

“The Loss of Location Privacy in the Cellular Age”

Stephan Latta & Stefan Taute



11. Dezember 2012

Thema

„The Loss of Location Privacy in the Cellular Age“

**(Verlust der Privatsphäre im
Mobilfunkzeitalter)**

Gliederung

- 1 Einleitung
- 2 Grundlagen
- 3 Location Privacy
- 4 Location Anonymity
- 5 Fazit
- 6 Fragen

Hintergrundinformation zur Thematik

- „Location Privacy“ häufiger Begriff in Datenschutzdebatten
- mögliche Risiken, Gefahren des Verlusts der örtlichen Privatsphäre
- heutzutage besitzen die meisten Menschen ein Smartphone, somit jederzeit lokalisierbar
- entscheidene Unternehmen sind Apple und Google
- Brisanter Fund April 2011: Alasdair Allan und Peter Warden finden Datei namens „consolidated.db“

Hintergrundinformation zur Thematik

- Apple gab zu MAC-Adressen und Signalstärken von Access Points aufzuzeichnen, Speicherung in Kombination mit Zeitstempel und einem Geo-Tag
- Apple zeichnet des Weiteren IDs und Signalstärken von Mobilfunkmasten auf, Speicherung in Kombination mit iPhone Geo-Daten
- Apple versicherte die Daten werden nur anonymisiert genutzt, die Daten werden nur zur Verbesserung von „Location Based Services“ verwendet

⇒ **Je besser die Lokalisierungstechniken, desto schwieriger die Anonymität und Privatsphäre zu wahren.**

Video:

„iPhone Tracking Discussion“

[Start Video](#)

Zielsetzung der Ausarbeitung & des Vortrags

- Einblick in das Thema „Location Privacy“
- Grundlage war der wissenschaftliche Artikel
„The Loss of Location Privacy in the Cellular Age“
(Stephen B. Wicker¹, August 2012 CACM)
- Grundlagen zum Verstehen der Thematik
- Gefahren & Risiken bzgl. Privatsphäre im
Mobilfunkzeitalter
- Möglichkeiten zum Schutz der Privatssphäre
(anonymisierte Location Based Services)



¹Professor der „School of Electrical and Computer Engineering Cornell University“ und ist Mitglied der Fachbereiche „Computer Science, Information Science, Applied Mathematics

- um „Location Based Services“ und die restliche Thematik verstehen zu können bedarf es der Erläuterung zugrundeliegender Ortungstechnologien
- Ortungstechnologien: hier wird der Ursprung der mobilen Ortung und in dem Zusammenhang GPS und Alternativen erläutert
- daraufhin werden die Begriffe *Location Based Services*, *Location Based Advertising*, *Privatsphäre*, *Anonymisierung* und *Ort* erläutert
- damit wird eine Grundlage für die Abschnitte „Location Privacy“ und „Location Anonymity“ geschaffen

Mobilfunküberwachung & E911

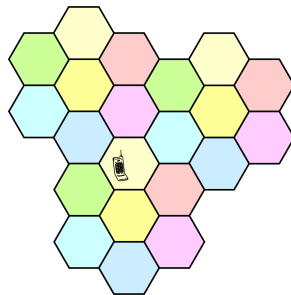
- Mobilfunknetze grundsätzlich darauf ausgelegt Endgeräte zu tracken, ursprünglich nur um nächstgelegenen Mast zu finden
- 1996 erste Versuche die Ortung zu verfeinern (**E911** durch die *Federal Communication Commission*)
- **E911** sollte die Mobilfunkanbieter zwingen die Ortsinformation bei einem 911-Anruf an die Notrufzentrale zu übermitteln
- **E911** war sozusagen der Grundstein für die Ortung im Mobilfunksektor, unter anderem Grund dafür das die meisten mobilen Endgeräte heute auch andere Lokalisierungstechniken besitzen

GPS

- heutzutage verfügen Smartphones über GPS womit die Ortung noch exakter ist
- das **G**lobal **P**ositioning **S**ystem ist ein Satelliten gestütztes Ortungssystem
- grundsätzlich nicht für Smartphones konzipiert, sonder für allg. Einsatz im Außenbereich
- GPS-Signale enthalten Orte und Umlaufbahnen der jeweiligen Satelliten
- Daten ermöglichen dem Empfänger die Lokalisierung
- langsame Datenübertragung, Ortung kann daher bis zu 12,5 Minuten dauern
- Daten werden nur mit 50 kbps übertragen um Signalstörungen und gegenseitige Beeinflussung zu vermeiden

Netzwerkbasierte Lokalisierung

- wegen der meist langsamen Ortung durch GPS sucht man aktiv nach Alternativen
- eine ist die netzwerkbasierte Positionsbestimmung
- ein gängiger Ansatz ist Cell-of-Origin (COO)
- hierbei wird die Position des Mobilfunkmastes (Basiszelle) genutzt
- Wabe = Basiszelle
- Standort durch Wabengröße sehr ungenau



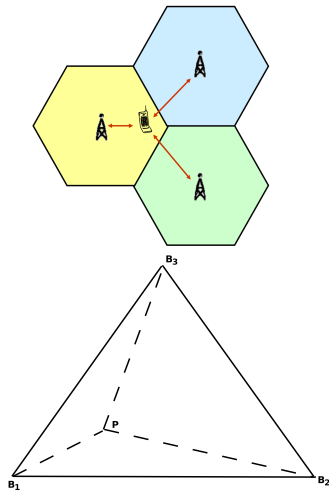
Identifizierung von Access-Points

- noch besserer Ansatz ist die Identifizierung von Access-Points (AP) sowie Mobilfunkmasten
- Apple und Google sammeln daher schon länger entsprechende Daten über ihre Endgeräte
- großer Vorteil ist der meist feste Standort der APs und Masten
- durch die gesammelten Daten lässt sich heute bis auf die Hausnummer genau bestimmen wo sich das Endgerät befindet
- Position wird durch „Triangulierung“ bestimmt

Identifizierung von Access-Points

- Waben zusammen sind vereinfacht eine Ortungskarte
- Triangulierung auf Basis der dem Engerät am nächstliegenden 3 Ortungsbereiche (Waben)
- Berechnung durch WCL (Weighted centroid localization, gewichteter Schwerpunkt)

$$P(x, y) = \frac{(\sum_{i=1}^n (w_i * B_i(x, y)))}{(\sum_{i=1}^n w_i)}$$



Definition LBS

- darunter versteht man standortbezogene Dienste, kurz LBS
- Dienste berücksichtigen die aktuelle Position
- zum Ort werden auch noch die aktuelle Zeit und Infos über den Nutzer vom LBS berücksichtigt
- Definition von Jochen Schiller und Agnes Voisard:

„Location Services can be defined as services that integrate a mobile device's location or position with other information so as to provide added value to a user.“

- oft genutzt in Informationsdiensten zu Sehenswürdigkeiten, Einkaufsmöglichkeiten oder Ärzten in der näheren Umgebung

LBS - Unterteilung in Kategorien


LBS-Dienste	Anwendung
Sicherheitsrelevante Dienste	Notfallsituation, Notruf, Unfallruf, Diebstahlüberwachung von Gütern, Ärzte, Krankenhäuser,
Angebots- und Informationsdienste	Verkehrsinformationen, Fahrpläne, Hotels, Restaurants, Kinos, Tankstellen,
Routen-/Logistikdienste	Tracking von Gütern, Routenplanung, Flottenmanagement, Überwachung von Fahrtrouten,
Unterhaltungsdienste	Persönliche Bekannte, Freunde, lokale Angebote an Erotik-Services,

LBS - Hotelsuche


Back
Search
Home

MAIN ST, Dallas, TX USA
 Check-in: None Selected
 Check-out: None Selected
 Rooms: 1, Adults: 2, Children: 0


Search Options >



West End Hotel Downtown ...
 0.1 Miles From MAIN ST, Dallas, TX USA
 ★★ | Guest Rating: 4.2 of 5
 from \$99.00 Lowest Avg Nightly Rate



The Adolphus-A Noble Hou...
 0.1 Miles From MAIN ST, Dallas, TX USA
 ★★★ | Guest Rating: 4.6 of 5
 from \$139.00 Lowest Avg Nightly Rate



The Magnolia Hotel
 0.1 Miles From MAIN ST, Dallas, TX USA

LBS - Restaurantsuche

Filtern nach: [Entfernung ▾](#) | [Restauranttyp ▾](#) | [Nutzerbewertung ▾](#)

restaurant in der Nähe von Unter den Linden, Berlin

Kategorien: [Restaurants und Gaststätten](#), [Restaurants und Gaststätten Betriebsgesellschaften](#)

Anzeigen

[Unter den Linden Berlin](#)

Save on Hotels in **Berlin**
Call 1-800-447-4136 Or Book Online
www.HotelReservations.com



[Restaurant Dressler](#) - [mehr Infos >](#)

Unter den Linden 39, 10117 Berlin - 030 20450655

★★★★☆ [8 Beurteilungen](#) - [Beurteilung schreiben](#)

"Das Dressler ist sehr verkuehrguengstig im Herzen von Mitte direkt 'Unter den ..."



[Hotel The Westin Grand, Berlin](#) - [mehr Infos >](#)



Friedrichstrasse 158-164, 10117 Berlin - 030 20270

Kategorie: Restaurants
★★★★☆ [266 Beurteilungen](#) -

[Beurteilung schreiben](#)

"Übernachtung vom 26.04.08 bis 27.04.08 - Lage Top. Besser geht es in Berlin fast ..."



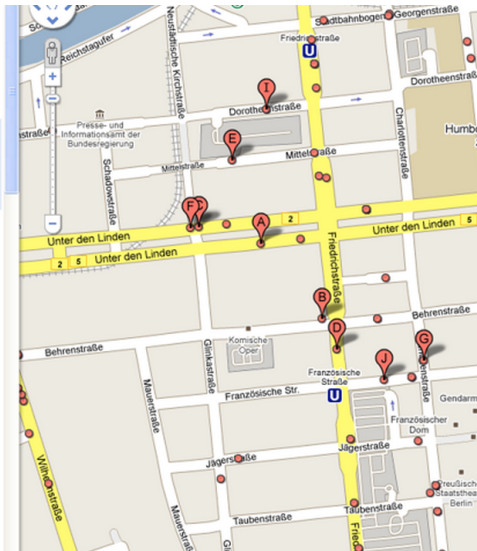
[NewsCafe Gaststätten GmbH](#) - [mehr Infos >](#)



Unter den Linden 42, 10117 Berlin - 030 20214347

Kategorie: Restaurants und Gaststätten

★★★★★ [12 Beurteilungen](#) - [Beurteilung schreiben](#)



Erläuterung von Location Based Advertising

- kurz LBA, auch als Location Based Marketing (LBM) bekannt
- LBA beruht auf LBS
- Verknüpfung zwischen Marketing (inkl. Werbung) und LBS
- basierend auf Präferenzen, aktuellem Ort und der aktuellen Zeit wird dem Nutzer eine maßgeschneiderte Werbung präsentiert

Erläuterung von Privatsphäre & Anonymisierung

- Begriff Privatsphäre nicht klar abgrenzbar
- Definition nach Alan Westin:

„Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy, or, when among larger groups, in a condition of anonymity and reserve.“

Erläuterung von Privatsphäre & Anonymisierung

- nach A. Westin hat jeder Mensch Anrecht selbst zu bestimmen, was er von sich preisgibt
- außerdem wird deutlich das Privatsphäre mit dem Recht auf Anonymität einhergeht
- „Anonymität“ erlaubt es einer Person unter einer Menge von Personen nicht identifiziert zu werden

Auffassungen vom Begriff „Ort“

- es gibt verschiedene Auffassungen
- im geografischen Sinne ein Raum bzw. fester Standort
 - charakterisiert durch räumliche Ausdehnung und Position, gegeben durch Längen- sowie Breitengrade
- eine philosophische Auffassung nach dem Geograf und polit. Philosoph John Agnew
 - **Location:** Wo - Position, die beispielsweise durch Längen- und Breitengrad gegeben ist
 - **Locale:** Gestalt des Ortes, die z. B. durch Grenzen (Mauern, Zäune, Bäume, Flüsse usw.) geprägt ist
 - **Sense:** durch Standort und örtliche Gegebenheiten generierte/verbundene persönliche Emotionen

Aufassungen vom Begriff „Ort“

- dem Ort wird nun eine gewisse Bedeutung, die von örtlichen Gegebenheiten und subjektiven Empfinden der Person abhängt zugewiesen
- andere Phänomenologen und Geografen haben das ganze soweit aufgefasst das der Ort bzw. Platz zu einen tiefgreifenden Zentrum der menschlichen Existenz zählt

Location Privacy - Bedenken, Risiken & Gefahren

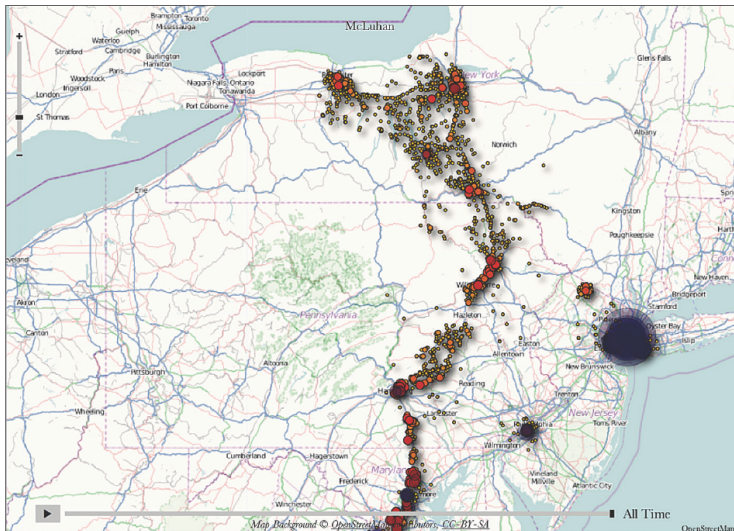
- eine allg. Definition gibt es wie für „Privatsphäre“ nicht
- Definition nach R.Beresford und F.Stajano:

„[...] the ability to prevent other parties from learning one's current or past location.“

- Definition nach Duckham und Kulik:

„[...] a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others.“

Bewegungsprofil des iPhones von S. Wicker



Hauptbedenken von Datenschützern

- aus dem Profil lässt sich problemlos ableiten das sich Wicker oft in Washington und New York aufhält
- durch Bewegungsprofile kann unmittelbar nachvollzogen werden, wo sich eine Person aufgehalten hat
- das ganze durch besser werdende Technik bis auf Adressebene
- Problem, solche anonymen Daten können mit Hilfe anderer öffentlich zugänglicher Daten leicht de-anonymisiert werden

Mögliche ableitbare Informationen

- **Zuhause**

Adresse, Art der Nachbarschaft \Rightarrow Hypotheken, steuerliche Abgaben, sozioökonomischer Status usw.

- **Freunde**

Art des Zuhause, Besuchsfrequenz und -dauer \Rightarrow enge Freunde, Bekannte usw.

- **Religiöse Einrichtungen**

Religion \Rightarrow Glauben oder eventuell gar nicht gläubig

- **Einkaufsläden**

Einkaufsmuster \Rightarrow Vorlieben, persönliche Laster usw.

Mögliche ableitbare Informationen

- **Ärzte & Kliniken**

Häufigkeit, Dauer, Fachgebiet des Arztes ⇒
Krankheitsanfälligkeit, ernste oder vielleicht chronische
Krankheit usw.

- **Einrichtung zur Unterhaltung/Freizeit**

z. B. Möglichkeit zu ermitteln welchen Musikstil eine Person
bevorzugt und viele andere ableitbare Informationen

⇒ laut S. Wicker könnte diese Liste noch weiter fortgeführt
werden

Kernaussage

- Kernaussage soll sein, dass durch die adresslevel-genaue Lokalisierung Informationen über Vorlieben, Eigenschaften, Laster, Glauben und Verhalten einer Person in bestimmten Fällen ableitbar sind
- das ist auch der Grund warum diese Daten für gewisse Menschen, Konzerne und Kriminellen so begehrt sind
- gerade für Marketing-Unternehmen stellen die Daten einen unschätzbaren Wert da
- „InfoUSA“ pflegt z.B. eine Liste mit 210 Mio. Konsumenten, durch LBS ist dies nun wesentlich einfacher und besser
- **Früher:** Person macht Yoga
Heute: Yoga + Yogastudio + aktuell Vorort + Wie oft? etc.
- LBA geht über normales Marketing weit hinaus

Warum LBA Risiko für Privatsphäre?

- Welchen Einfluss kann Werbung auf einen Menschen nehmen?
- Autorin Judith Williamson beschreibt Werbung als Mittel zur Verschiebung des Sinns bzw. der Bedeutung eines semantischen Netzwerks zu einen anderen
- Beispiel der Autorin:
 - Schauspielikone Catherine Deneuve steht neben einer Parfümflasche.
 - Ziel: Konsumenten sollen das Parfüm mit einer schönen Frau verbinden.
 - Verschiebung eines semantischen Netzwerks
Schauspielerei ⇒ Parfümmarke

Warum LBA Risiko für Privatsphäre?

- ähnliches Potential zur Sinnverschiebung hat LBA
- man kann durch Werbung die Bedeutung die mit einem Ort assoziiert wird ändern
- Marketer können basierend auf aktuellen Standort der Person zielgerichtete Werbung ausliefern und sein Reaktion überprüfen
- Gilles Deleuze meint durch LBA kann das Verhalten und Handeln einer Person gezielt beeinflusst werden (durch ständigen abgleich der Reaktion auf eine Werbung, bei ungewünschten Verhalten wird Werbung verändert)
- Lokalisierung und LBA kann die Beziehung einer Person zu seiner Umwelt manipulieren

Warum LBA Risiko für Privatsphäre?

- Stephen Wicker fast wie folgt zusammen:

„LBA has the potential to detract from the experience of [...] familiar and meaningfilled environs. One's surroundings may thus lose their 'placeness' through LBA, including their meaning, and become merely a path to be traversed. As places become locations, meaning is lost to the individual. That is, we lose some of ourselves, as well as one of the critical processes through which we become a self.“

Allgemeines zu Location Anonymity

- um auf Vorzüge von LBS und LBA nicht verzichten zu müssen, müssen die Daten anonymisiert werden
- das Löschen von Gerät-ID, Namen oder Telefonnummern aus den Datensätzen ist nicht ausreichend
- innerhalb weniger Wochen gelang es Arvind Narayanan und Vitaly Shmatikov mittels sogenannten „Correlation Attacks“ so anonymisierte Daten zu de-anonymisieren

Erläuterung Correlation Attacks

- Correlation Attacks: Prinzip ist der Vergleich der Daten mit anderen nicht anonymisierten Daten unter folgenden zwei Hauptaspekten:
 - 1 Konzentration auf selten vorkommende Datenattribute
 - 2 der zutreffendeste Treffer sollte eine viel höhere Punktzahl haben als ein weniger zutreffender Treffer \Rightarrow „False Positives“
- Wicker versucht ein beispielhaftes Model zur Erklärung des Erfolgs bzw. Misserfolgs von „Correlation Attacks“ aufzustellen, auf Grundlage einer Theorie von Claude Shannon

Shannon - „Unicity Distance“

- 1949 veröffentlichte Claude Shannon den Artikel „Communication Theory of Secret System“
- dort definierte er die „*Unicity Distance*“:
Die minimale Menge von Chiffretext, die benötigt wird, so dass die Unbestimmtheit über einen Teil eines Klartextes nicht mehr gegeben ist.
- der Ansatz kann auf die De-anonymisierung übertragen werden:
Es gibt eine minimale Menge von anonymen Daten die ausreicht, um im Abgleich mit nicht anonymisierten Daten, einige zu de-anonymisieren.

Shannon-theoretischer Ansatz eines Models

Basierend auf dem Paper erfolgt an der Tafel ein
Shannon-theoretischer Versuch diesen Sachverhalt zu
verdeutlichen.

Schlussfolgerung

- **Reduzierung der Länge der Lokalisierungslisten**
Hat die Mapping-Funktion weniger Informationen zum Mappen, dann wird ein P Vektor mit weniger t Koordinaten generiert.
- **Reduzierung der Fähigkeit der Mapping-Funktion bestimmte Lokalisierungsdaten in konkrete Koordinatenwerte des P Vektors aufzulösen**
Möglich indem der Bereich bzw. die Größe eines Ortungspunktes der Lokalisierungsliste reduziert wird.

Anonymisierte Location Based Services

- LBS sollen helfen die Anonymität und Privatsphäre von Personen zu bewahren
- Erläuterung von LBS erfolgt an einem Beispiel aus dem Paper
- LBS namens „The Doppio Detector“, dient dazu die Richtung zum nächstgelegenen Espresso-Shop zu zeigen

Erläuterung am Beispiel

- zwei Informationen müssen hier miteinander verknüpft werden
aktueller Standort + Standorte von nahegelegenen Espresso-Shops
- durch einen Navigationsalgorithmus lässt sich so ein Weg errechnen

⇒ zwei strukturelle Funktionen eines LBS:

- ① Position bzw. Ort an dem sich eine Person befindet, mit dem notwendigen Grad an Genauigkeit ermitteln
- ② eine Datenbank nutzen, um die Positionsdaten abzugleichen und so die gewünschte Information ermitteln zu können

Unabhängige GPS-Ortung

- im Hinblick auf anonymisierte LBS, beste Mittel unabhängige GPS-Ortung
- mobile Endgeräte müssen Positionsdaten empfangen können ohne selbst Informationen preisgeben zu müssen
- Zitat S. Wicker:

„[. . .] the more that can be done within the handset and kept within the handset, the greater the preservation of anonymity.“

- Endgeräte müssten demnach alle Daten direkt vom GPS-Satelliten abfragen, was wie schon erwähnt sehr lange dauern kann

Unabhängige GPS-Ortung

- eine Möglichkeit: Service Provider stellt Informationen zur Konstellation bereit
- dadurch entweichen zwar auch Informationen über das mobile Endgerät, jedoch sind diese Informationen sehr grob
- grob, weil der Service Provider nur den Mobilfunkmast über den das mobile Endgerät kommuniziert, kennen muss
⇒ gibt wenig über das Verhalten oder die Vorlieben einer Person preis
- technisch: ein generierter Eigenschaftsvektor enthält somit nur sehr wenige Koordinaten mit Informationen

Weitere Ansätze

- Ansatz von Khoshgozaran und Shahabi
 - kurz gesagt: Das Netzwerk übernimmt die Ortung.
 - Netzwerk wird aber daran gehindert das Endgerät korrekt zu lokalisieren
 - das Endgerät überträgt seine Position mit einer vorherigen Translation
 - der Server erhält die verfälschte Position und gibt den Standort zurück
 - das Endgerät macht auf dem empfangen Standort die Translation rückgängig und hat somit die korrekten Daten
- ⇒ grundsätzlich kann geschlussfolgert werden, dass die Privatsphäre nicht zwingend leiden muss

Bewahrung Privatsphäre ↪ zweite LBS Funktion

- zwei weitere Hürden:
 - ① **Konsistente Eingabegenauigkeit**
Eine Person die den nächstliegenden Espresso-Shop sucht, benötigt die Richtung auf Adresslevel-Ebene.
 - ② **Bekannte Position**
Viele LBS-Anfragen beinhalten Objekte/Ziele deren Position bekannt ist.
- um Anonymität trotz Mappings zu bewahren, gibt es einige Mittel

„k-anonymity“ Ansatz

- eins ist der sogenannte „k-anonymity“ Ansatz:

*„Auf Positionsdaten bezogen versteht man unter **location k-anonymity** den Zustand, dass der Benutzer innerhalb einer Gruppe von k Benutzern nicht identifiziert werden kann. Hergestellt wird diese Bedingung dadurch, dass die vom Benutzer preisgegebenen Positionsdaten ununterscheidbar sind von mindestens $k - 1$ weiteren Benutzern (z.B. in dem statt einer präzisen Position lediglich eine größere Region mitgeteilt wird). Ein Rückschluss auf eine bestimmte Person ist also nur mit Wahrscheinlichkeit $\frac{1}{k}$ möglich.“*

- für LBS Mapping-Funktionen bedeutet der Ansatz, dass Informationen die eine Person identifizieren bei k Anfragen gelöscht werden
- dabei können trotz dessen noch unerwünschte Informationen nach außen dringen

Weitere Ansätze

- ein weiterer Ansatz benutzt keine exakten Ortsinformationen
- beispielsweise schickt man nur die Ortsangabe „Altstadt Stralsund“
- eine Espresso-Shop-LBS könnte dann einfach eine Karte mit den Espresso-Shops in der Altstadt schicken
- der Nutzer kann nun einen Shop wählen und das mobile Endgerät berechnet die Route dorthin selbst

Weitere Ansätze

- noch ein anderer Ansatz wäre die Länge einer Lokalisierungsliste zu begrenzen
- ein Dienst wird somit behindert, festzustellen von welchem konkreten Endgerät die Anfrage stammt
- laut Wicker ist demnach auch eine Authentifizierung mittels „Public-Key“-Infrastrukturen und verschlüsselter Autorisierung möglich und das ohne die Identität preiszugeben
- außerdem können mittels zufälligen Tags häufig anfragende Personen anonymisiert werden
- sozusagen ergibt das wieder eine *k-anonymity*
- kombiniert mit groben Ortungen oder zufälligen Verzerrungen besteht ein vielversprechender Ansatz die Privatsphäre zu schützen

- „Location Privacy“ ist ein ernstzunehmendes Thema
- durch besser werdende Technik Positionsbestimmung auf Adressebene möglich
- Gefahren & Risiken:
 - Gefahr, dass jemand durch Kenntnis der aktuellen Position einer Person ständig verfolgt werden kann (Stichwort Stalker)
 - Manipulation und Bedrohung der Selbstbestimmtheit bzw. Autonomie einer Person
 - Einflussnahme als auch Störung der Beziehungen von Personen hinsichtlich ihres Umfelds
 - ernste Gefahr für die Privatsphäre durch Adresslevel-genaue Lokalisierung, da hierdurch Vorlieben, Eigenschaften, Verhalten als auch Glauben einer Person aufgedeckt werden können
- daher ungemein wichtig die Entwicklung anonymisierter LBS voranzutreiben, um Anonymität und Privatsphäre zu schützen

**Vielen Dank für ihre
Aufmerksamkeit!**

**Vielen Dank für ihre
Aufmerksamkeit!**

Fragen?