolle und zum Feedback dazu, wer welche Informationen sehen kann oder gesehen hat
  - plausible Abstreitbarkeit (“weiße Lügen”; bin grade nicht da oder so etwas)
  - begrenzte Speicherdauer
  - dezentrale Steuerung
  - Sonderregelungen für Notfälle, in denen Privacy weniger wichtig ist
- *Abgesehen von der Notfallregelung zu den vorgestellten Prinzipien kompatibel*



# Confab-Architektur (1/3)

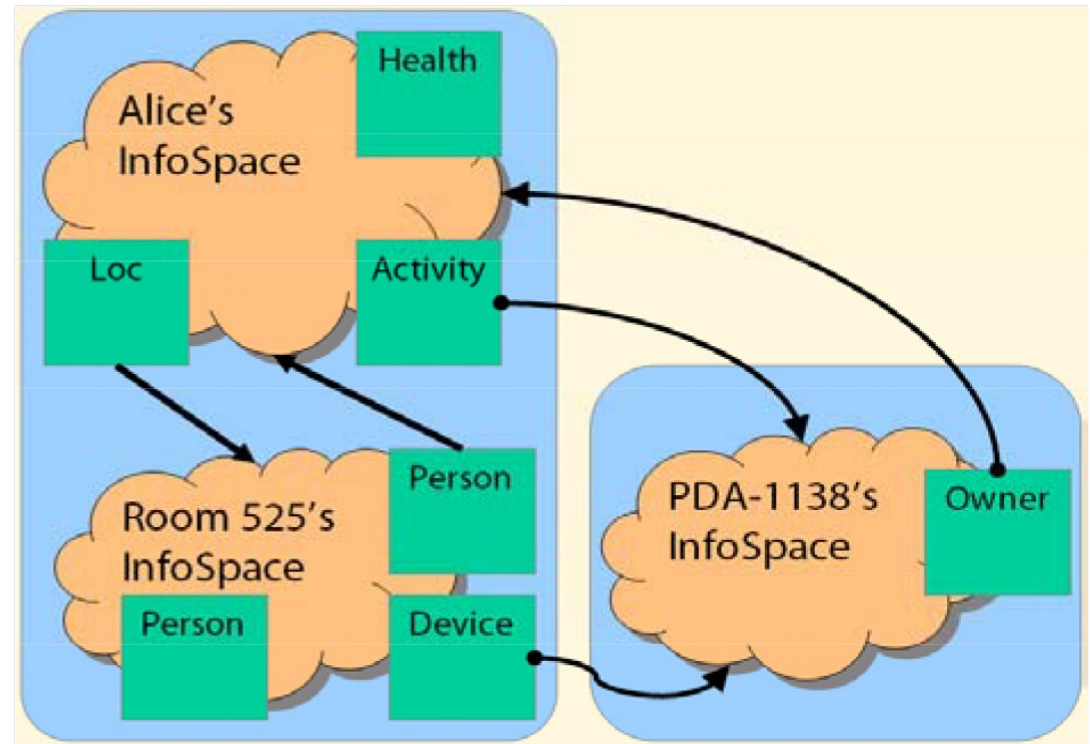
Einführung

DS-Prinzipien

PawS

Confab

- Persönliche InfoSpaces
  - jedem Nutzer sind ein oder mehrere InfoSpace zugeordnet, die seine persönlichen Daten enthalten
  - InfoSpace kann z.B. der pers. Rechner des Nutzers sein
  - Privacy-Regeln für Daten, die die InfoSpace verlassen



Quelle: [3]



# Confab-Architektur (2/3)

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Layermodell
  - Presentation
    - Nutzerschnittstelle für P3P, Operatoren
  - Infrastructure
    - Toolkit, Operatoren
  - Physical/Sensor
    - Datenquellen für Lokationsdaten, Umgebungsdaten, Nutzerinformationen



# Confab-Architektur (3/3)

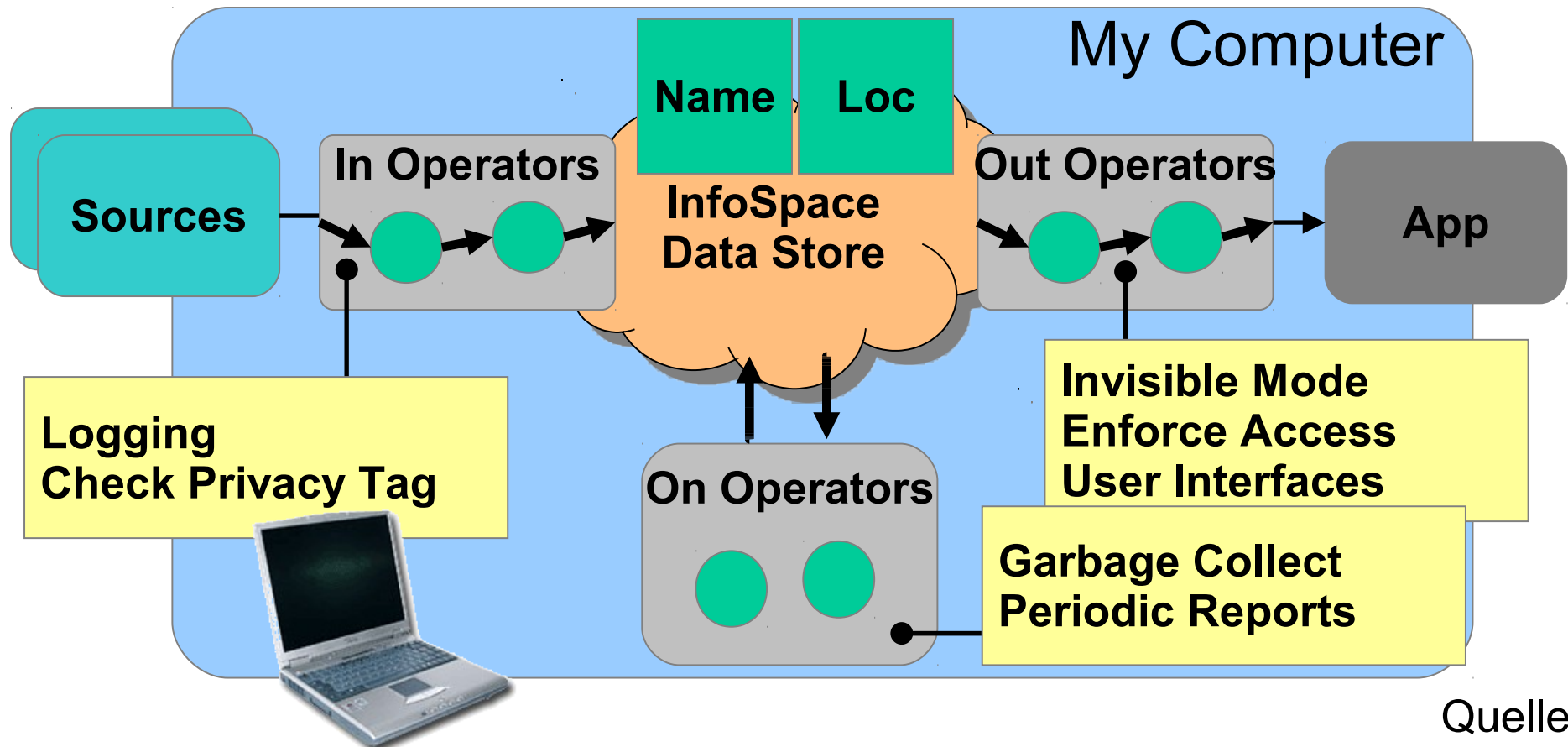
Einführung

DS-Prinzipien

PawS

Confab

- Ziel: So viele persönliche Daten wie möglich im pers. InfoSpace des Betroffenen speichern und verarbeiten
  - erlaubt direkte Kontrolle beim Umgang mit den Daten



Quelle: [3]



# Infrastructure Layer (1/2)

Einführung

DS-Prinzipien

PawS

[Confab](#)

- Operator-Typ **In**
  - Zugriffsregeln, Privacy-Tags, Benachrichtigungen zu eingehenden Informationen ausführen
- Operator-Typ **Out**
  - Zugriffsregeln, Privacy-Tags, Benachrichtigungen zu ausgehenden Informationen ausführen
  - Privacy-Tags hinzufügen
- Operator-Typ **On**
  - Daten verarbeiten, löschen
  - periodische Reports





## Infrastructure Layer (2/2)

[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Beispiel: Out-Operator “Flow Control”
  - Ziel: Informationen unterschiedlichen Nachfragern zur Verfügung stellen (oder auch nicht)
- Bedingungen
  - Age of data
  - Requestor Domain
  - Requestor ID
  - Requestor Location
  - Data Format
  - Data Type
  - Current Time
- Aktionen
  - Lower Precision
  - Set (fake value)
  - Invisible (no out data)
  - Interactive
  - Allow
  - Hide (data is removed)
  - Timeout (fake net load)
  - Deny (forbidden)

Quelle: [3]





# Presentation Layer (1/3)

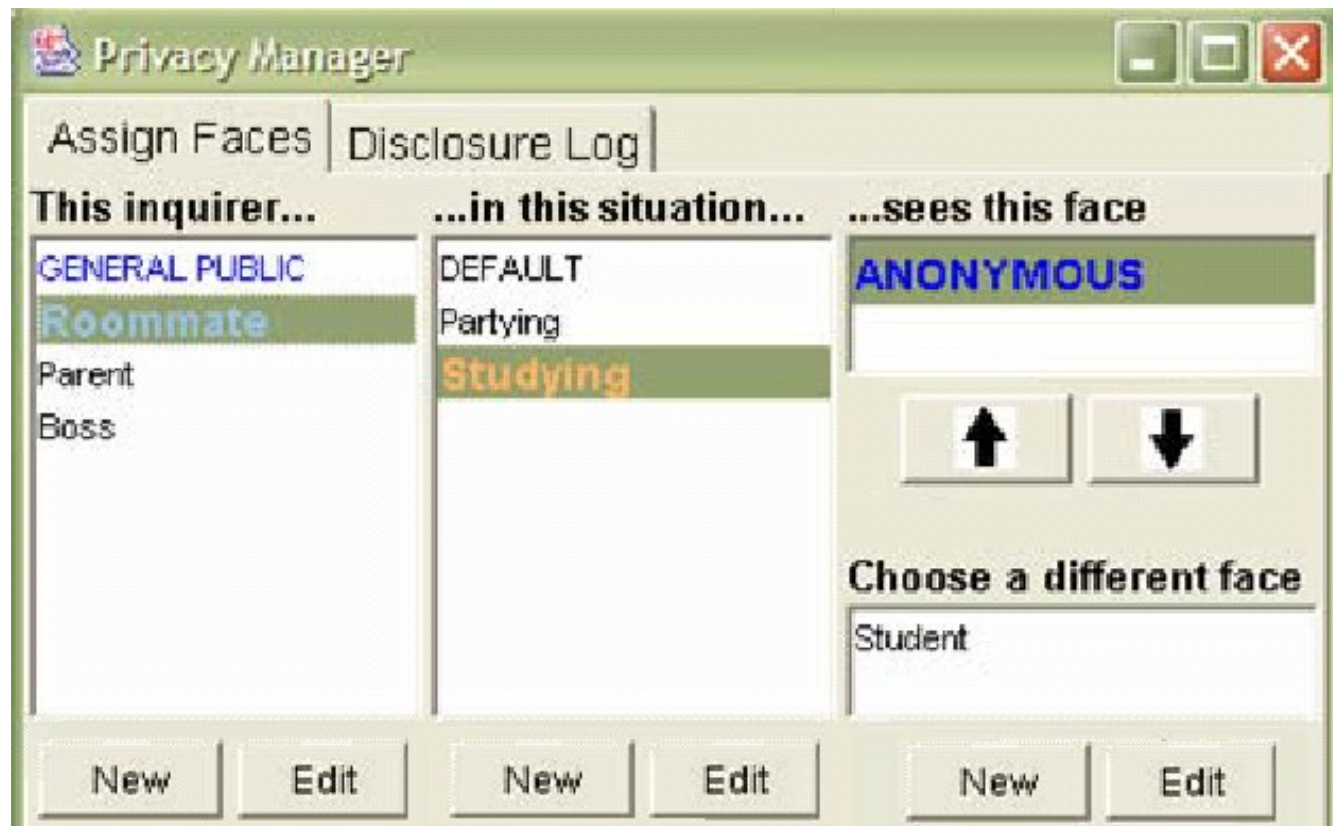
[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Beispiel: Interface für Flow Control für Bildinformationen (*vgl. vorangegangene Folie*)
  - Festlegen, wann und unter welchen Umständen welche Informationen weitergegeben werden



Quelle: [3]



## Presentation Layer (2/3)

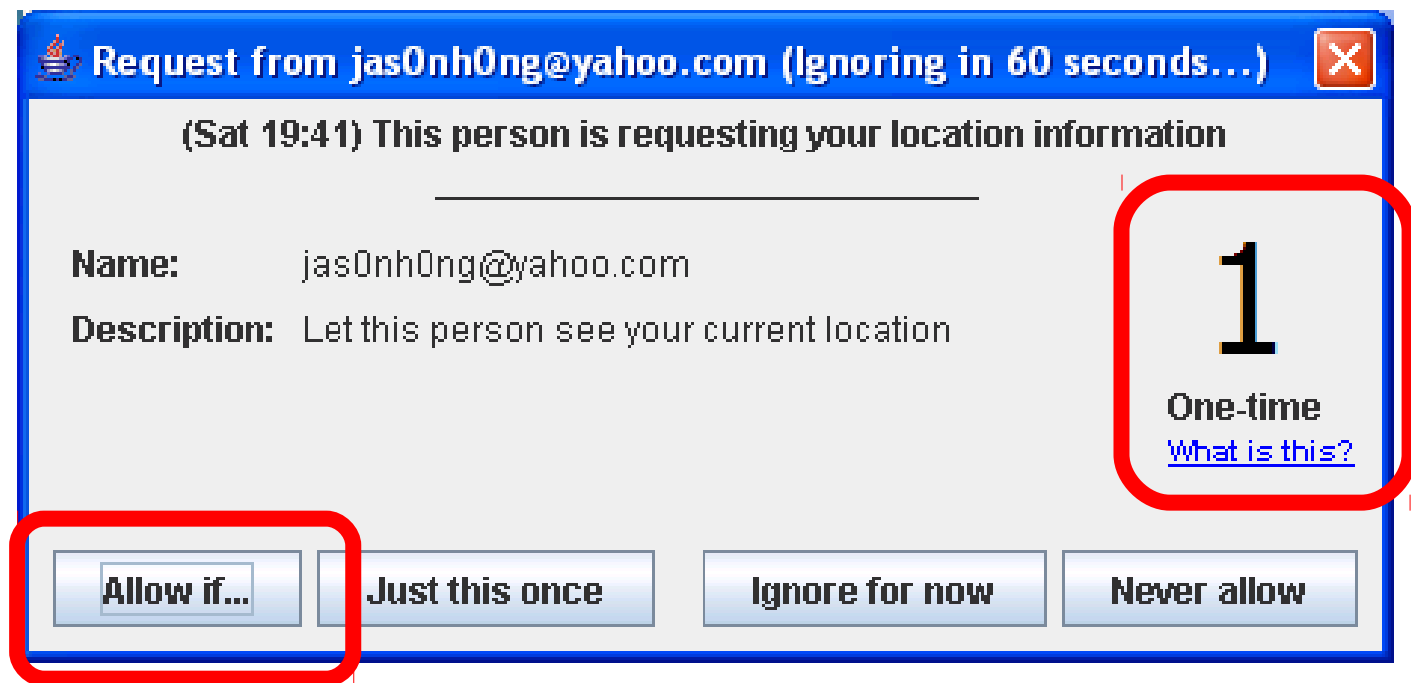
Einführung

DS-Prinzipien

PawS

[Confab](#)

- Beispiel: Benachrichtigung wenn andere auf Lokationsinformationen zugreifen wollen (pull)
  - Vorgabe ist “unknown” (plausible deniability)



Quelle: [3]



# Presentation Layer (3/3)

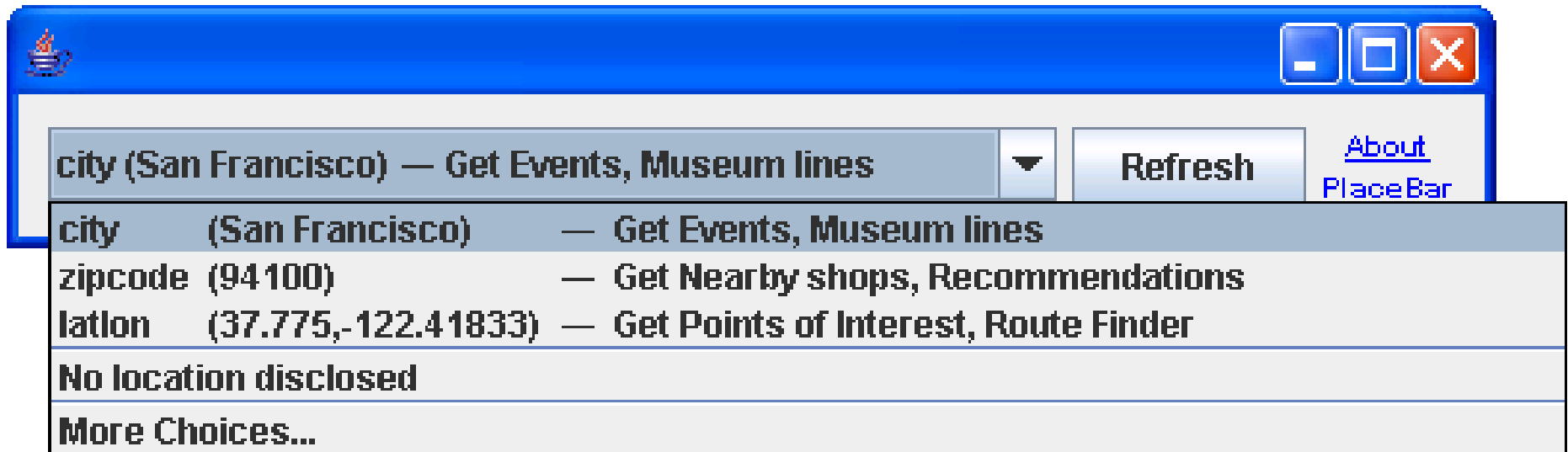
[Einführung](#)

[DS-Prinzipien](#)

[PawS](#)

[Confab](#)

- Beispiel: Aushandeln vom Detailgrad weiterzugebender Informationen
  - Detailgrad “Stadt”: Dienst kann Events oder Museen empfehlen
  - Detailgrad “exakte Koordinaten”: Dienst kann Routen berechnen oder POI anzeigen



Quelle: [3]





# Privacy in Confab

Einführung

DS-Prinzipien

PawS

Confab

- Defaultwert für alle Daten: UNKNOWN
  - plausible Abstreitbarkeit
- Zugriff nur auf explizite Zustimmung des Nutzers
- Alle Daten können mit Privacy Tags versehen sein
  - DRM für private Informationen  
*siehe nächste Folie*





# Privacy Tags

Einführung

DS-Prinzipien

PawS

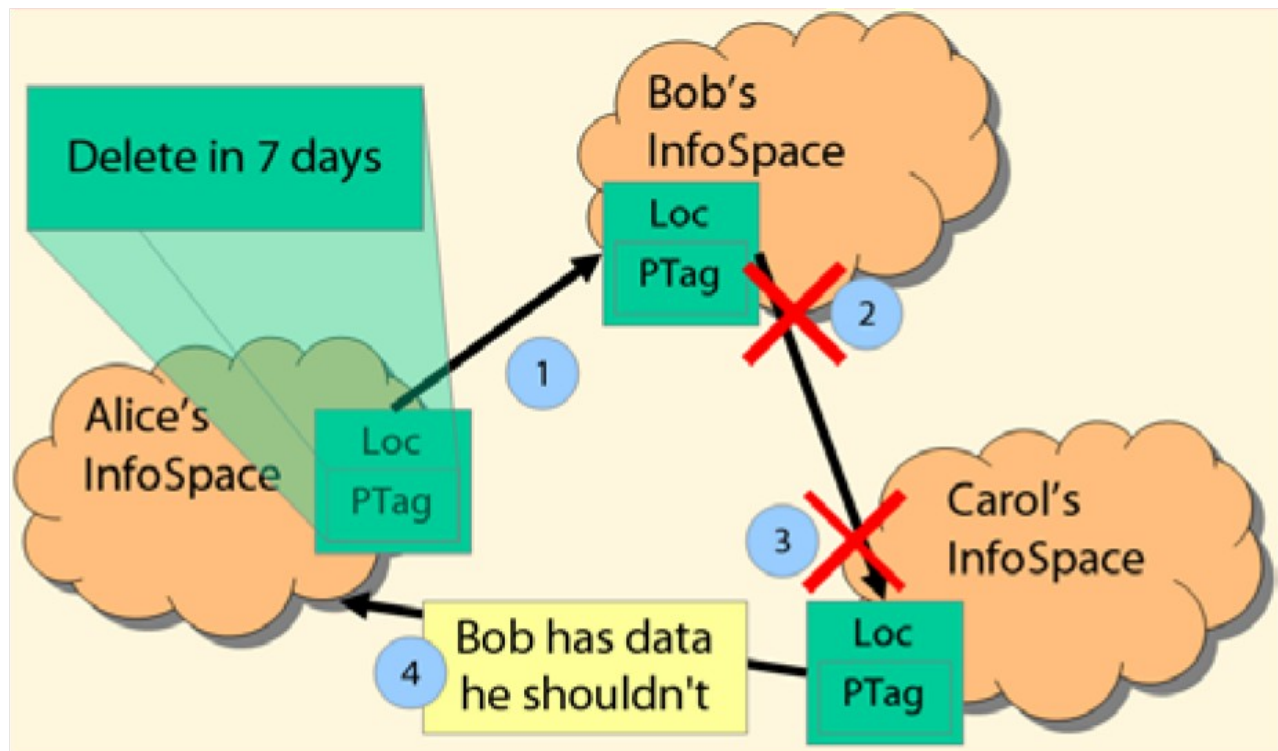
[Confab](#)

- Privacy Tag beschreibt, wie mit den Daten zu verfahren ist, wenn diese sich außerhalb des Computers des Anwenders befinden
  - *Time to Live*; Lebenszeit
  - *MaxNumSightings*; ob ältere Versionen der Daten aufbewahrt werden dürfen (z.B. nicht nur die aktuelle Nutzerposition, sondern sein Bewegungsprofil)
  - *Notify*; wann der Nutzer zu benachrichtigen ist
  - *GarbageCollect*; unter welchen Umständen Daten zu löschen sind (z.B. wenn der Nutzer ein Gebäude verlässt)



# Enforcement durch Privacy Tags

- (1) Alice: Lokationsdaten mit Bob austauschen,  
*Privacy-Tag: Informationen in 7 Tagen löschen, anderenfalls Benachrichtigung*
- (2) Bob's InfoSpace: *unabsichtliche* Weitergabe nach 7 Tagen verhindern, Daten löschen
- (3) Carol's InfoSpace: bemerkt, dass die von Bob erhaltenen Daten hätten gelöscht werden müssen
- (4) Carol's InfoSpace: benachrichtigt Alice





# Abschluss Ubicomp. Teil 2



# Zusammenfassung

- Datenschutz in Smart Environments ist Kompromiss
  - Verzicht auf Datenerhebung ist keine Option  
→ Dienste funktionieren dann nicht
  - Verzicht auf Dienstnutzung ist keine Option  
→ Dienste sind *nützlich*
  - **Principle of Minimum Asymmetry**
- Zwei Ansätze
  - PawS
  - Confab-Toolkit
- Problematisch: hochkomplexe Systeme, schwer zu kontrollieren





# Literatur

- [1] Marc Langheinrich, *Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems*, Ubicomp 2001
- [2] Marc Langheinrich, *A Privacy Awareness System for Ubiquitous Computing Environments*, Ubicomp 2002
- [3] Jason Hong, James Landay, *An Architecture for Privacy-Sensitive Ubiquitous Computing*, MobiSys 2004

