Location Based Services[1]

Georg Lechner

ggl@chello.at

Schlagworte: Location based data, Datenschutz, e-commerce, Standortdaten.

Abstract: Mit der Verwendung von Standortinformationen („Location Based Data") treten die Dienste der Informationsgesellschaft in ein vollkommen neue Phase. Die Möglichkeiten zur Verwertung sind groß, aber die neuen Techniken werfen auch große Datenschutzprobleme auf.

Ein „Location based Service (LBS)" ist ein Dienst der Informationsgesellschaft, dessen wesentliche Eigenschaft darin besteht, Information abhängig von der Position des Benutzers zu liefern.

Dieser Beitrag beschäftigt sich mit Diensten in Mobilen Netzwerken (GSM und UMTS), die auf einer Ortsangabe aufbauen. Sehr viele dieser Dienste sind zur kommerziellen Verwertung bestimmt. Für die Betreiber von Handynetzen sind neue Einkünfte wichtig. Mit herkömmlichen Leistungen (Sprachtelefonie und SMS) lässt sich immer weniger Geld verdienen.

1. Techniken zur Lokalisierung

1.1. Im Mobiltelefonnetz

Jedes Mobiltelefonnetz besteht aus Gebieten, die von Handy-Funksendern abgedeckt werden, sog Zellen. Jedes Handy gibt ständig Signale ab, die dem Netzwerk mitteilen, in welcher Zelle sich das Handy befindet. Diese Information ist unbedingt erforderlich, um Anrufe an das Handy weiterzuleiten.

Die ständigen Signale des Handys können aber auch zur Lokalisierung verwendet werden.

Die Messgenauigkeit hängt von verschiedenen Faktoren ab, wie zB der Qualität des Handy-Netzes, Barrieren (Gebäuden, Keller) und etwai-

---

[1] Die Erwähnung von Produkten und Diensten dient zur Illustration der technischen Möglichkeiten und ist keinesfalls als Werbung oder Empfehlung zu verstehen.

gen Störfaktoren. Derzeit beträgt die Messgenauigkeit bei GSM 200-500 Meter; UMTS soll eine Standortbestimmung auf bis zu 25 Meter gestatten.

1.2. Global Positioning System (GPS)

Es ist möglich, ein Handy mit einem GPS-Satellitenempfänger zu versehen. GPS ist ein amerikanische Technologie, die weltweit verfügbar ist. Die Europäische Union will unter dem Projektnamen GALILEO ein vergleichbares System schaffen.[2]

Der GPS-Empfänger wertet Signale von speziellen Satelliten aus, um seinen genauen Standort zu ermitteln. GPS-Empfänger sind bereits sehr klein, und können auch in ein Handy eingebaut werden[3]

Die US-Regierung, die GPS kontrolliert, hat am 2. Mai 2000 eine bisher nur für das Militär zugängliche Genauigkeitsstufe für zivilen Gebrauch freigegeben[4]. GPS wird damit auf 20 Meter genau, allerdings ist der GPS-Empfang in Gebäuden schlecht.

GPS hat keinen Rückkanal, dh ein GPS-Empfänger sendet keine Daten.

2. Mögliche Dienste

2.1. Location Based E-Commerce

Der Benutzer erhält gegen Bezahlung Informationen über den Ort, an dem er sich befindet (Sehenswürdigkeiten, Karte der Umgebung, Verkehrslage), oder wird auf Wunsch zu bestimmten Orten dirigiert (Restaurant, Apotheken, Museen, sogar öffentliche Toiletten(!)[5]). Der Benutzer kann auch Taxis oder Pizza mit Botendienst an seinen Standort bestellen, etc.

---

[2] http://www.esa.int/export/esaSA/navigation.html.

[3] Der finnische Handyhersteller *Benefon* (http://www.benefon.com) liefert bereits derartige Geräte.

[4] Lesen Sie dazu http://www.igeb.gov/sa/. Die Seite „Examples of Civilian Benefits" enthält weitere Anwendungen für GPS, die aber nicht „Location Based Services" sind.

[5] Es gibt bereits einen WAP-Dienst, der im Ruhrgebiet (Deutschland) bei der Suche nach einer Toilette hilft (http://www.woklo.de/). Wenn man die erste Verblüffung über diesen „anrüchigen" Dienst überwindet, erscheint woklo.de als ein Dienst, der zB in Fremdenverkehrsorten durchaus Sinn ergibt.

Der gesamte Komplex der Probleme bei Online-Bestellungen taucht hier auf: Vertragsabschluss, Nachweis der Vertragsbeziehung, Bezahlung, Gerichtsstand. Da der Kunde oftmals die Leistung nicht an eine nachprüfbare Privat- oder Geschäftsadresse liefern lässt, ist die Gefahr für den Unternehmer doppelt groß, Opfer eines üblen Scherzes oder eines Betruges zu werden. Gleichermaßen ist für den Kunden das Risiko groß, Opfer eines betrügerischen Unternehmers zu werden, der im Voraus kassiert, nicht oder schlecht liefert, und anschließend behauptet, die Lieferung habe korrekt stattgefunden. Wie soll ein Tourist in einen fremden Land nachweisen, dass er die bezahlte Pizza nicht erhalten hat?

Es erscheint wichtig, technische und organisatorische Vorkehrungen zu treffen, die das Risiko von Betrug und Missbrauch minimieren ohne dass personenbezogene Daten übermittelt oder unfangreiche Kontrollen erforderlich werden. Als Beispiel kann ein Protokoll genannt werden, bei dem die Bestellung per digitaler Signatur abgewickelt wird, sodass beide Seiten einen Beleg des Geschäftes haben, und in der Folge die Bezahlung so abgewickelt wird, dass der Verkäufer von einer vertrauenswürdigen dritten Stelle (zB einer Bank) die Information erhält, dass die Kaufsumme verfügbar ist, aber der Kunde die Zahlung erst autorisiert, wenn er die Lieferung erhalten hat.

2.2. Location Based Advertising

Werbung abhängig vom Ort scheint bereits vielen Unternehmen attraktiv. Ein Handy-Benutzer, der an einem Geschäft vorbeigeht, erhält Werbung[6].

Solche Dienste lassen sich nur mit einer Zustimmung realisieren. Angesichts der Kosten für Handy-Telefonate, die vielen Anwendern über den Kopf wachsen, können Werbeagenturen als Sponsoren auftreten. Dieses Phänomen – kostenlose oder verbilligte Leistung gegen Werbung – funktioniert im Internet bereits seit Jahren hervorragend. Werbefinanzierte Leistungen im Internet sind primär Webspace und E-Mail-Dienste. Da wie dort sind die Werbeunternehmen an personenbezogenen Daten der Kunden und Besucher sehr interessiert, was beträchtliche Probleme verursacht. Während der Kunde selbst seine Zustimmung erteilen wird, ist die Zustimmung eines Gesprächspartners des Kunden weniger gewiss. Wei-

---

[6] Es gibt sogar bereits eine Organisation der Werbewirtschaft, die Mobile Marketing Association (MMA) (http://www.mmaglobal.com).

ters existieren bereits Programme, die Werbebanner ausfiltern[7]. Die Frage der rechtgeschäftlichen Verhältnisse bei werbefinanzierter Kommunikation wird sich bei mobilen Diensten stellen; vor allem im Verhältnis zum Gesprächspartner, der keine Zustimmung erteilt hat.

2.3. Location Sensitive Billing

Der Handybetreiber lässt den Teilnehmer in einer bestimmten Zone verbilligt telefonieren. Diese Art von Dienst wird bereits angeboten[8]. Location Sensitive Billing ist ein Dienst, der nur vom Provider selbst angeboten werden kann. Location Sensitive Billing soll den Betreibern von Handynetzen ermöglichen, besser in Konkurrenz zum billigen, aber ortsgebundenen Festnetz zu treten. Für diese Art von Dienst genügt die Information, in welcher Funkzelle der Teilnehmer sich aufhält.

Eine Variante ist vorstellbar, bei der ein Sponsor die Kosten aller Gespräche zwischen Personen, die sich in einem bestimmten Gebiet aufhalten, übernimmt (zB Clubbings, Kommunikation auf einem großen Firmengelände etc). Damit wird allerdings eine genauere Ortsbestimmung erforderlich, die beträchtliche Datenschutzprobleme aufwirft.

2.4. Notfalldienste

Die Federal Communications Commission (FCC) hat entschieden, dass bis Ende 2002 alle in den USA verkauften Handys im Falle eines Notrufes lokalisierbar sein müssen[9].

Die Betreiber können bei großen Katastrophen mit Dutzenden Vermissten oder auch unidentifizierten Toten helfen, indem sie bekannt geben, ob vermisste Benutzer zur fraglichen Zeit in der Zelle des Unfallortes waren[10].

Die deutsche Firma Vitaphone (www.vitaphone.de) bietet ein Spezialhandy, das mit Hilfe von Sensoren das EKG des Trägers messen kann. Im Fall von Herzproblemen kann das Handy über GPS lokalisiert und ein Rettungsdienst verständigt werden.

---

[7] http://www.webwasher.com/.

[8] Von VIAG Interkom in Deutschland (http://www.genion.de).

[9] Siehe http://www.fcc.gov/e911/.

[10] Siehe zB http://www.fema.gov/nwz01/nwz01_108.htm.

2.5. Verfolgung von Fracht und Fahrzeugen

Transport- und Kurierfirmen sind an Technologien zur Verfolgung von Fracht, Fahrzeug und Fahrer interessiert.

Eisenbahngesellschaften sind auch an derartigen Technologien interessiert, weil sie damit eine billige und europaweit einheitliche Methode erhalten, um Züge und einzelne Waggons (nicht personenbezogen!) zu verfolgen. Ein Problem ist dabei die Stromversorgung der auf Waggons montierten Elektronik. Die ÖBB verwenden heute schon GPS als Teil ihres Sicherheitssystems.

Die elektronische Verfolgung kann einen Eingriff in die Grundrechte des Fahrers darstellen, ihm aber auch im Falle eines Verbrechens oder Unfalls das Leben retten. Die Verfolgung der Fracht ist datenschutzrechtlich unbedenklich, die Verfolgung des Fahrers nicht.

2.6. Maut

Mit hinreichend genauer Ortung kann auch die Maut für ein Fahrzeug mit Hilfe von Handys administriert werden. Der Fahrer gibt die Kennung seines Handys bekannt und das Mautsystem kontrolliert den Gebrauch der Mautstrasse durch Verfolgung des Handys.

Eine zusätzliche Kontrolle muss sicherstellen, dass die Maut für das Fahrzeug, in dem der Handybenutzer sitzt, angemessen ist (zB jemand entrichtet die Maut für einen PKW und fährt einen Sattelschlepper). Außerdem kann die Verfolgung des Fahrzeuges zu Bewegungsprofilen führen.

2.7. Kontrolle von Mitarbeitern

Vorgesetzte haben ein wirtschaftliches Interesse daran, ihre Mitarbeiter im Außendienst oder auf Rufbereitschaft zu kontrollieren. Dabei ergeben sich etliche Rechtsfragen ganz neuer Art, die noch geklärt werden müssen. Die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, welche die Menschenwürde berühren, bedarf gemäß § 96 Abs 1 Z 3 Arbeitsverfassungsgesetz einer Zustimmung des Betriebsrates.[11]

[11] Gemäß § 79c Beamten-Dienstrechtsgesetz 1979 ist die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren, sogar vollkommen unzulässig.

2.8. Kontrolle von Minderjährigen

Ein großes datenschutzrechtliches Problem kommt in Form von Technologien, die den Standort von Minderjährigen weitermelden, auf uns zu.[12] Die Wünsche der Eltern auf Aufzeichnung von Kontakten müssen gegen die Rechte der Minderjährigen auf Wahrung ihrer Privatsphäre abgewogen werden.

2.9. Kontrolle von Straftätern

Ortungsdienste können auch zur Überwachung von Straftätern auf Bewährung bzw Freigang oder sogar Untersuchungshäftlingen („elektronische Fußfessel"[13]) verwendet werden. Dabei müssen die Datenschutzrechte der Betroffenen gegen die öffentlichen Rechte an der Kontrolle abgewogen werden.

Andererseits bietet die „elektronische Fußfessel" eine interessante Alternative zur Strafhaft, wenn damit verhindert werden kann, dass ein bisher unbescholtener Übeltäter im Gefängnis erst richtig kriminell wird.

Die Freiwilligkeit der Zustimmung – falls keine gesetzliche Grundlage für die Anwendung vorhanden ist – stellt bei Personen, die einer Strafmaßnahme zugeführt werden, immer ein Problem dar.

Derzeit ist die Technik noch teuer, aber wenn die Kosten für GPS und Mobilfunk weiter sinken, kann die elektronische Fußfessel auch ein Beitrag zur Senkung der Kosten für Gefängnisunterbringung sein. Beim Eingriff in Grundrechte aus Gründen der Kostenersparnis ist die Angemessenheit der Maßnahme immer ein Problem. Weiters kann es zum exzessiven Einsatz gegen Personen kommen, die normalerweise nicht eingesperrt würden (zB notorische Ruhestörer, rückfällige Kleinkriminelle etc).

Die Technik muss auch sehr sicher gegen Manipulation sein, damit ein Verdächtigter nicht die „Fußfessel" entfernen und fliehen oder eine weitere Straftat begehen kann.

2.10. Community Services

Dienste, die Personen gestatten, sich zu treffen und miteinander zu kommunizieren, gibt es bereits im Internet. Mit Hilfe von Ortungsdaten

---

[12] Ein Beispiel ist der „GPS personal locator for children" der Firma Wherify: http://www.wherify.com/prod_watches.htm.

[13] Eine Pilotprojekt finden Sie unter http://www.bewaehrungshilfe.de/fu1.htm.

lässt sich diese Art von Dienst auf geographische Regionen übertragen. Man erhält ein Signal, wenn ein Freund in der Nähe ist.

Es ist auch möglich, einen Dienst für „Blind Dates" aufzubauen, bei dem die Benutzer ihre persönlichen Interessen eingeben, und wenn zwei Personen mit zueinander passenden Interessensprofilen am selben Ort sind, erhalten beide ein Signal, und werden zusammengeführt.

- Die Siemens-Tochter Mobile Family (www.mobile-family.com) plant ein Familien-Kommunikationssystem mit Ortung.
- Der Handynetzbetreiber maxmobil hat den „Friendfinder" eingeführt, ein Ortungssystem auf freiwilliger Basis.

Derzeit sind solche Dienste noch Spielereien, aber wenn die Benutzer auf den Geschmack kommen, lässt sich damit Geld verdienen. Dem Wunsch der Beteiligten nach Wahrung ihrer Privatsphäre gegenüber dem Handynetzbetreiber und etwaigen Partnern steht der Bedarf an Schutz gegenüber unseriösen Teilnehmern gegenüber; Die Sicherheitsbehörden werden rasch ein Interesse an Logfiles entwickeln, zB im Zusammenhang mit Clubbings, wo mit Drogen gedealt wird.

3. Rechtsgrundlagen?

Die gemeinsame Standpunkt im Ratsdokument Nr 15396/2/01 vom 28. Jänner 2002 („Common Position adopted by the Council on 28 January 2002 with a view to the adoption of a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector"[14]) enthält in Art 9 eine Bestimmung über den Gebrauch von Standortdaten („Location Data"). Standortdaten, die nicht zu den Verkehrsdaten gehören, dürfen nur mit Zustimmung für „Dienste mit Zusatznutzen" verwendet werden. Die Frage der Zustimmung kann leicht zu einem Morast aus internationalem Privatrecht, umfangreichen AGB's und unvorsichtigen Anwendern werden. Die Gefahr, dass Anwender nicht mit der notwendigen Sorgfalt die AGB's studieren, scheint bei mobilen Anwendungen besonders hoch, weil damit zu rechnen ist, dass die Anwender Dienste anfordern, ohne sich lange mit dem Studium von Verträgen aufzuhalten. Die optimale Lösung wird wohl eine Kombination aus einfachen Zustimmungs- und Widerrufregeln, zuverlässigen Protokollen für die Bezahlung

[14] http://www.europarl.eu.int/commonpositions/2002/pdf/c5-0035-02_de.pdf.

und strengen rechtlichen Regelungen gegen die Übervorteilung der Anwender sein. Dazu können ua Regeln gehören, die auf dem bestehenden Regeln über verborgene oder gröblich benachteiligende Vertragsklauseln (§ 879 Abs 3 ABGB) aufbauen.

Leider hat die Erfahrung mit Dialerprogrammen gezeigt, welche Missbräuche mit kostenpflichtigen Zusatzdiensten im Telekombereich möglich sind. Dialer sind Programme, die auf einem Computer installiert werden und dann die bisherige Einwahlnummer auf eine kostenpflichtige Mehrwertnummer ändern, für die der Inhaber des Telefonanschlusses[15] zu bezahlen hat. Prinzipiell sind Dialer nicht illegal; der Missbrauch beginnt, wenn Kunden dazu gebracht werden, einen Dialer zu installieren, der entweder gar nicht erwünscht war[16] oder der hohe Kosten verursacht, die in keinem Verhältnis zur der Leistung stehen, die der Anbieter des Dialers liefert.[17].

Notdienste werden sich auf die entsprechenden Bestimmungen im Datenschutzgesetz berufen können (§§ 1 Ab. 2, 8 Abs 3 Z 3 und 9 Z 7 DSG 2000).

Weitere Information

http://www.lbszone.com/index.html
http://www.mobilein.com/location_based_services.htm
http://www.magic-e.co.uk/location_services.htm
http://www.locationforum.org/
http://www.netlight.se/positioning.html
http://www.trueposition.com/

---

[15] Dies ist der Teilnehmer nach § 87 Abs 3 Z 2 TKG, BGBl I Nr 100/1997.

[16] Der Dialer wird als „Sicherheitsupdate", Spiel oder sonstige Software ausgegeben.

[17] Dialer werden häufig als Methode der Bezahlung für Porno-Websites eingesetzt, wobei es leicht ist, für geringfügige Leistungen exorbitante Kosten zu verrechnen.