

# Datenschutz- und Sicherheitsaspekte von Ortsinformationssystemen

Anna-Nina Simonetto  
Fachseminar Verteilte Systeme  
Betreuer: Marc Langheinrich

# Übersicht

1. Was bedeutet Location Privacy?
2. Warum sind Ortsinformationen besonders schützenswert?
3. Worin unterscheiden sich ortsbasierte Dienste und welche Lösungsansätze existieren für diese?

# Location *Privacy*



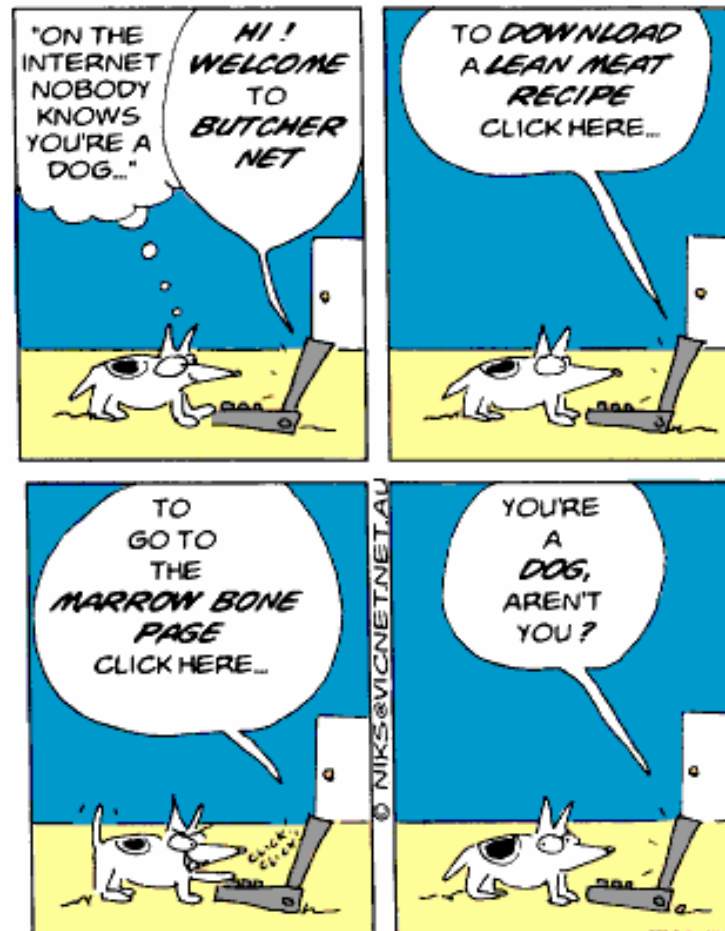
Verhindern, dass *der Falsche* aktuelle oder vergangene Ortsinformationen erfährt.

Ansonsten kann es vorkommen, dass

- Missbrauch stattfindet
- Misstrauen in eine Anwendung ihren Nutzen überwiegt

# Warum ist der Ort schützenswert?

- Die Orte, an denen man sich aufhält, lassen Rückschlüsse zu:
  - (Soziale, ethische, ...) Identität  
→ Reality Mining
  - Aktuelle Aktivität  
→ Reno



# Das Problem?

- Jemand findet heraus, dass ich gestern um 15.30 im IFW-Gebäude war.
- Jemand findet heraus, wo ich zu jeder Minute der letzten zwei Wochen gewesen bin.
  - Dienste, welche mit Pervasive Computing möglich werden, sind teilweise auf solche Ortsinformationen angewiesen.

# Bedrohungen

- Kommerzielle:
  - Ortsbasierter Spam
  - Data Miner, die persönliche Profile erstellen
- Kriminelle:
  - Vereinfachung von Stalking oder anderen physischen Attacken
- „Unannehmlichkeiten“:
  - Streit, Misstrauen, Vertrauensverlust
  - Rechtliche Probleme (Arbeitsrecht, ...)

# Das ideale Ziel

- Anonymes Benutzen von ortsbasierten Diensten
  - Ist nicht für jeden Dienst möglich
  - Annahme: Anonyme Kommunikation möglich (abhörsicher etc.)

# Ortsbasierte Dienste: 3 Klassen

1. „Sobald du an einer Starbucks-Filiale vorbeikommst, informieren wir dich über neue Produkte.“
2. „Wenn du fünf deiner Lieblingskaffees bei uns gekauft hast, ist der sechste Kaffee gratis.“
3. „Wenn du dich in einem Starbucks aufhältst, informieren wir alle deine Freunde, dass du hier bist.“



# Ortsbasierte Dienste: 3 Klassen

1. „Sobald du an einer Starbucks-Filiale vorbeikommst, informieren wir dich über neue Produkte.“
2. „Wenn du fünf deiner Lieblingskaffees bei uns gekauft hast, ist der sechste Kaffee gratis.“
3. „Wenn du dich in einem Starbucks aufhältst, informieren wir alle deine Freunde, dass du hier bist.“

# 1. Anonyme Dienste

- Dienste jedem in einer bestimmten Region anbieten
  - Durch Auslösen eines Infrarot-Sensors
  - Durch Broadcasten der Nachrichten
  - ...
- Spam verhindern?

# Selbstpositionierung

→ Finde selber heraus, wo ich bin.

- Cricket

- Ortsinformationen über Beacons, mobile Geräte agieren als Listeners.

- GPS

- Zum Beispiel in Kombination mit einer CD auf der alle Starbucks-Filialen der Region eingetragen sind.

# Grenzen der Selbstpositionierung

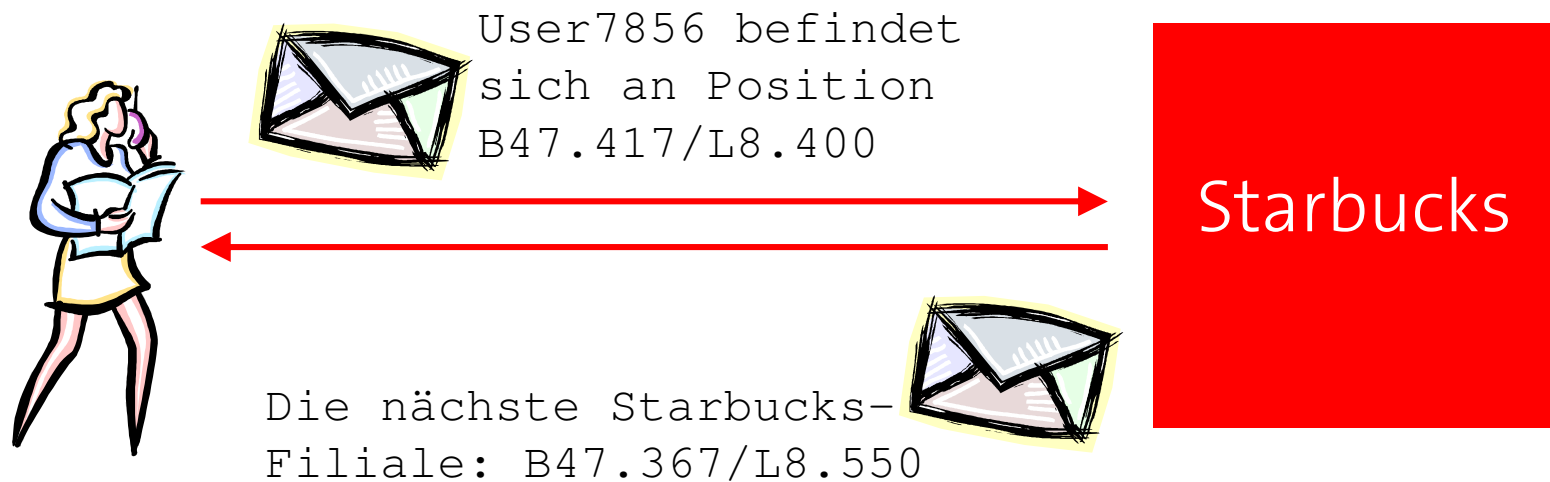
- GPS + CD: Statisch!
  - „Wo befindet sich die nächste Starbucks-Filiale?“
  - „In welcher Starbucks-Filiale habe ich im Moment die kürzeste Wartezeit?“

# Ortsbasierte Dienste: 3 Klassen

1. „Sobald du an einer Starbucks-Filiale vorbeikommst, informieren wir dich über neue Produkte.“
2. „Wenn du fünf deiner Lieblingskaffees bei uns gekauft hast, ist der sechste Kaffee gratis.“
3. „Wenn du dich in einem Starbucks aufhältst, informieren wir alle deine Freunde, dass du hier bist.“

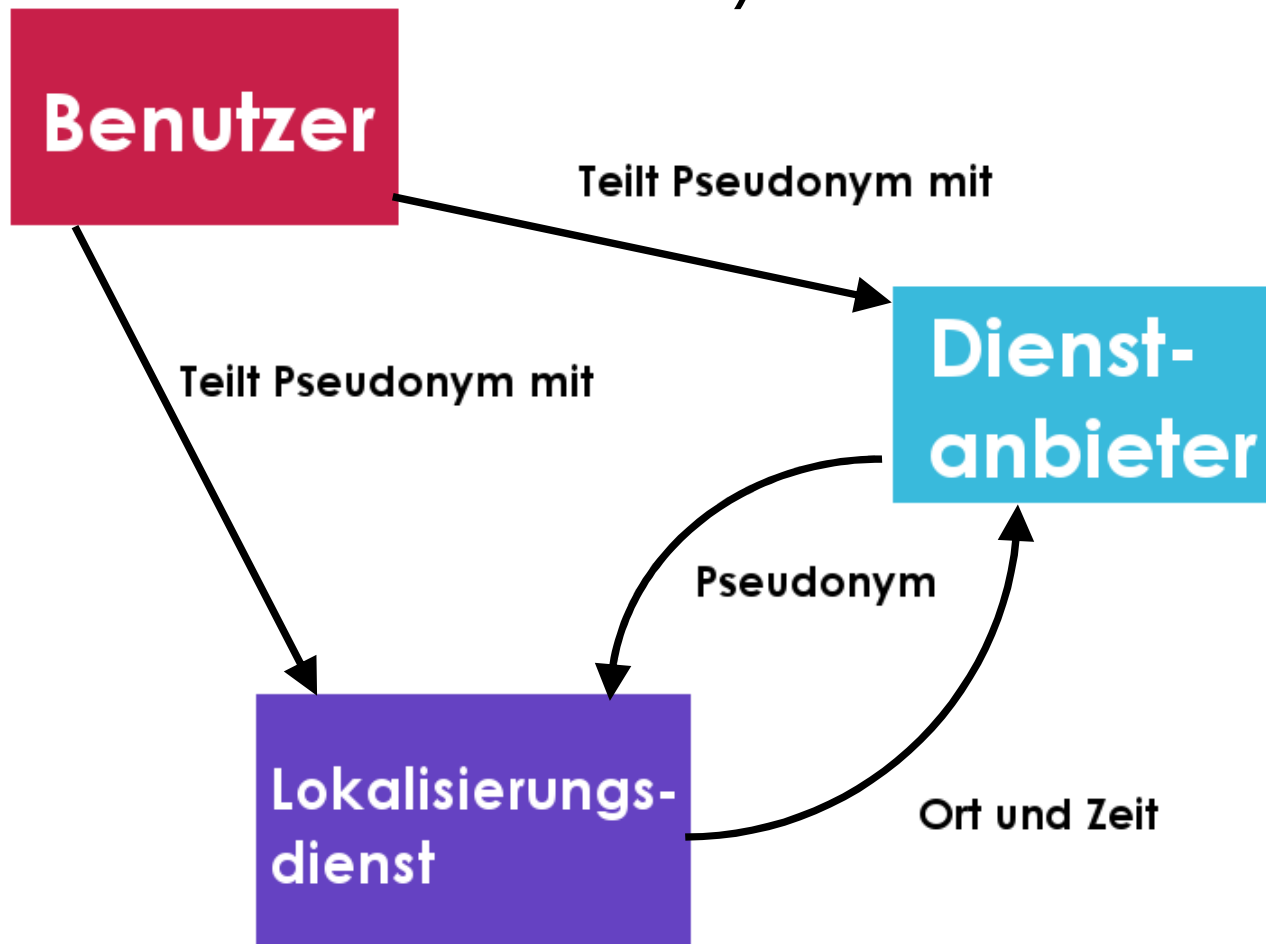
## 2. Pseudonyme Dienste

- Idee: Verwende zur Kommunikation ein Pseudonym



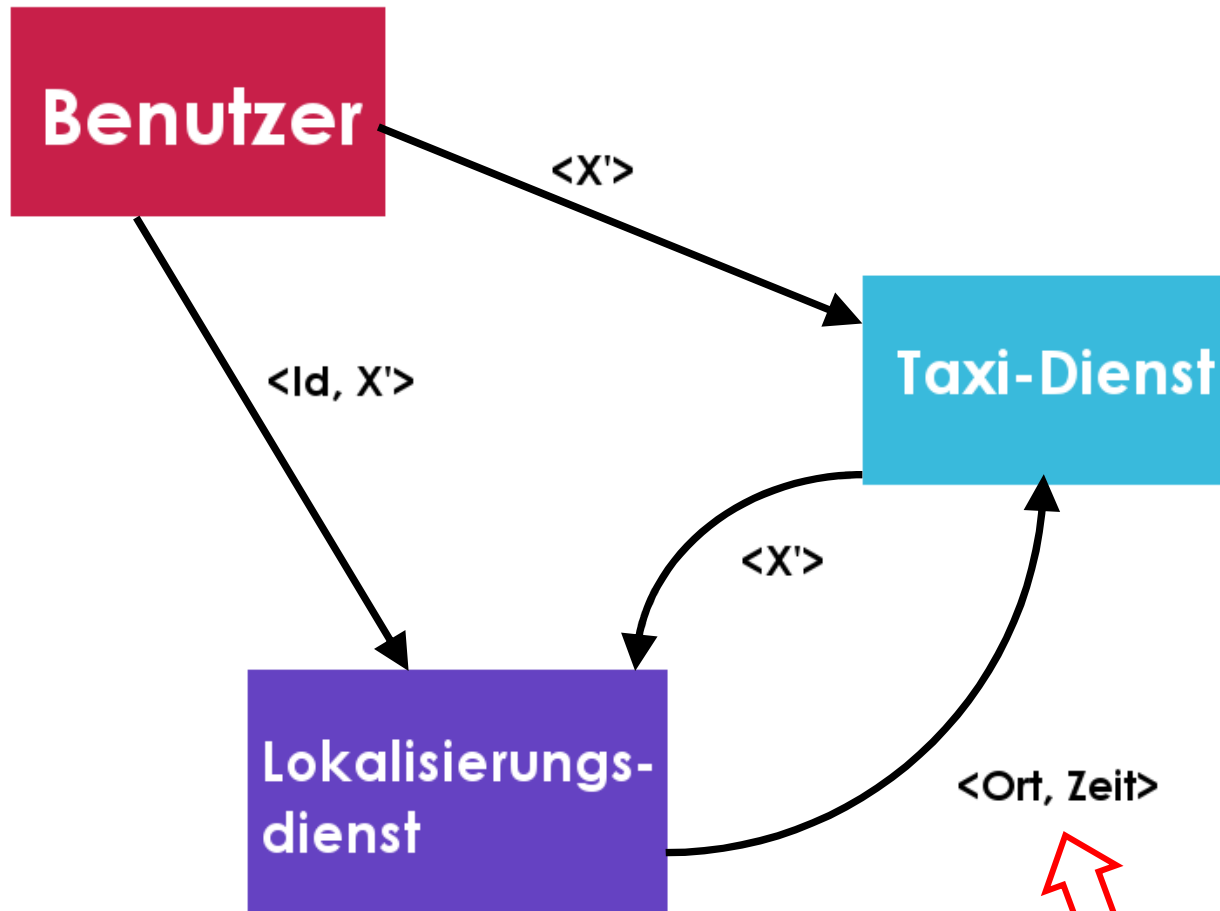
Pseudonymisiert

# Pseudonyme und Dienstleistungsverträge (T. Rodden et al.)



Pseudonymisiert

# Ablauf: Taxi-Dienst benutzen



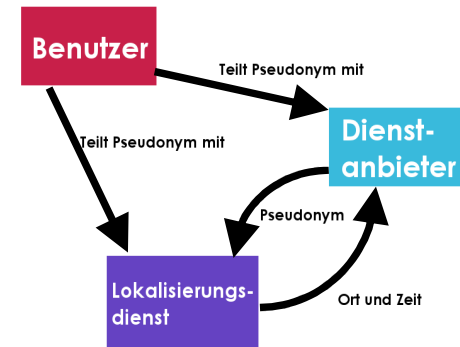
Pseudonymisiert

Oder: <user not found>



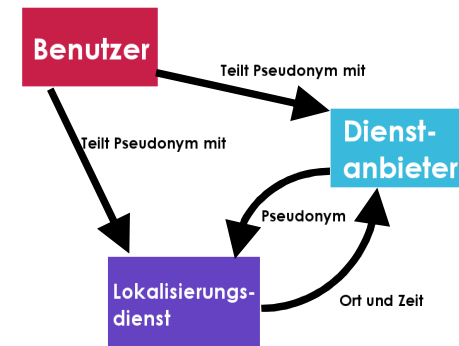
# Funktionsweise (I)

- Dienstleistungsvertrag: Kenntnis des aktiven Pseudonyms.
- Aktive Pseudonyme werden beim (vertrauenswürdigen) Lokalisierungsdienst registriert.
- Wechsel des Pseudonyms kündigt diesen Vertrag.



# Funktionsweise (II)

- Lokalisierungsdienst speichert Tripel:  
 $\langle X', \text{Zeit}, \text{Ort} \rangle$



- Zusätzlich werden die Pseudonyme auf dem Lokalisierungsdienst nach Dienstanbieter verschlüsselt abgelegt:  
 $\langle \text{Taxi-Dienst}, \text{ENC}(K_{\text{Taxi-Dienst}}, X') \rangle$ 
  - Pseudonyme direkt beim Lokalisierungsdienst updaten!

Pseudonymisiert

# Vorteile / Herausforderungen

- Man muss sich zu jederzeit nur die momentan berechtigten Dienstanbieter merken.
- Die Kontrolle hat der Benutzer!

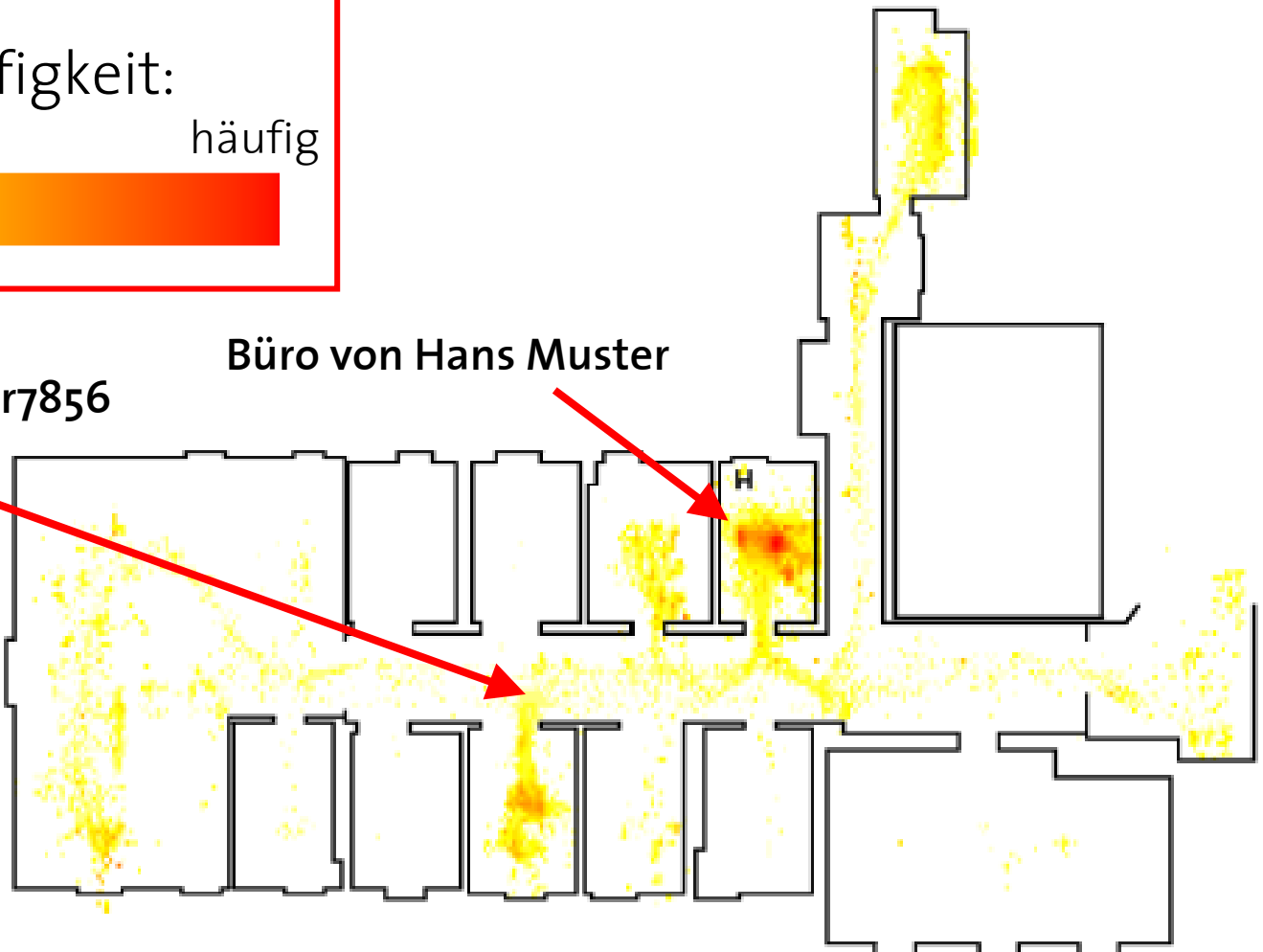
→ Statische Pseudonyme?

# Das Problem mit statischen Pseudonymen



Location Trace von User7856

Büro von Hans Muster



Pseudonymisiert

# Pseudonyme wechseln

Logfile auf Lokalisierungsdienst-Server 123:

<b>Position (Meter)</b>	<b>Zeit (Sekunden)</b>	<b>Benutzer</b>
0 / 5	t0 = 0	user1234
0.36 / 5	t1 = 0.25	user1234
0.73 / 5	t2 = 0.5	user8976
1.09 / 5	t3 = 0.75	user8976
1.45 / 5	t4 = 1	user3378

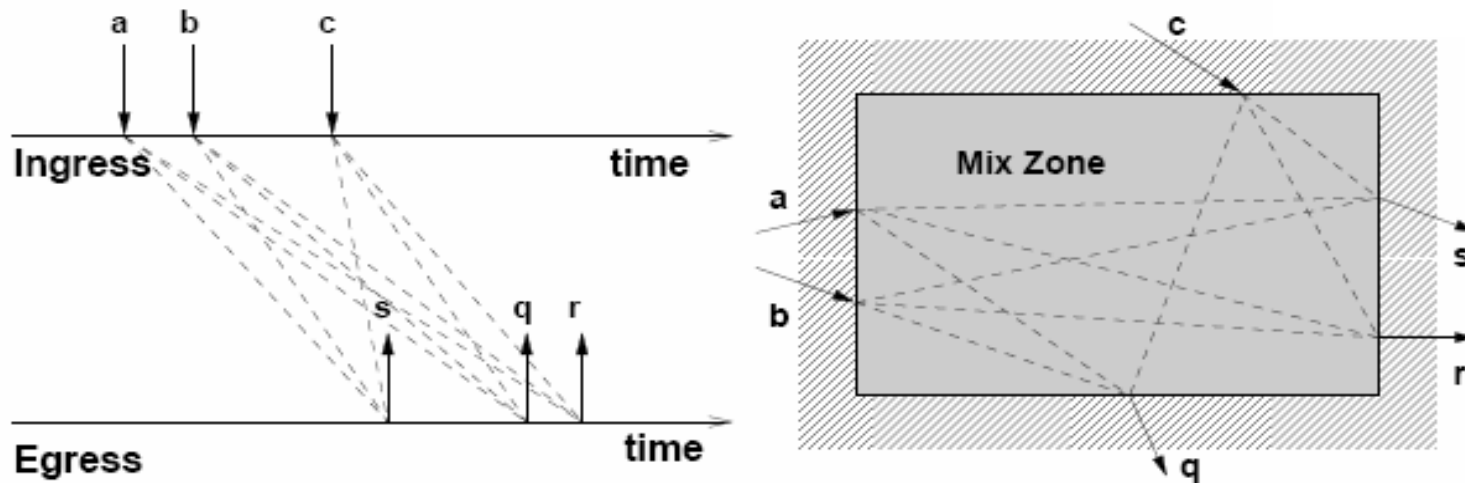
Pseudonymisiert

# Lösung: Mix-Zonen (Beresford & Stajano)

- Für Pseudonym-Wechsel begeben wir uns in eine Mix-Zone.
  - Räumliches Gebiet in dem nur Benutzer sind, die keinen ortsbasierten Dienst abonniert haben.
  - Keine Übertragung von Ortsinformationen, keine Logfiles.
  - Lokalisierungsdienst nicht mehr notwendigerweise vertrauenswürdig.

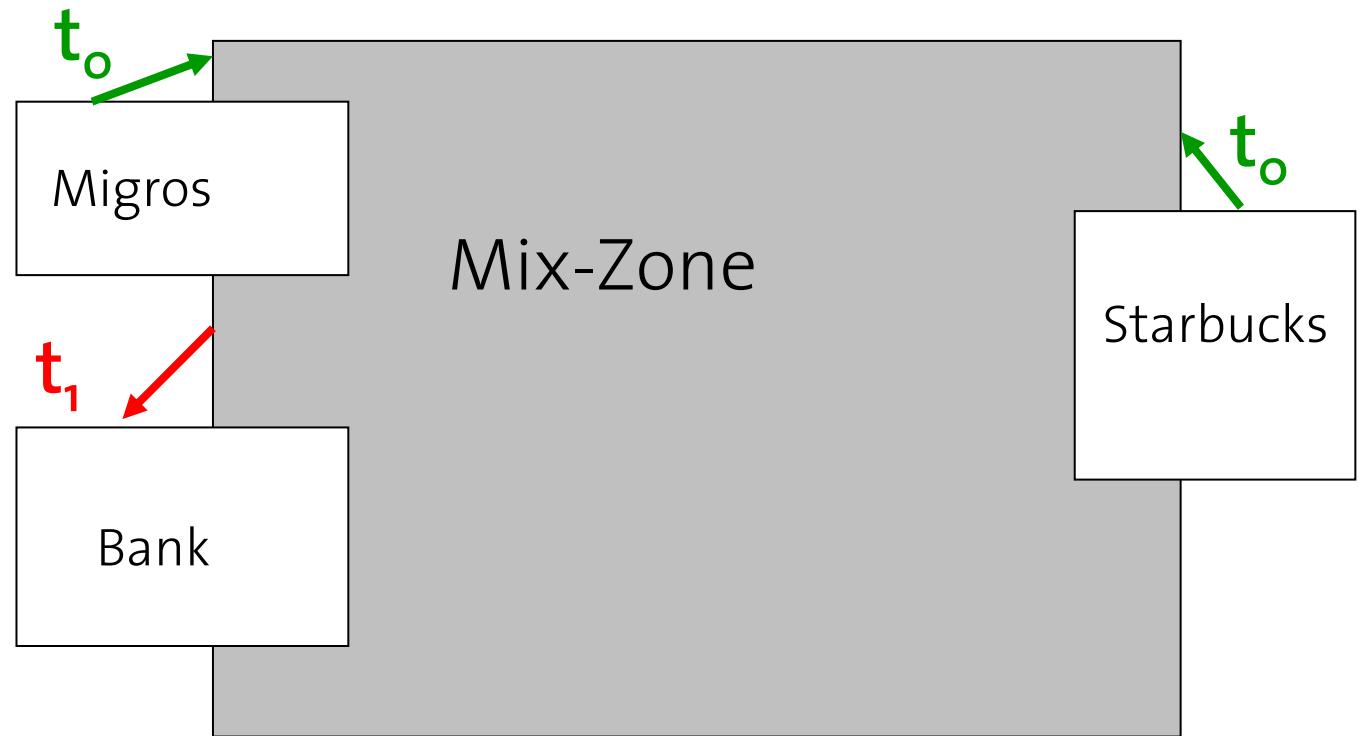
# Sicht eines Angreifers

- Wer ging wohin?



Pseudonymisiert

# Probleme von Mix-Zonen?



<b>Position</b>	<b>Zeit (Sekunden)</b>	<b>Benutzer</b>
<Starbucks, exit>	$t_0 = 0$	user1234
<Migros, exit>	$t_0 = 0$	user8976
<Bank, entry>	$t_1 = 5$	user3378

Pseudonymisiert

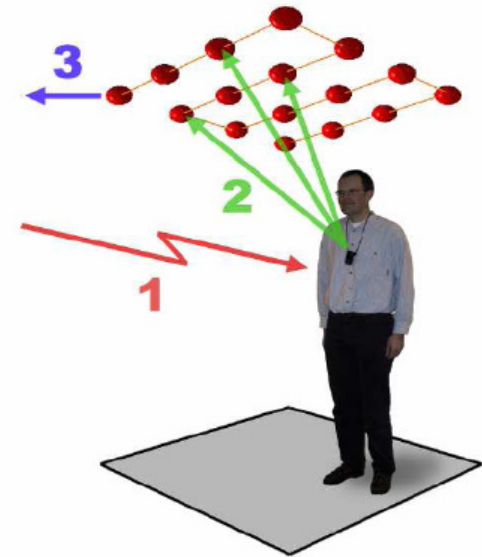


# Güte einer Mix-Zone

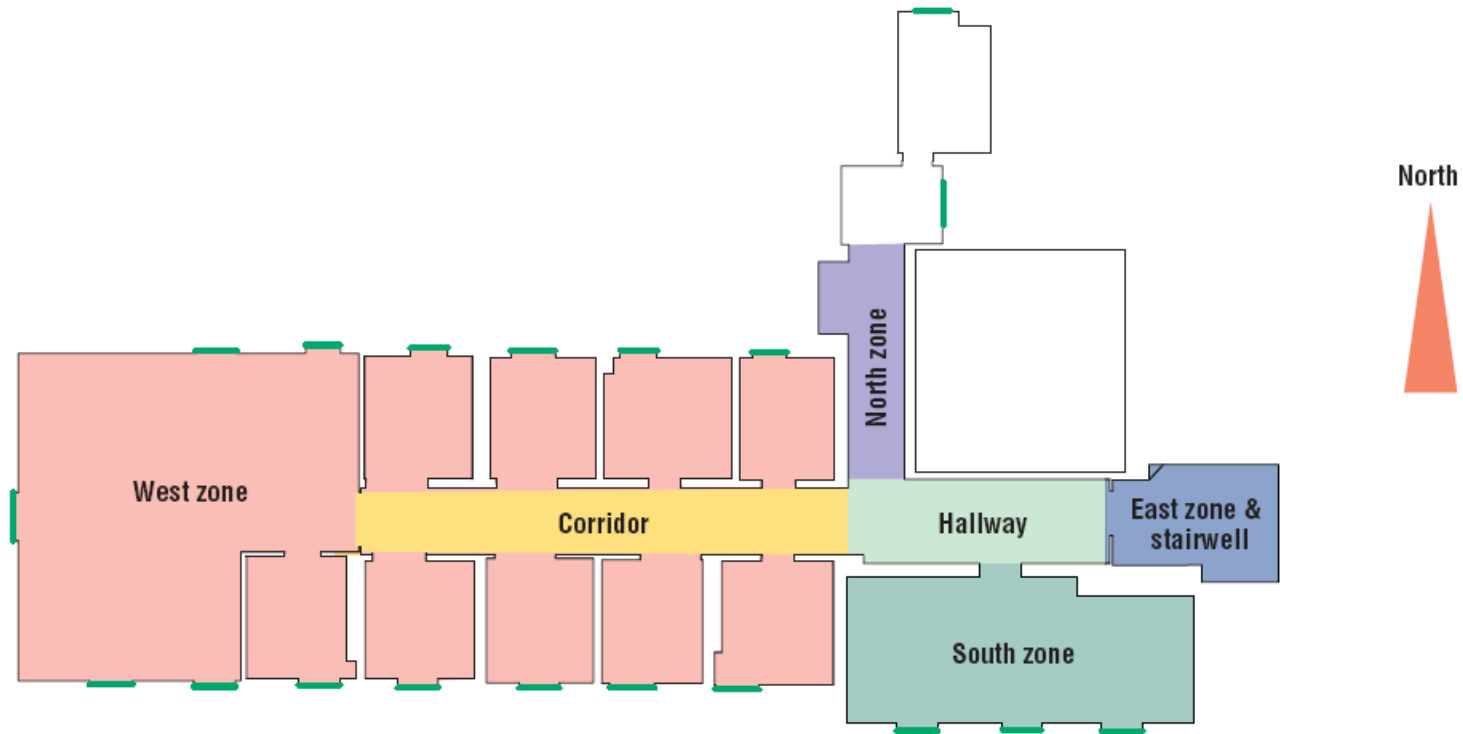
- Je mehr Benutzer sich in einer Mix-Zone aufhalten, desto anonymmer ist man.
- Man spricht von  $k$ -Anonymität, wenn eine Person von mindestens  $k-1$  anderen nicht unterscheidbar ist („*anonymity set*“)

# Mix-Zonen Experiment

- AT&T Labs Cambridge
- Lokalisierung: *Active Bats*
  - *Bats* emittieren Ultraschall-Signal an Gitter von Sensoren an der Decke
  - In 95% aller Fälle auf 3 cm genau
  - Ortsinformation wird 10-mal pro Sekunde aktualisiert
- Es wurden während 2 Wochen Ortsinformationen aller Forscher aufgenommen.



# Mix-Zonen der AT&T Labs



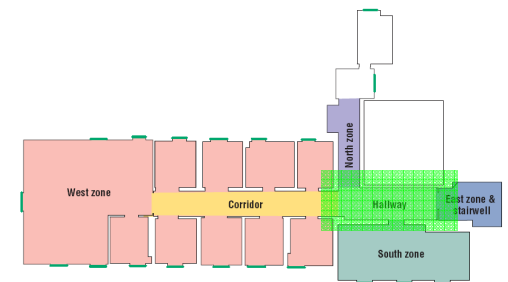
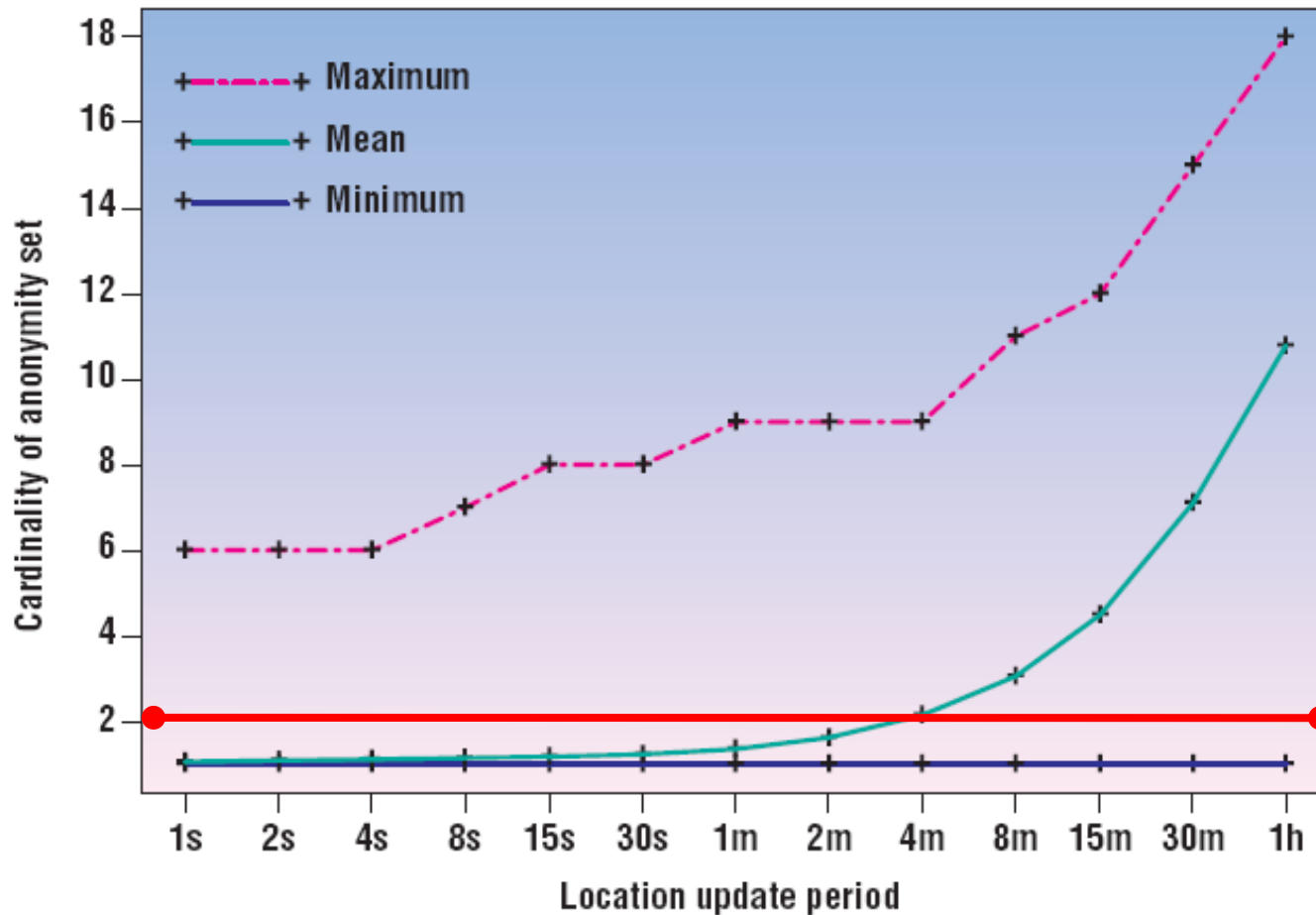
$z_1$ : Hallway

$z_2$ : Corridor + Hallway,

$z_3$ : Hallway, Corridor + Stairwell (auf 3 Stockwerken)

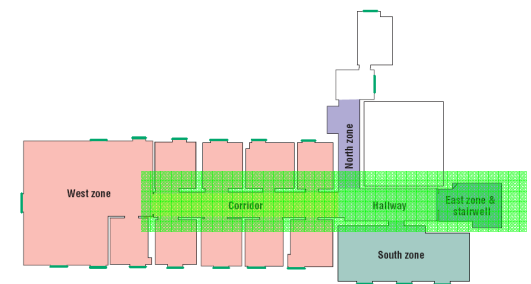
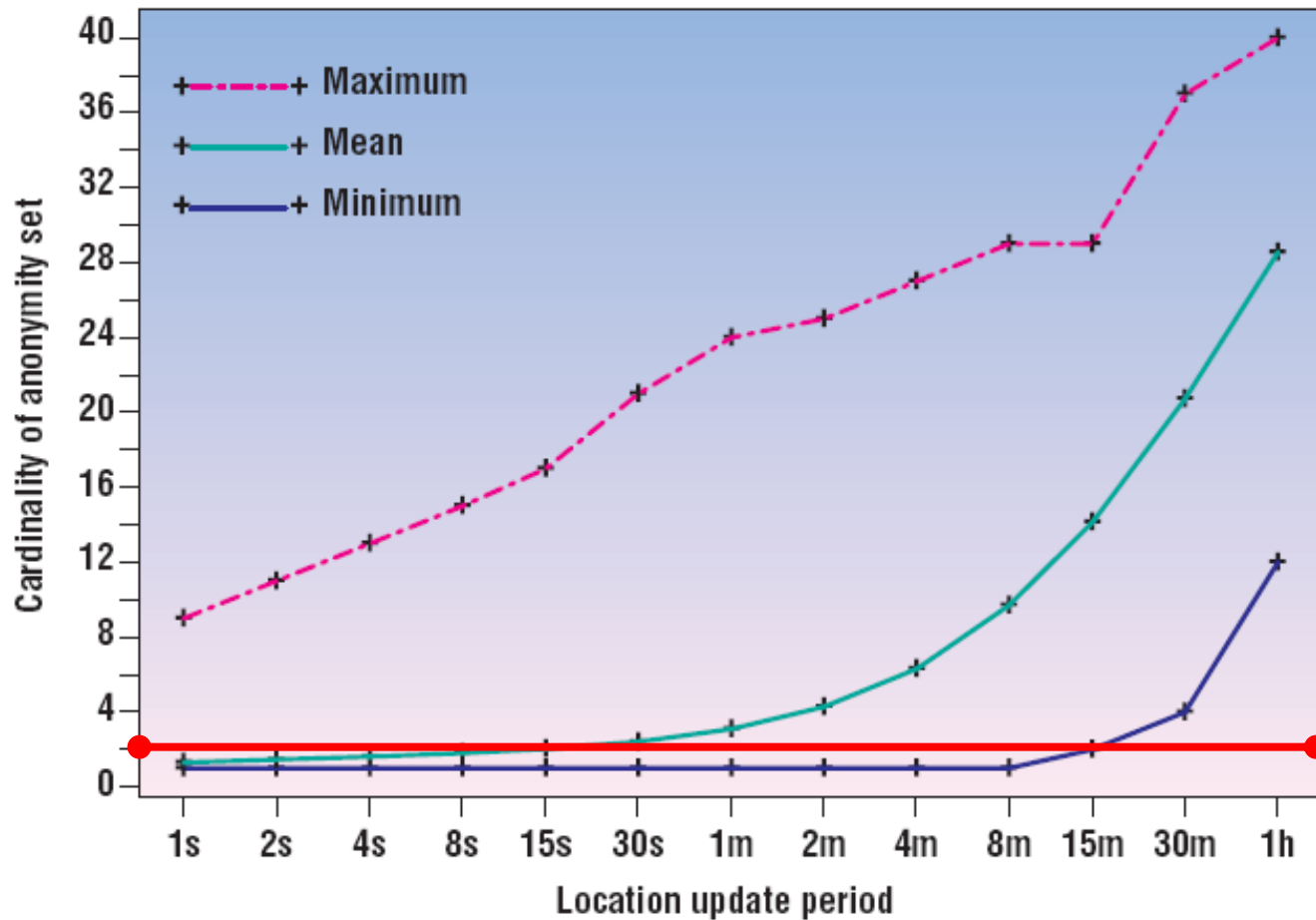
Pseudonymisiert

# Anonymitäts-Güte für $z_1$



Pseudonymisiert

# Anonymitäts-Güte für $z_3$



Pseudonymisiert

# Grenzen von Mix-Zonen

- Für diesen speziellen Versuch bieten Mix-Zonen zu wenig Location Privacy.
  - Zu wenig Benutzer auf dieser Fläche,
  - Hochauflösendes Lokalisierungssystem,
  - Geometrie der Mix-Zonen, ...
  - Alternative Versuchsanordnung? (GSM Zellen, Stadtzentrum)
- Ein Benutzer soll vor dem Nutzen eines Dienstes selber entscheiden können, ob die momentane Anonymität ausreichend ist.
  - Was ist ausreichend?
  - Was, wenn sie nicht ausreichend ist?

# Ortsbasierte Dienste: 3 Klassen

1. „Sobald du an einer Starbucks-Filiale vorbeikommst, informieren wir dich über neue Produkte.“
2. „Wenn du fünf deiner Lieblingskaffees bei uns gekauft hast, ist der sechste Kaffee gratis.“
3. „Wenn du dich in einem Starbucks aufhältst, informieren wir alle deine Freunde, dass du hier bist.“

# 3. Location Privacy für nicht-anonyme Dienste

- Zugriffskontrolle
  - Liste aller Personen, die befugt sind, meine Ortsinformationen abzurufen.
  - Sicher, einfach zu implementieren, aber aufwändig zu unterhalten.



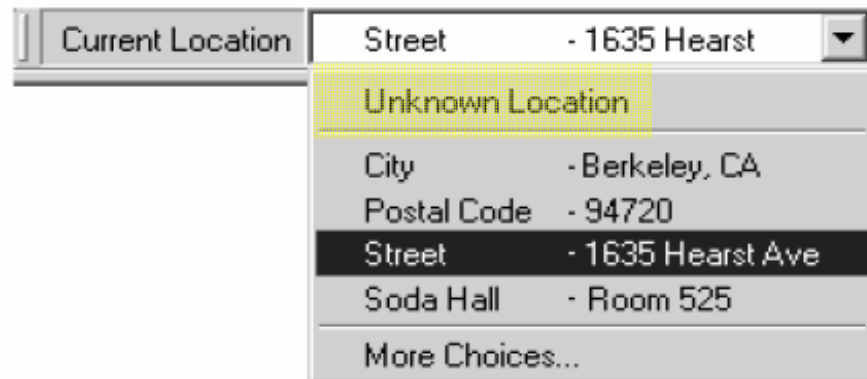
# Erweiterungen

- Rollenbasierte Zugriffskontrolle
  - Chef / Kollege / Freund / Familie / ...
  - Umgebungsbedingte Rollen denkbar („Jeder der im selben Gebäude ist, darf...“)
  - Regeln die von mehreren Personen gleichzeitig erfüllt werden müssen („X und Y dürfen nur gemeinsam...“)

# Obfuscation / Unschärfe

- Selektives „Verwischen“ der Genauigkeit / Richtigkeit der angebotenen Ortsinformationen.

→ Reno?



Identifiziert

# Zusammenfassung

- Location Privacy: Informationelle Selbstbestimmung in Bezug auf Ortsinformationen.
- Ortsinformationen bilden Kontext (Identität, Aktivität) und sind deshalb schützenswert.
- Viele Dienste lassen sich je anonymener genutzt desto weniger Informationen beim Dienstleister über den Benutzer notwendig sind.
- Lösungsansätze: Selbstpositionierung, Dienstleistungsverträge, Mix-Zonen, Zugriffskontrolle.

# Wie sieht die Zukunft aus?

- *Die Lösung gibt es nicht.*
  - Art der gewünschten Ortsinformation (Genauigkeit, Präzision) von Anwendung abhängig!
  - Privatsphären-Anspruch von Situation / Kontext abhängig.
  - Für kommerzielle Dienste sinnvoll realisierbar.
- Menschen die nicht ständig ortbar sein möchten, werden sich solche Anwendungen auch nicht zulegen.
  - Es gibt ja auch Menschen die nicht ständig erreichbar sein möchten und sich deshalb kein Handy zulegen.
  - Wird man diese Entscheidungsfreiheit in Zukunft auch noch haben?

# Referenzen (Auswahl)

You're a Dog Comic: <http://kj.uue.org/presentations/internet-privacy/gfx/newdog.gif>

Chapter 3 of A. Beresford's PhD thesis: Location Privacy in Ubiquitous Computing

A. R. Beresford and F. Stajano: Location Privacy in Pervasive Computing

J. I. Hong, G. Boriello, J. A. Landay, D. W. McDonald, B. N. Schilit, J.D. Tygar: Privacy and Security in the Location-enhanced World Wide Web

T. Rodden A. Friday, H. Muller and A. Dix: A Lightweight Approach to Managing Privacy in Location-Based Services