Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 11. Jahrgang, Heft 2, Juni 2011

Schwerpunkt:

Location Based Services

fokus: Datenschutz in ortsbasierten Diensten
fokus: Location Privacy in RFID-Systemen
report: Offene Deklaration von Web Analytics

Schulthess §

inhalt

fokus

Schwerpunkt:
Location Based Services

Datenschutz in ortsbasierten Diensten

Ortsbasierte Dienste ermöglichen eine Nutzung von Mobiltelefonen als persönliche Informationsquelle und helfen dabei, die für eine Person relevante Information aus der Datenflut des Internets herauszufiltern. Der Autor erklärt die Probleme von ortsbasierten Diensten und erläutert mögliche Lösungsansätze.

Datenschutzgerechte ortsbasierte Dienste

Bei vielen ortsbasierten Diensten besteht die Gefahr, dass die Diensteanbieter exzessiven Zugang zu den personenbezogenen Daten über die Nutzer erhalten. Wie können ortsbasierte Dienste rechts- und datenschutzkonform gestaltet werden?

Location Privacy in RFID-Systemen

RFID-Systeme ermöglichen die automatische drahtlose Identifikation von Objekten und stellen eine allgegenwärtige Technologie mit zahlreichen Anwendungsmöglichkeiten dar. Welches sind die Sicherheits- und Datenschutzanforderungen an solche Anwendungen?

Schutz von Lieferketten mit RFID-Tags

Das Einschleusen von Fälschungen stellt heute eine grosse Gefahr für Warenlieferketten dar. Das System «Tracker» setzt einfache RFID-Tags als Ersatz für herkömmliche Barcodes ein, um Lieferketten gegen eingeschleuste Fälschungen abzusichern und ausserdem neugierige Mitbewerber davon abzuhalten, die eigene Warenlieferkette auszuspähen.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Offene Deklaration von Web Analytics

Website-Betreiber sammeln und analysieren eine Fülle an Daten, ohne dies offen zu deklarieren. Datenschutz-Gütesiegel wie EuroPriSe erhöhen die Transparenz beim Einsatz von Web Analytics.

Häusliche Gewalt

StPO und OHG regelten die Mitteilung von Name und Adresse von Opfern an eine Beratungsstelle abschliessend und damit bleibe für kantonales Recht kein Raum, kritisieren Kettiger/Schwander einen in digma 2010.4 erschienenen Artikel von Glockengiesser/Stämpfli. Stimmt nicht ganz, wenden die beiden Autorinnen des ersten Beitrages ein, und weisen darauf hin, dass in Fällen von häuslicher Gewalt ausserhalb des Geltungsbereichs der StPO durchaus kantonaler Regelungsspielraum und -bedarf besteht.

Raserei auf der Strasse

Wer mit seinem Auto auf der Strasse zu schnell unterwegs ist, riskiert, geblitzt zu werden. Höchste Zeit, dass das Strassenverkehrsgesetz geändert und die Höchstgeschwindigkeit abgeschafft werden. Eine abwegige Argumentation? Mitnichten, wenn man die Reaktion auf ein Bundesverwaltungsgerichtsurteil zu einer anderen «Raserei auf der Strasse» hört …

Datenschutz in ortsbasierten Diensten

Über Gefahren für die Privatsphäre und die Chancen bei sinnvollem Umgang mit ortsbasierten Diensten

Martin Werner, Wissenschaftlicher Mitarbeiter am Lehrstuhl Mobile und Verteilte Systeme, Ludwig-Maximilians-Universität München, München, Deutschland martin.werner@ifi.lmu.de

Ortsbasierte Dienste sind kleine Helfer bei vielen Alltagsaufgaben. Sie bergen aber mitunter Risiken für die Privatsphäre, die leicht übersehen werden.

Ortsbasierte Dienste sind in den letzten Jahren durch die weite Verfügbarkeit von mobilem Internetzugang und Positionierungssystemen wie GPS zu einem Massenphänomen geworden. Insbesondere im Bereich von Mobiltelefonen wird seit langer Zeit versucht, die Bedienbarkeit des Systems durch Ortsinformation zu verbessern.

Die grundlegende Idee ist, dass ein Dienst nur Ergebnisse zurückliefert, welche für den Aufenthaltsort des Nutzers relevant sind. Darüber hinaus gibt es die Möglichkeit, einen Dienst erst dann zu erbringen, wenn sich der Benutzer an einem bestimmten Ort befindet. Diese Art von Diensterbringung bezeichnet man als proaktiv: Der Dienst reagiert nicht nur auf den Benutzer, sondern der Benutzer wird vom Dienst über relevante Informationen informiert. Dieser Unterschied der Diensterbringung ist etwa mit der Möglichkeit bei Online-Immobilienbörsen zu vergleichen, entweder eine spontane Suchanfrage zu stellen, die auf eine spontan gestellte Frage eine Antwort generiert, oder eine Suchanfrage zu speichern, die dann regelmässig neue Ergebnisse per E-Mail zurückliefert.

Um die Gestalt und den Inhalt von ortsbasierten Diensten besser verstehen zu können, werden im Folgenden einige sehr beliebte Dienste kurz erläutert.

Ortsbasierte Dienste

Der Dienst *Facebook Places*[1] steht unter dem Motto «Teile mit, wo Du dich gerade aufhältst!». Es handelt sich um einen Dienst, der es Mitgliedern des Sozialen Netzwerkes Facebook ermöglicht, den eigenen Aufenthaltsort über das soziale Netz bekannt zu geben. Interessanterweise wird hier auch mit einer Funktion geworben, mit der man Facebook-Freunde markieren und deren Aufenthalt am selben Ort in seiner Statusmeldung veröffentlichen kann. Sicherlich ist die Nutzung dieser Möglichkeit eine schwere Verletzung der Persönlichkeitsrechte der betroffenen Facebook-Freunde. Diese müssen nämlich nicht vorher und bewusst ihr Einverständnis mit der Veröffentlichung dieses Ortes aussprechen. Der Dienst *Facebook Places* ist ein klassischer proaktiver Dienst, da die Facebook-«Freunde» aktiv darüber informiert werden, dass ich mich jetzt am besagten Ort aufhalte.

Google Maps[2] ist ein weit verbreiteter ortsbasierter Dienst, welcher mittlerweile neben der Anzeige von qualitativ hochwertigen Karten und Informationen zu interessanten Punkten und einer integrierten ortsabhängigen Suche auch Navigationsdienste ermöglicht. Dieser Dienst ist im Gegensatz zu Facebook Places ein klassischer reaktiver Dienst. Er benötigt meine Aufmerksamkeit und überträgt eher keine Informationen im Hintergrund.

Die Dienste *Gowalla*[3] und *Foursquare*[4] erlauben es den Nutzern ähnlich zu Facebook Places, sich an einem Ort «einzuchecken» und damit den eigenen Aufenthaltsort bekannt zu geben. Diese Dienste ermöglichen einen ähnlichen Funktionsumfang wie Facebook Places, allerdings ohne die zwingende Verkettung mit einem sozialen Netzwerk.

Die Firma *Aloqa*[5] hat einen verhältnismässig datenschutzfreundlichen, proaktiven Dienst entwickelt, mit dem relevante Informationen über die Umgebung automatisch oder auch in manueller Interaktion geladen und angezeigt werden können. Der Schwerpunkt liegt hier bei der Auffindung von interessanten Orten (etwa Geldautomaten einer bestimmten Bank oder Bushaltestellen mit Abfahrtszeiten). Dieser Dienst unterscheidet sich von vielen Konkurrenten darin, dass er ein hochentwickeltes und wissenschaftlich fundiertes Framework zum Management von Ortsdaten verwendet.

Als letzten grossen Bereich ortsbasierter Dienste seien mobile Marketing-Plattformen wie

Coupies[6] genannt, über die ein Anbieter Gutscheine und Coupons ortsbasiert und digital verteilen kann.

Damit diese Systeme das Leben der mobilen Nutzer tatsächlich vereinfachen, muss die zusätzliche Informationsquelle des Ortes (oder auch andere Messdaten über die Umgebung des Nutzers) automatisch erfasst und verwendet werden. Schliesslich ist eine gespeicherte Suchanfrage auch recht nutzlos, wenn die Suche immer noch manuell angeworfen werden muss.

Auf dem Handy gewinnen solche Dienste insbesondere dadurch an Attraktivität, dass die Eingabe von komplexen und vollständigen Suchanfragen über eine Bildschirmtastatur oder gar einen Ziffernblock in der Praxis kaum möglich ist. Wenn man die Apotheken im direkten Umkreis mit einer Websuche finden will, wird man eine Suchanfrage wie «Apotheke +München» eingeben. Mit einer ortsbasierten Suche, wie sie zum Beispiel in *Google Maps* möglich ist, reicht die Eingabe der ersten drei Buchstaben «Apo». Eine allgemeine Websuche nach Texten, die «Apo» enthalten, würde natürlich so viele unbrauchbare Treffer zurückliefern, dass eine Verwendung zur Auffindung von Apotheken kaum noch möglich ist.

Problematik

Im Hinblick auf den Schutz der individuellen Privatsphäre werden solche Systeme dann problematisch, wenn wiedererkennbare Eigenschaften des Nutzers (im einfachsten Fall der Name, bisweilen aber auch nur technische Informationen wie Netzwerkadresse oder die vom Hersteller eindeutig festgelegte Geräte-ID des Mobiltelefons) ebenfalls zur Diensterbringung verwendet werden. Dann kann nämlich durch den beschriebenen Automatismus der Übertragung von Ortsinformation für die Erbringung von proaktiven Diensten ein sehr genaues Verhaltensbild und Bewegungsprofil des Nutzers abgeleitet werden. Der Kern des Problems liegt aber auch hier tiefer: Der Nutzer ist sich in der Regel nicht einmal bewusst, dass diese Information über ihn übertragen und angesammelt wird, weil er ja gerade keinen für den Laien erkennbaren Dienst nutzt.

Diese Situation ist in jüngster Vergangenheit mehrfach zu Klagen gegen Anbieter von Diensten eskaliert. Die meiste öffentliche Aufmerksamkeit wurde hier einem der bekanntesten Premium-Anbieter geschenkt: Apple. So meldete die Süddeutsche Zeitung[7] am 29.12.2010: «[…] Weil Apple-Geräte angeblich ungefragt Nutzerdaten sammeln und weitergeben, gehen vier Kunden gerichtlich gegen den Konzern vor. Auch App-Entwicklern droht Ärger. […]». Kern dieser Klage ist der Vorwurf, dass der Konzern Apple persönliche Daten, die durch das iPhone oder das iPad erfasst werden, ohne das Wissen der Nutzer an Firmen u.a. der Werbebranche weitergebe. Neben Apple richtet sich diese Klage auch gegen einige Hersteller von Programmen für diese Smartphone-Plattform, die ebenfalls Nutzerdaten ungefragt übertragen.

An dieser Stelle sei darauf hingewiesen, dass auch andere Hersteller von Programmen und Geräten wie Google regelmässig mit ähnlichen Datenschutzvorwürfen konfrontiert sind. So steht beispielsweise der Browser *Chrome*[8] von Google von Anfang an im Verdacht, nur der Gewinnung von Nutzerinformation gewidmet zu sein. Auch das kostenlose Nutzungsanalyse-Tool *Google Analytics* ist ein Dienst, der ohne Interaktion mit dem Benutzer Daten über einen Besuch auf einer beliebigen Webseite, die dieses Tool verwendet, ohne Zustimmung des Nutzers an Dritte (nämlich Google) übermittelt. Die hierbei erfassten Informationen stellen in der Regel persönliche Daten dar und dürfen daher nicht ohne die bewusste Zustimmung des Nutzers verwendet werden.

Der Nutzer ist sich nicht einmal bewusst, dass diese Information über ihn übertragen und angesammelt wird, wenn er keinen für den Laien erkennbaren Dienst nutzt.

Detaillierte Informationen über den Datenschutz bei Google Analytics finden sich auf der Wikipedia-Seite zu Google Analytics[9] und den dortigen Verweisen. Zum Datenschutz bei Googles Smartphone-Betriebssystem *Android* findet sich dann leider nur die eher nutzlose Analyse[10], dass Google-Handys genauso viel Information an

Kurz&bündig

Ortsbasierte Dienste ermöglichen eine Nutzung von Mobiltelefonen als persönliche Informationsquelle und helfen dabei, die für eine Person relevante Information aus der Datenflut des Internets herauszufiltern. Allerdings müssen bei der Freigabe des persönlichen Aufenthaltsortes durch den Nutzer einige schwierige Entscheidungen getroffen werden, die mitunter nicht einfach sind. So kann man nicht immer erkennen, wann und wie ein Dienst persönliche Daten verarbeitet, und daher auch nicht fundiert bewerten, welche Risiken daraus entstehen. Obwohl es einige ausgereifte technische Möglichkeiten gibt, ortsbasierte Dienste auf einem gehobenen Niveau im Hinblick auf Datensicherheit und Privatsphäre zu betreiben, fehlt es oft an der Sensibilität der Nutzer und damit am Druck für die Anbieter, diese Techniken auch einzusetzen. Dieser Artikel erklärt die grundlegendsten Probleme von ortsbasierten Diensten und erläutert mögliche Lösungsansätze.

Google schicken, wie die Geräte anderer Hersteller, auf denen diese Google-Dienste verwendet werden. Diese Sichtweise – so nutzlos sie zunächst aussieht – ist aber die korrekte: Man muss die Programme, die auf einem Smartphone installiert und benutzt werden, einzeln untersuchen und bewerten.

Die Probleme für den Datenschutz auf mobilen Geräten kann man aber nur verstehen, wenn man sich eingehend mit der Motivation für die vorherrschende Praxis der Datensammlung beschäftigt. Schliesslich ist das Sammeln und Speichern von persönlichen Daten zunächst auch ein immenser Aufwand für die Unternehmen, und die rechtlichen Unsicherheiten und internationalen Unterschiede vergrössern diesen Aufwand noch wesentlich. Dass diese Nachteile nicht überwiegen, begründet sich in der derzeitigen Finanzierungsstruktur des Internets: Viele Dienste werden kostenlos angeboten, wobei kostenlos nur bedeutet, dass keine finanzielle Gegenleistung des Nutzers erwartet wird. Die finanzielle Gegenleistung wird derzeit im Wesentlichen durch die Werbebranche erbracht, die für zielgruppengerichtete Werbung immense Summen bezahlt. So erwirtschaftete Google laut Geschäftsbericht[11] im vierten Quartal 2010 etwa 5,67 Milliarden US-Dollar durch Werbung auf den eigenen Internetseiten und über Werbung auf Partnerseiten weitere 2,49 Milliarden US-Dollar. Diesen immensen Summen steht natürlich gegenüber, dass die Werbung auf Google-Webseiten sehr effizient funktioniert, weil die Profilinformationen und die Suchanfragen in die Auswahl geeigneter Werbeanzeigen integriert werden. Die Grundlage hierfür ist allerdings die Kenntnis der Vorlieben der Nutzer.

Bei den ortsbasierten Diensten, bei denen dem Nutzer nicht klar ist, wann und wie genau ihre persönlichen Informationen verarbeitet werden, ist mit Missbrauch zu rechnen.

Gefahren

Trotz aller Gefahren sind ortsbasierte Dienste ein notwendiges Instrument, um die Bedienbarkeit von mobilen Endgeräten zu verbessern und den Informationshunger der Allgemeinheit effizient zu stillen. Aufgrund der Finanzierungsstruktur des kommerziellen Internets ist bei kostenlosen Diensten jedoch Vorsicht geboten. Glücklicherweise gibt es aber auch eine Menge ortsbasierter Dienste und ortsbasierter Techniken, die die übertragene und ausgetauschte Information minimieren und anonymisieren und so die Nutzung von ortsbasierten Diensten mit weniger Problemen für die Privatsphäre ermöglichen.

Die Gefahren, welche sich aus der Nutzung von ortsbasierten Diensten ergeben, gliedern sich in zwei Klassen: Gefahren für das Individuum und Gefahren für die Gesellschaft.

Gefahren für die Gesellschaft

Die Gefahren für die Gesellschaft liegen hauptsächlich darin, dass die Nutzung eines ortsbasierten Dienstes in aller Regel Informationen zum Anbieter zurückspielt, mit welchen er seinen Dienst optimieren kann. Derjenige Anbieter, welcher zum Zeitpunkt der Verbreitung der Funktion schon den besten Datenbestand hat, wird durch die Nutzung gestärkt, insbesondere weil dieser Anbieter mehr Einnahmen mit Werbung machen kann. In diesem Markt können sich dann in aller Regel keine anderen Dienstanbieter effektiv platzieren und dieser Dienstanbieter erarbeitet sich so eine monopolartige Stellung. Da nun die Konkurrenten keine vergleichbaren Dienste mehr anbieten können und Dienste, die die Beschaffung von Informationen ermöglichen, sicherlich irgendwann zur kritischen Infrastruktur gezählt werden müssen, besteht die Frage, ob und wie man den Missbrauch der Vormachtstellung solcher Anbieter effektiv verhindern kann und soll.

Eine andere gesellschaftliche Gefahr besteht in der Ausnutzung der gesammelten Information zu Zwecken, für welche diese Informationen nicht von den Benutzern zur Verfügung gestellt wurden.

So hat etwa Israel – laut einer Meldung der Jerusalem Post[12] vom 23.11.2010 – die Daten des sozialen Netzwerkes Facebook durchsucht, um zu überprüfen, ob Frauen, die den Kriegsdienst mit Hinweis auf eine besonders strenge Einhaltung des Sabbat verweigert haben, diesen religiösen Lebenswandel auch tatsächlich pflegen. Hierbei wurden Party-Einladungen für Freitagabend verschickt (der Abend des Freitags zählt im strengen jüdischen Glauben bereits zum Sabbat) und Bilder überprüft, ob sie Indizien gegen strenggläubige Lebensweise enthalten.

Insbesondere bei den ortsbasierten Diensten, bei denen dem Nutzer im Allgemeinen nicht klar ist, wann und wie genau ihre persönlichen Informationen verarbeitet werden, ist mit ähnlichem Missbrauch zu rechnen.

Gefahren für den Einzelnen

Aus der Nutzung von ortsbasierten Diensten ergeben sich allerdings auch direkte Gefahren für die einzelnen Nutzer. So kann zum Beispiel durch die Profilierung und den Verkauf oder Diebstahl dieser Profildaten so viel über das Verhalten einer

Einzelperson in Erfahrung gebracht werden, dass eine persönliche Gefährdung im Hinblick auf Einbruch, Diebstahl und Betrug recht gross wird. So wurden Fälle von Einbruchdiebstahl gemeldet[13], bei denen die Einbrecher die Abwesenheitsmeldungen auf den Seiten von sozialen Netzwerken verwendet haben.

Notwendiger Schutz

Diese grundlegenden Probleme sind schon lange Gegenstand intensiver Forschung sowohl im Bereich der Informatik und Kryptografie als auch im Bereich der Gesellschaftswissenschaften. Bereits im Jahr 2002 hat das Europäische Parlament in der Direktive 2002/58/EC[14] die Gefahren von ortsbasierten Diensten für die Privatsphäre öffentlich zu bedenken gegeben. In Deutschland regelt das Telemediengesetz unter anderem die Verarbeitung von personenbezogenen Daten durch IT-Dienste. Kern des Gesetzes ist die Pflicht des Anbieters, den Nutzer über die erhobenen Daten aufzuklären und eine bewusste und eindeutige Zustimmung einzuholen.

Damit hat der Gesetzgeber im Wesentlichen die Ergebnisse diverser wissenschaftlicher Studien in Recht umgesetzt, nach denen ein akzeptabler ortsbasierter Dienst die folgenden Eigenschaften mindestens haben muss[15]:

- Der Benutzer wird in Echtzeit über möglicherweise die Privatsphäre einschränkende Operationen informiert.
- Der Dienst erlaubt eine einfache und schnelle, kurzzeitige Deaktivierung.

Wenn wir die heutigen ortsbasierten Dienste im Hinblick auf obige Eigenschaften betrachten, so wird klar, dass kaum ein kommerzieller Dienst diese Anforderungen erfüllt. Dies hat neben der erwünschten Verschleierung der Gefahren auch den Grund, dass die Präsentationsfläche auf mobilen Endgeräten und PCs beschränkt und der Dienst somit in der Anwenderfreundlichkeit eingeschränkt ist: Die durch den Dienst erbrachte Information wird automatisch schwieriger zu erkennen.

Bezüglich der zweiten Forderung kann man sicherlich sagen, dass durch die Gestaltung von Benutzerschnittstellen und das Verstecken von Konfigurationseinstellungen, die insbesondere den Transport von Ortsinformation betreffen, eine einfache Deaktivierung nicht immer möglich ist. Bei einigen Produkten kann man sogar nur die Applikation deinstallieren. Von dieser Option wird man aber für eine kurzzeitige Unterbrechung der Dienstnutzung keinen Gebrauch machen, weil dabei natürlich sämtliche Einstellungen verloren gehen.

Im Zusammenhang mit den Datenschutz-Vorwürfen gegen Apple hat sich unter anderem auch die deutsche Bundesjustizministerin Leutheusser-Schnarrenberger[16] zu Wort gemeldet und gefordert, dass zum einen die Benutzer von Apple-Geräten besser informiert werden und Datenschützer die Speicherung und Verwendung dieser Daten überwachen. Sicherlich wäre dies eine interessante Idee, allerdings ist unwahrscheinlich, dass man durch solche Regelungen dem Problem entgegentreten kann. Denn es ist davon auszugehen, dass die Kosten für die Überwachung den Nutzen übersteigen und ein solcher Eingriff in die unternehmerische Freiheit wegen der Ineffizienz nicht gerechtfertigt ist.

Schutztechniken

Helfen kann an dieser Stelle nur ein gut informierter Nutzer, der die notwendigen Werkzeuge erhält, um sich vor den Gefahren solcher Dienste zu schützen. In der Forschung werden dazu Mechanismen entwickelt, die dabei helfen, die Privatsphäre bei ortsbasierten Diensten zu schützen. Ein einfaches Beispiel solch datenschutzfördernder Technologien sind Schalter, mit denen die Übertragung von Ortsinformation abgeschaltet werden kann. Solche einfachen Schalter finden sich mittlerweile auch in den meisten gängigen Smartphones und lassen sich so platzieren, dass man sie schnell und einfach bedienen kann.

Eine grundsätzliche Studie[17] aus dem Jahr 2009 hat festgestellt, dass solche technischen Hilfsmittel von Nutzern tatsächlich verwendet werden. Die schlechte Nachricht aus dieser Forschungsarbeit liegt allerdings darin, dass alle Hilfsmittel, die die permanente Aufmerksamkeit des Benutzers benötigen, in der Praxis fehlschlagen. Als Ergebnis kann man insgesamt also festhalten, dass bei Diensten, die die permanente Aufmerksamkeit des Benutzers nicht erfordern, die Privatsphäre grundsätzlich nur durch automatische Mechanismen geschützt werden kann.

Helfen kann nur ein gut informierter Nutzer, der die notwendigen Werkzeuge erhält, um sich vor den Gefahren solcher Dienste zu schützen.

Anonymisierung

Eine etwas komplexere grundsätzliche Philosophie besteht in der Übertragung von systematisch verfälschten Ortsinformationen[18]. Diese verfälschte Ortsinformation kann dann natürlich in aller Regel nicht mehr einem tatsächlichen Aufenthaltsgebiet zugeordnet werden. Ein Dienst kann aber in diesem verfälschten Gebiet unter-

suchen, wie zwei (oder mehr) Teilnehmer zueinander stehen. So könnte man zum Beispiel die Anfragen an einen Dienst stets irgendwo mitten in den Pazifik verlegen und dennoch (bei Verwendung einer gemeinsamen und geheimen Verfälschungsregel) die Distanz zwischen den verschiedenen Teilnehmern berechnen. Ein anderer Ansatz besteht in der Sicherstellung von sogenannter *k*-Anonymität. *k*-Anonymität bezeichnet ein populäres Mass für Anonymität im Sinne der Ununterscheidbarkeit von Individuen in einer Gruppe. Eine übertragene Information ist *k*-anonym, wenn sie sich nicht von *k-1* anderen übertragenen Informationen unterscheidet. Es ist bei der Übertragung von Ortsinformation immer möglich, *k*-Anonymität herzustellen. Dazu muss man nur einen ausreichend grossen Bereich auswählen und über ein gemeinsames Verfahren mit einem Pseudonym (ähnlich einer Postleitzahl) versehen und sicherstellen, dass alle Teilnehmer in diesem Bereich nicht ihre Position, sondern dieses gemeinsame Orts-Pseudonym übertragen.

Methoden, welche die Privatsphäre über Anonymisierung schützen wollen, scheitern allerdings an der tatsächlichen Dienstnutzung.

Leider eignen sich diese beiden Techniken nur zur Sicherstellung einer gewissen Anonymität in Diensten, bei denen keine andere Information (Kreditkarte, technische Identifikation, Account, …) mit übertragen wird. Schon ein Dienst, bei dem ein Kartenausschnitt geladen werden soll, kann mit solchen Mechanismen nicht funktionieren.

Verschlüsselung

Für diese Situation gibt es mächtige, aber wenig bekannte kryptografische Methoden. So kann man mit dem Konzept «Private Information Retrieval»[19] eine Datenbankabfrage über das Netzwerk so gestalten, dass weder ein Mithörer auf dem Netzwerk noch der Server, der die Anfrage beantwortet, den Inhalt der Anfrage oder der Antwort kennt. Allerdings ist solch ein Verfahren natürlich sehr aufwendig. Wenn ein Serverdienst nämlich keinen Hinweis auf den Inhalt der Anfrage hat, so muss er letzten Endes mehr oder weniger die gesamte Datenbank untersuchen, in welcher Weise ein Eintrag in der Datenbank für die Antwort verwendet wird. Die Rechenzeit kann hierbei durchaus die Zeit übertreffen, die benötigt würde, um die gesamte Datenbank auf den Client herunterzuladen. Somit eignen sich solche Methoden eher in Bereichen mit sehr wertvollen Datenbanken und extremen Sicherheitsanforderungen oder in Kombination mit einer räumlichen Aufteilung der Datenbank in Teildatenbanken, von denen ohne Gefahr für die Privatsphäre Daten abgerufen werden können.

Diese Methoden, welche die Privatsphäre über Anonymisierung schützen wollen, scheitern allerdings an der tatsächlichen Dienstnutzung. So kann selbstverständlich über einen längeren Zeitraum oder durch Fusion mit anderen Nutzungsdaten auf Eigenschaften oder Ort eines Nutzers geschlossen werden. Eine Applikation, welche mir mitteilen können soll, ob sich ein Freund in meiner Nähe befindet, kann natürlich mit sozialem Wissen (gegebenenfalls einfach aus einem sozialen Netzwerk) attackiert werden, indem sie mit einem gefälschten Ort verwendet wird. So kann ich erfahren, ob mein «Freund» sich an einem beliebigen Ort nicht befindet.

Vertrauen

Im Hinblick auf die hohe Rechenleistung für automatische Verfahren und die gängige Praxis, ortsbezogene Dienste mehr oder weniger ohne Rücksicht auf die Privatsphäre zu betreiben, liegt es nahe, einen relativen Schutz durch vertrauenswürdige Plattformen zu konstruieren. So könnte beispielsweise ein Anbieter als Treuhänder für Ortsinformation die permanente Verwaltung von Ortsinformation übernehmen und die teilnehmenden Dienste über Meldungen informieren. Insbesondere in dem Fall, dass diese «Trusted Third Party» solche Informationen ohnehin schon hat – so wie beispielsweise ein Mobilfunkbetreiber immer eine grobe Information über den Aufenthaltsort der Nutzer besitzt – und eine vernünftige Finanzierungsstruktur den effektiven Schutz der Daten vor Missbrauch zu einer wirtschaftlichen Einnahmequelle macht, führen solche Kon-

Literatur

- Louise Barkhuus, Privacy in Location-Based Services, Concern vs. Coolness, in: Workshop on Location System Privacy and Control, Mobile HCI. 2004.
- Thorben Burghardt/Erik Buchmann/Jens Müller/Klemens Böhm, Understanding User Preferences and Awareness: Privacy Mechanisms in Location-Based Services, in: On the Move to Meaningful Internet Systems (OTM'09), Springer 2009, 304–321.
- Michael Dürr/Martin Werner, Re-Socializing Online Social Networks, in: International Symposium on Social Computing and Networking (SocialNet'10), 2010.
- Marco Gruteser/Dirk Grunwald, Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In: Mobile Systems, Applications and Services, 2003.
- Gabriel Ghinita/Panos Kalnis/Ali Khoshgozaran/Cyrus Shahabi/Kian-Lee Tan, Private Queries in Location-Based Services: Anonymizers are not Necessary. in: Management of Data (SIGMOD), 2008, 121–132.
- John Krumm, A Survey of Computational Location Privacy, Personal and Ubiquitous Computing, 2008.
- Axel Küpper, Location-Based Services: fundamentals and operation. John Wiley & Sons, 2005.

zepte vielleicht zu einer zufriedenstellenden Lösung.

Eine weitere Möglichkeit, die Risiken beim Austausch von privaten Informationen über ein Netzwerk zu verringern, liegt in einer Änderung der grundlegenden Kommunikationsparadigmata. Während das Internet noch grösstenteils zentralisiert funktioniert, könnten Peer-To-Peer-Methoden[20] auf lange Sicht die Menge an gesammelter Information effektiv reduzieren. Bei diesen Kommunikationsmethoden findet die inhaltliche Kommunikation nur noch direkt zwischen den Kommunikationsendpunkten statt und nicht mehr über eine zentrale Plattform. Daher kann solch eine Plattform die ausgetauschten Daten nicht mehr sammeln. Leider ergeben sich daraus Probleme für solche Dienste, die auch in dem Fall Informationen zurückliefern sollen, dass der jeweilige Nutzer nicht online ist. Hier kann durch die Veröffentlichung solcher Daten auf DSL-Routern oder kostenlosem Webspace beim Internetprovider immer noch eine Verteilung der Daten erreicht werden, auch wenn dies dann mit einem höheren Aufwand verbunden ist.

Noch weiter in der Zukunft könnte dann vielleicht eine kontextabhängige und vollautomatische Kontrolle der Gefahren für die Privatsphäre durch künstliche Intelligenz auf dem Mobiltelefon ermöglicht werden. Solche Ansätze scheitern derzeit an der begrenzten Rechenleistung und auf modernen Handys, wo die Rechenleistung im Prinzip ausreichen würde, am resultierenden Stromverbrauch.

Fazit

Nach diesen kritischen Betrachtungen von ortsbasierten Diensten auf mobilen Endgeräten soll aber nochmals an die Vorteile im privaten wie geschäftlichen Umfeld erinnert werden. Eine Websuche nach einer Apotheke auf einem Handy ist ohne Übertragung von Ortsinformation kaum in vernünftiger Zeit machbar. Auch im geschäftlichen Umfeld können durch die Nutzung gut konstruierter ortsbasierter Dienste immense Wettbewerbsvorteile entstehen. Aktuelle Anwendungsfelder beinhalten Unified Communication, Zugangskontrolle oder auch Qualitätssicherung in der produzierenden Industrie. Denkbar sind aber auch automatische ortsbasierte Systeme, die helfen können, das Customer-Relationship-Management oder auch das Workflow-Management zu vereinfachen.

Auf dem Weg zum «Semantischen Web», in welchem das Internet nicht mehr über Adressen, sondern über Inhalte gesteuert wird, sind ortsbasierte Dienste und soziale Netzwerke sicherlich eine wichtige Vorentwicklung. Sie sollten daher in der Diskussion nicht verteufelt werden. Im Gegenteil, die gesellschaftlichen und persönlichen Herausforderungen in diesem Bereich müssen erkannt und angenommen werden. ■

Weiter in der Zukunft könnte vielleicht eine kontextabhängige und vollautomatische Kontrolle der Gefahren durch künstliche Intelligenz auf dem Mobiltelefon ermöglicht werden.

Fussnoten

1 <http://www.facebook.com/places/>.
2 <http://maps.google.com/>.
3 <http://gowalla.com/>.
4 <http://foursquare.com/>.
5 <http://www.aloqa.com/>.
6 <http://www.coupies.de/>.
7 <http://www.sueddeutsche.de/digital/datenschutz-bei-iphone-und-ipad-apple-kunden-klagen-wegen-vermeintlichem-datenleck-1.1041007>.
8 <http://www.datenschutzbeauftragter-online.de/google-chrome-die-intention-liegt-auf-der-hand/>.
9 <http://de.wikipedia.org/wiki/Google_Analytics>.
10 <http://www.pcwelt.de/news/Google-Datenschutz-bei-T-Mobile-G1-genauso-wie-bei-anderen-Handys-45979.html>.
11 <http://investor.google.com/earnings/2010/Q4_google_earnings.html>.
12 <http://www.jpost.com/Israel/Article.aspx?id=196426>.
13 <http://www.zeit.de/digital/internet/2010-02/einbrecher-facebook-versicherung>.
14 Directive 2002/58/ec of the European Parliament and of the Council, 2002.
15 Barkhus (2004).
16 <http://www.heise.de/newsticker/meldung/Leutheusser-Schnarrenberger-kritisiert-Apples-Datenschutzregeln-1029687.html>.
17 Burghardt/Buchmann/Müller/Böhm (2009).
18 Gruteser/Grunwald (2003).
19 Ghinita/Kalnis/Khoshgozaran/Shahabi/Tan (2008).
20 Dürr/Werner (2010).

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §