JENS-MARTIN LOEBEL

PRIVACY IS DEAD – EIN FÜNF-JAHRES-SELBSTVERSUCH DER BEWUSSTEN ORTSBESTIMMUNG MITTELS GPS

Einleitung

Die ubiquitäre Verfügbarkeit von energieautarken persönlichen Ortungsgeräten in Form von Mobiltelefonen oder Navigationssystemen erlaubt eine Vielzahl von neuen Lokalisierungsdiensten und -anwendungen, welche sich großer Beliebtheit erfreuen. Das Anwendungsspektrum reicht dabei von der elektronischen Routenführung im Auto, der Trainingsmotivation und -analyse beim Laufsport, der virtuellen Schnitzeljagd (genannt Geocaching) bis hin zur Anreicherung von Urlaubsfotos um den genauen Aufnahmeort oder die Verabredung mit Freunden über lokationsbasierte soziale Netzwerke. Durch die in die Geräte integrierte Satelliten-Empfangseinheit ist es jederzeit möglich, den genauen Standort des Gerätes – und damit den Aufenthaltsort des Nutzers – genau zu bestimmen.

Heutige mobile Geolokationsanwendungen basieren alle auf dem gleichen Prinzip und nutzen das satellitengestützte US-amerikanische NAVSTAR[1] Global Positioning System (GPS) als technische Basis.[2] Daneben kommen verschiedene Hilfssysteme zum Einsatz, die einerseits die Genauigkeit der bestimmten Position verbessern und/oder andererseits die Zeit bis zur erfolgreichen Positionsbestimmung verkürzen.

GPS-basierte Systeme haben die Gesellschaft durchdrungen, denn obwohl das Verfahren komplexe Berechnungen und eine mehrstufige Signalverarbeitung beinhaltet, ist die Nutzung des Systems denkbar einfach. Die Signalverarbeitungskette wird von einem dedizierten Hardwarechip übernommen, der die geforderten Millionen von Rechenoperationen pro Sekunde in Echtzeit durchführt. Durch Massenproduktion und damit sinkende Preise haben diese Chips Einzug in viele elektronische Geräte gehalten, wie beispielsweise mobile Navigationssysteme, Mobiltelefone sowie Fotoapparate und Kameras. Darüber hinaus sind GPS-Systeme ein wichtiger Bestandteil von Industrie und Forschung mit breit gefächertem Einsatzspektrum, wie beispielsweise in sicherheitstechnischen Anwendungen, als elektronische Fahrtenbücher, bei der See-

---

1 NAVSTAR ist ein Akronym für Navigation Satellite Timing And Ranging Global Positioning System.

2 Das europäische System *Galileo* ist derzeit im Aufbau sowie das russisches Pendant *GLONASS*. Ihre Funktionsweise ist analog zu GPS. Zudem werden die Systeme technisch zu GPS kompatibel sein. Die GPS-Empfänger von führenden Herstellern sind bereits für *Galileo* gerüstet.

notrettung und -navigation oder der Überwachung von landwirtschaftlichen Geräten.

Mit den ständig steigenden Nutzerzahlen geht jedoch auch ein erhöhtes Missbrauchspotenzial einher. So ist es prinzipiell möglich, mit den anfallenden Lokationsdaten Bewegungsprofile zu erstellen, die detaillierte Rückschlüsse über Tagesabläufe, Lebensgewohnheiten und soziale Kontakte eines Nutzers erlauben.

Um dieses Missbrauchspotenzial ins Bewusstsein zu rücken, habe ich in einem langfristig ausgelegten Versuch mithilfe mehrerer GPS-Empfänger jeden meiner Schritte im öffentlichen Raum über einen Zeitraum von fünf Jahren aufgezeichnet. Mit den so gesammelten Daten konnte ich ein eigenes umfassendes Bewegungsprofil erstellen und auswerten. Meine Fragestellungen waren dabei, welche Rückschlüsse sich aus diesen Daten auf meine Kontakte und persönliche Lebensführung ziehen lassen, wie viele Datensätze und welcher Aufzeichnungszeitraum für Vorhersagen meiner künftiger Bewegungen notwendig sind und inwieweit die bewusste Aufzeichnung meinen Lebensalltag verändert.

Um das Selbstexperiment besser zu verstehen, ist es notwendig, die technischen Hintergründe des GPS-Systems und die Problematik der verdeckten Datenübermittlung kurz zu beleuchten.

Technische Hintergründe und die Problematik der verdeckten Datenübermittlung

Das GPS-System besteht aus insgesamt 24 aktiven Satelliten, welche die Erde auf unterschiedlichen Bahnen in einer Höhe von 20.183 km zweimal innerhalb eines Sterntages (etwa 23 Stunden und 56 Minuten) umkreisen.

Das System wurde 1973 vom US-Verteidigungsministerium zur Steuerung von Kriegsgerät entwickelt und ist seit 1994 voll funktionsfähig. Die ursprüngliche Konzeption für militärische Anwendungen bedingte technische Entscheidungen, die sich in systeminhärenten Eigenschaften wie möglichst hoher Genauigkeit bei der Positionsbestimmung oder der Resistenz gegen Störungen äußern.

Wichtigstes Merkmal ist jedoch die rein passive Positionsbestimmung. So können GPS-Empfänger ihre Position allein durch die empfangenen Satellitensignale errechnen, ohne selbst Signale auszusenden. Für meinen Selbstversuch war dies von entscheidender Bedeutung. Die Positionsdaten werden autark im Empfänger berechnet und können von mir daher jederzeit und ständig mitgeschnitten werden.

Das Hauptprinzip der Positionsbestimmung bildet die indirekte Messung der Entfernung zwischen den gleichzeitig beobachteten GPS-Satelliten und der Antenne des Empfängers. Mithilfe einer eingebauten Atomuhr berechnet

jeder Satellit ständig seine orbitale Position voraus und sendet diese Daten als Ephemeriden (von griechisch „ephēmeris“: „für/an dem Tag“; sinngemäß Tagebuch bzw. Journal) zusammen mit der aktuellen Uhrzeit im GPS-Signal per Funk aus.[3] Das GPS-Gerät auf der Erde, welches ebenfalls über eine Uhr verfügt, empfängt nun gleichzeitig die Daten der über dem Horizont sichtbaren Satelliten. Zur Distanzberechnung werden die Differenzen aus der empfangenen und der aktuellen Uhrzeit gebildet. Zusammen mit den Bahnpositionen aus den Ephemeriden ließe sich so theoretisch die Entfernungen zu den jeweiligen Satelliten errechnen.

Allerdings wird das Satellitensignal auf dem Weg durch die Schichten der Erdatmosphäre gestört, verlangsamt und abgelenkt, seine Laufzeit also verändert. Die errechnete Distanz entspricht somit nicht der tatsächlichen geometrischen Entfernung, sondern stellt lediglich eine Pseudoentfernung (engl. *pseudorange*) dar.[4]

Da gewisse Codes zur Entschlüsselung des Signals geheim sind, können zivile GPS-Empfänger die Störungen insbesondere der Ionosphäre nicht herausrechnen, was die Genauigkeit der errechneten Position deutlich senkt. Sie benötigen hierfür Korrekturdaten aus anderen Systemen.

Das Funksignal selbst wird so übertragen, dass es äußerst resistent gegen ungewollte oder beabsichtige elektromagnetische Interferenzen, z. B. durch feindliche Störsender (genannt Jammer) ist.[5]

Die errechneten Pseudoentfernungen spannen eine Kugelfläche um jeden Satelliten und das Empfangsgerät auf. Rechnerisch bildet die Schnittmenge zweier dieser Kugeln einen Kreis, bei drei Kugeln erhält man zwei Schnittpunkte, wovon einer die Position des Empfängers darstellt. Der andere Schnittpunkt befindet sich in oder über der Plasmasphäre und kann daher verworfen werden. In der Praxis ist jedoch mindestens die Position einer vierten Kugel vonnöten, da die Berechnung der Pseudoentfernungen durch Laufzeitmessung eine exakte Synchronisation der Uhren von Satellit und Empfänger erfordert. Während im Satelliten eine Atomuhr arbeitet, ist die Uhr des Empfängers in der Regel deutlich ungenauer. Durch den Empfang des vierten Satelliten kann die Abweichung der Uhren genau ermittelt werden und in die Laufzeitmessung einfließen. Zur Positionsbestimmung werden daher immer

---

[3] Die verschickten Tabellen enthalten alle Angaben, um die exakte Bahnposition des Satelliten an einem beliebigen Zeitpunkt des Sterntages berechnen zu können. Notwendig dazu sind u. a. die Referenzepoche mit polynominellen Koeffizienten, die numerische Exzentrizität der Ellipse des Gangfehlers der Satellitenuhr, die Quadratwurzel der großen Halbachse der orbitalen Ellipse, die Nummer des Satelliten sowie diverse Korrekturkoeffizienten.

[4] Der betragsmäßig größte Messfehler ergibt sich durch dispersive komplexe physikalische Wechselwirkungen der Funkwellen mit der Ionosphäre (ionosphärischer Effekt). Es kommt zur Streuung und Verzerrung der Signale. Der troposophische Effekt und relativistische Effekte bilden weitere Störquellen. Vgl. Guochang Xu, *GPS – Theory, Algorithms and Applications*, 2. Aufl., Berlin, 2007, S. 2, S. 32, S. 37 f uns S. 43-67.

[5] Hierzu kommt das CDMA/Spread-Spectrum-Verfahren (Code Division Multiple Access, ein Codemultiplexverfahren mit Frequenzspreizung um eine Trägerfrequenz) zum Einsatz.

mindestens vier gleichzeitig empfangene GPS-Satelliten benötigt. Jeder weitere Satellit erhöht die Genauigkeit des Schnittpunktes und damit der ermittelten Position.

Seit der Abschaltung der zusätzlichen künstlichen Signalverschlechterung (*Selective Availability*) durch Präsident Clinton im Jahre 2000, ist die aus den offenen L1-Daten errechenbare Position auf etwa 20 bis 50 Meter genau. Dies machte das GPS-System für eine Vielzahl ziviler Anwendungen interessant. Um die Abweichung auf ein Maß von unter 10 Metern zu senken, kommen heutzutage eine Kombination von Satelliten-, Funkzellen- und internetgestützten Erweiterungssystemen zum Einsatz, welche zusätzliche Korrekturinformationen liefern. Für die satellitengestützten Systeme kommen feste, geografisch weiträumig verteilte Referenzstationen mit GPS-Empfänger zum Einsatz, welche ständig ihre errechnete Position mit der eigenen, bekannten Position vergleichen. Das Netz von Stationen beschreibt damit eine grobe Karte der ionosphärischen Störungen. Diese Informationen werden anschließend über geostationäre Satelliten in Form von Korrekturdaten ausgesendet und können von entsprechend ausgerüsteten GPS-Empfängern interpretiert werden. Dieses Differential-GPS (DGPS) genannte Verfahren wird in verschiedenen geografischen Regionen in zueinander kompatiblen Systemen betrieben.[6] Für mobile Empfangsgeräte mit Internetzugang (z. B. Smartphones) finden zusätzlich Verfahren Anwendung, mit denen sich die Zeit bis zur ersten stabilen Positionsermittlung deutlich verkürzen lässt. Eine Startverzögerung bei der ersten Positionsbestimmung ergibt sich aus der Tatsache, dass zur Berechnung und Synchronisation die vollständigen Daten der aktuellen Ephemeriden benötigt werden, welche im Regelfall erst vom jeweiligen Satelliten bezogen werden müssen. Alternativ können diese Daten aber auch von Datenbanken aus dem Internet bezogen werden.

Beim sogenannten Assisted-GPS (AGPS)[7] werden vom Empfangsgerät Zusatzinformationen, wie beispielsweise GSM-Funkzellen, mit denen ein Mobiltelefon verbunden ist oder die Hardwarekennung (*MAC-Adresse*) von in der Nähe befindlichen WLAN-Netzen erfasst.[8] Diese Daten werden nun über eine bestehende Internetverbindung an entsprechende Auskunftsdienste gesendet. Die abgefragten Datenbanken enthalten geografische Koordinaten aller Mobilfunk-Sendemasten sowie kommerzieller und privater WLAN-Netze (soweit erfasst).

Durch die Verwendung von externen kommerziellen Diensten entsteht ein Machtgeflecht zwischen Nutzer und Firma sowie ein Spannungsfeld zwischen

---

6 Bereits aktiv sind das Wide Area Augmentation System (WAAS) in Nordamerika, der European Geostationary Navigation Overlay Service (EGNOS) in Europa sowie das Multi-Functional Satellite Augmentation System (MSAS) in Japan.

7 AGPS ist seit einigen Jahren Standard im Mobilfunkbereich und in Europa und den USA flächendeckend möglich.

8 Vgl. Dodel/Häupler (2010), *Satellitennavigation*, S. 238-242.

Selbst- und Fremdaufzeichnung, welches ich mit meinem Selbstversuch zu entwirren versuche.

Die zur Positionsbestimmung notwendigen Millionen von Rechenoperationen pro Sekunde werden üblicherweise von einem dedizierten Hardwarechip im Hintergrund ausgeführt. Komplexität von Empfang, Berechnung und Decodierung des Verfahrens bleiben dem Anwender somit verborgen. Gleichzeitig führte die kostengünstige Verfügbarkeit dieser Chips zu einem hohen Verbreitungsgrad bei mobilen Endgeräten und ermöglicht so eine Vielzahl neuer nützlicher Geolokationsanwendungen und -dienste.

Kartendatum und Adressauflösung

Am Ende der Verarbeitungskette steht die ermittelte Position, bestehend aus einem Kartendatum mit Längen- und Breitengrad und Höhe über dem Meeresspiegel. Dabei gehört zu einem Kartendatum systembedingt immer auch ein aktueller Zeitstempel. Eine GPS-Positionsangabe ist also vierdimensional.[9]

Um für den Nutzer verwendbar zu sein, muss dem Kartendatum (z. B. „52° 30.87533‘ N, 13° 21.0063‘ E“) in der Regel eine sinnvolle semantische Konnotation (hier „Siegessäule, Großer Stern, Berlin, Deutschland“) zugewiesen werden. Dies geschieht über die Abfrage von Ortsdatenbanken. In jedem Fall aber wird eine digitale Karte benötigt, um die Position im geografischen Kontext anzuzeigen. Die Verwendung von Assistenzsystemen sowie die Übertragung von Lokationsdaten zum Abgleich mit Ortsdatenbanken oder Karten – zumeist über die Internetverbindung des Mobiltelefons – fügen dem rein passiven GPS-Empfang einen aktiven Rückkanal hinzu.

Verdeckte Datenübermittlung

Die abgefragten Ortsdatenbanken sind dabei größtenteils kommerziellen Ursprungs und eine Aggregation von Standortinformationen dementsprechend wertvoll. Neben kostenpflichtigen Angeboten wie z. B. der Firmen Navteq oder Tele-Atlas, bietet Google als einer der größten Anbieter sein Kartenmaterial und seine Ortsdatenbank gratis als Service im Internet an. Durch den Einsatz führt jede Ortsbestimmung oder Routenberechnung auf mobilen Geräten mit dem Google-Betriebssystem (Android), aber auch auf dem iOS-Geräten von Apple zwangsweise zu einer Übertragung der aktuellen Position an Google. Wird AGPS verwendet, wird die Position zusätzlich an den Mobilfunkbe-

[9] Die Angaben erfolgen oft in Grad und Bogenminuten nach dem World Geodetic System von 1984 (WGS-84). Dieses geodätische Referenzsystem definiert einen (in Längen- und Breitengrade eingeteilten) sogenannten Referenzellipsoid um die Erde und ihre Atmosphäre, der als einheitliche Grundlage für Positionsangaben auf der Erde und im erdnahen Weltraum dient.

treiber oder – bei WLAN-Ortung – an weitere Firmen mit Standortdatenbanken gesendet. Neben Google und Apple sei hier die Firma Skyhook Wireless (http://www.skyhookwireless.com/) als einer der größten Anbieter von WLAN-Standortinformationen erwähnt. Darüber hinaus betreiben Google und Apple als Anbieter von Betriebssystemen für mobile internetfähige Endgeräte aktiv den Aufbau und die Pflege eigener WLAN-Standortdatenbanken. Dazu werden über Telefone und andere mobile Geräte mit Google- oder Apple-Betriebssystem permanent die Gerätekennungen empfangener WLAN-Netze gesammelt und diese Informationen zusammen mit der per GPS ermittelten Position des Gerätes (anonymisiert) im Hintergrund an Google bzw. Apple übertragen.[10] So räumen beispielsweise die allgemeinen Geschäftsbedingungen (AGB) von Apple, die der Nutzer – will er die GPS-Funktionen (von Apple ‚Location Services' genannt) seines Gerätes benutzen – zwangsweise akzeptieren muss, Apple selbst, seinen Werbepartnern und allen Anbietern von Programmen aus dem App-Store das Recht zur Sammlung, Speicherung und Verarbeitung der GPS-Position ein:

> Um standortbezogene Dienste auf Apple Produkten anzubieten, können Apple und unsere Partner und Lizenznehmer präzise Standortdaten erheben, nutzen und weitergeben, einschließlich des geografischen Standorts deines Apple Computers oder Geräts in Echtzeit.[11]

Obwohl in den AGB eindeutig beschrieben, führt die Sorge um potenzielle Missbrauchsmöglichkeiten dieser Praxis seit 2010 zu Empörung und heftiger Kritik in der amerikanischen Fach- und Tagespresse[12] und bei diversen Online-Publikationen.[13] Aber auch der deutsche Bundesbeauftragte für den Datenschutz Peter Schaar sowie Bundesverbraucherschutzministerin Ilse Aig-

---

[10] Google sammelt zudem Standortinformationen und WLAN-Gerätekennungen im Rahmen seines Streetview-Programms durch den Einsatz spezieller WLAN-Empfänger und Software in den Kamerafahrzeugen, die systematisch alle Straßen einer Stadt abfahren. Der Sicherheitsexperte Samy Kamkar stellt unter http://samy.pl/androidmap/ einen Webdienst zur Verfügung, mithilfe dessen man überprüfen kann, ob das eigene (private) WLAN von Google erfasst wurde. Laut Kamkar hat Google in der Vergangenheit mehrfach versucht, den Webdienst zu blockieren.

[11] Apple Inc. (Hg.), „Apple Datenschutzrichtlinie", Teil der allgemeinen Geschäftsbedingungen, Stand vom 21. Mai 2012, auf: Apple, online unter: http://www.apple.com/de/privacy/, zuletzt aufgerufen am 25.06.2012.

[12] Vgl. u. a. David Sarno, „Apple Collecting, Sharing iPhone Users' Precise Locations", Artikel vom 21.06.2010, auf: *Los Angeles Times* (Onlineversion), online unter: http://latimesblogs.latimes.com/technology/2010/06/apple-location-privacy-iphone-ipad.html und Alasdair Allan/Pete Warden, „Got an iPhone or 3G iPad? Apple is Recording Your Moves", auf: O'Reilly radar, 20.04.2010, online unter: http://radar.oreilly.com/2011/04/apple-location-tracking.html, beide zuletzt aufgerufen am 01.09.2011.

[13] Vgl. Bobbie Johnson, „Researcher: ‚iPhone Location Data Already Used By Cops'", auf: GigaOM Blog, 21.04.2011, online unter: http://gigaom.com/2011/04/21/researcher-iphone-location-data-already-used-by-cops/, zuletzt aufgerufen am 01.09.2011.

ner verurteilten die verdeckte Übertragung von Standortinformationen in Mobiltelefonen bei der Nutzung von Geolokationsanwendungen.[14]
Dies verdeutlicht die heikle Verquickung von Identität, Person und Mobiltelefon, welches als ‚persönlicher Begleiter' immer dabei ist. Der Standort des Telefons deckt sich in vielen Fällen mit dem des Nutzers und wird intern als eigener Standort empfunden. Es entsteht eine Repräsentation des Selbst als Kartendatum. Diese ‚digitale Verdopplung' nimmt der Nutzer durch die Visualisierung der GPS-Position auf der digitalen Karte des Telefons oder Navigationsgerätes wahr. So verwenden fast alle Geräte einen Avatar (einen grafischen Stellvertreter), um die Position des Nutzers auf der Karte anzuzeigen. Apple beispielsweise blendet eine pulsierende Kugel ein, Garmin-Geräte zeigen u. a. ein (konfigurierbares) Miniaturauto, oder -boot.

Ein anderes Beispiel sind Online-Navigationssysteme für Autos, die während der Autofahrt ständig die genaue Position, Geschwindigkeit und Richtung des Fahrzeugs an den Hersteller der Navigationslösung übertragen. Diese Systeme, welche seit einigen Jahren im Gebrauch sind, gibt es entweder als dediziertes Navigationsgerät mit Anbindung an ein Mobilfunknetz oder als Software auf dem internetfähigen Mobiltelefon (Smartphone) des Nutzers. Die gesammelten Bewegungsdaten werden beim Hersteller ausgewertet, um daraus für alle Nutzer Verkehrsprofile mit entsprechenden Staugebieten für die gefahrenen Straßen zu errechnen. Die errechneten Informationen werden zurück an die Geräte gesendet und ermöglichen deutlich aktuellere und genauere Warnmeldungen zu Staus als beispielsweise Verkehrsinformationen durch den Hörfunk.[15] Auch hier stimmt der Nutzer vorher der Datenübermittlung per AGB zu. Der eigentliche Übertragungsvorgang passiert anschließend verdeckt im Hintergrund. Im Gegenzug für die aktuellen Staumeldungen erhält der Hersteller ein komplettes Bewegungsprofil des jeweiligen Nutzers.[16] Dabei besteht ein deutliches Missverhältnis zwischen dem wirtschaftlichen Wert eines kompletten Bewegungsprofils und dem Mehrwert einer akkurateren Stauumfahrung.

Der technisch einfache und oft verdeckte Zugriff auf diese Standortdaten weckt Begehrlichkeiten in der Privatwirtschaft. Insbesondere die Nutzung von Positionsdaten oder ganzer Bewegungsprofile für individualisierte und standortbezogene Werbung, genannt ‚Mobile Ad Targeting', steht hier im Vorder-

---

[14] Vgl. Carsten Meyer, „Datenschutzbeauftragter warnt vor Missbrauch bei Handy-Ortung", Artikel vom 30.05.2010, auf: *Heise-Newsticker*, online unter: http://heise.de/-1010712, zuletzt aufgerufen am 01.09.2011.

[15] Die Hersteller TomTom und Garmin vermarkten diese Funktion unter dem Namen „HD Traffic" (TomTom) bzw. „nüLink!-Online-Services" (Garmin). Vgl. http://www.tomtom.com/de_de/services/live/hd-traffic/ und http://www.garmin.com/de/products/strassennavigation/nulink/, zuletzt aufgerufen am 15.10.2011.

[16] Vgl. Kate Greene, „Staumeldung gegen Bewegungsprofil", Artikel vom 25.11.2008. auf: *Technology Review* (Online Version), online unter: http://www.heise.de/tr/artikel/Staumeldung-gegen-Bewegungsprofil-275834.html, zuletzt aufgerufen am 01.09.2011.

grund.[17] Für Privatunternehmen bringt eine solche Überwachung der Kunden viele Vorteile. Das Missbrauchspotenzial ist dementsprechend hoch. So berichtete auf *Zeit Online* ein Beta-Tester des geplanten elektronischen Ticketsystem *Touch&Travel* der Deutschen Bahn von seinen Erfahrungen mit dem System. Dieses basiert auf einer Applikation für internetfähige Mobiltelefone, mit deren Hilfe Nutzer elektronische Bahntickets direkt auf dem Handy erwerben können. Dazu ist nur die An- und Abmeldung unter Eingabe von Start- und Zielbahnhof erforderlich. Als er vergaß sich abzumelden, bekam er jedoch eine Mail der Deutschen Bahn, die seinen aktuellen Standort enthielt. Die Applikation nutzte anscheinend die GPS-Funktion seines Mobiltelefons:

> Offensichtlich wusste *Touch&Travel*, wo ich mich befand, als ich mich nachträglich ausloggte. Die App hatte die Position meines Handys an die Bahn übermittelt und den automatisch bestimmten Aufenthaltsort (Bielefeld) mit meiner manuellen Angabe (Berliner Hauptbahnhof) abgeglichen.[18]

Die AGB erlauben der Deutschen Bahn sogar die Erstellung eines Profils, auch wenn die Anwendung nicht aktiv ist:

> Das System verfolgt, mit welchen Funkzellen des Handynetzes sich mein Smartphone verbindet. Und das auch, wenn die *Touch&Travel*-App gar nicht aktiv ist. Die Bahn speichert also ganze Bewegungsprofile, während ich unterwegs bin.[19]

Welchen Stellenwert Lokationsdaten haben, zeigt exemplarisch der 2010 durch die Firma Symantec entdeckte Trojaner ‚AndroidOS.Tapsnake' für das Android-Betriebssystem. Dieser tarnt sich als Handyspiel und überträgt verdeckt die Positionsdaten des Telefons. Der Empfänger kann dabei vom Angreifer frei konfiguriert werden.[20] Aber auch für den Staat sind die Bewegungsdaten seiner Bürger von Interesse, wie sich am Beispiel der jüngst gestellten Forderung nach einer GPS-gestützten PKW-Maut zeigt.[21]

Paradoxerweise erlangt hauptsächlich der Dienstanbieter – nicht der Nutzer selbst – durch die Aggregation der im Gerät anfallenden Daten Wissen über den Nutzer. Während die Auswertung der Daten – und damit Rückschlüsse auf das eigene Verhalten zur Ermöglichung einer Selbstreflexion – auf den Endgeräten nur sehr begrenzt möglich ist, verfügt der Dienstanbieter über um-

---

[17] Apple bietet Nutzern die Möglichkeit der Verwendung ihrer Daten für standortbezogene Werbung zu widersprechen (Opt-Out). Dazu muss einmalig vom jeweiligen iOS-Gerät die Adresse http://oo.apple.com aufgerufen werden.

[18] Sebastian Horn, „Handy-Fahrschein: Von der Deutschen Bahn verfolgt", 27.09.2011, auf: *Zeit Online*, online unter: http://www.zeit.de/digital/2011-09/bahn-fahrschein-berlin, zuletzt aufgerufen am 01.10.2011.

[19] Ebd.

[20] Vgl. Sophie Curtis, „GPS Tracking Trojan Hidden In Android App", 17.08.2010, auf: *eWeek Europe*, online unter: http://www.eweekeurope.co.uk/news/gps-tracking-trojan-hidden-in-android-app-9048, zuletzt aufgerufen am 15.10.2011.

[21] Vgl. Achim Barczok, „Kretschmann will satellitengestützte PKW-Maut", Artikel vom 16.10.2011, auf: *Heise-Newsticker*, online unter: http://heise.de/-1361871, zuletzt aufgerufen am 15.10.2011.

fangreiche Werkzeuge zur Speicherung und Auswertung der aggregierten Profildaten. Es offenbart sich ein deutliches Ungleichgewicht. So erlauben beispielsweise Navigationsgeräte im Auto in der Regel lediglich, die zuletzt angefahren Orte, die Durchschnittsgeschwindigkeit und zurückgelegte Kilometer (bei neueren Geräten auch den CO_2-Verbrauch) anzuzeigen. Demgegenüber entstehen beim Anbieter digitale Repräsentationen in Form der aufgezeichneten Bewegungsprofile, welche einen Ausschnitt des Lebensalltags des Nutzers abbilden. Diese Profile zeichnen ein Bild des Selbst, das der Nutzer gar nicht erhält. Durch die Verknüpfungsmöglichkeiten mit anderen Datenbanken kann ein noch viel detaillierteres Abbild des Nutzers erstellt werden.

Um dieses Abbild selbst auswerten und beurteilen zu können, war es notwendig diese Daten im Selbstversuch bewusst zu erheben. Denn nur durch das Wissen über die Daten können reflexive Prozesse einsetzen und eine kritische Auseinandersetzung mit der Repräsentation erfolgen.

Lokationsdienste und Location-based Social Networks

Nicht immer jedoch geschieht die Datenübermittlung ungewollt oder verdeckt. In der Mehrzahl der Fälle stimmen die Nutzer der Übertragung bewusst zu oder initiieren diese, um einen Mehrwert zu erhalten.

1 – Anonymisierte Darstellung der ‚Meine Freunde suchen'-Funktion auf Apple Mobiltelefonen mit eigenen Daten

So baut u. a. die von Apple in iOS Version 5 eingebaute Funktion „Meine Freunde suchen" (http://www.apple.com/de/icloud/features/find-my.html) auf diesem Konzept auf. Mit dieser Funktion können Nutzer es Freunden erlauben, den eigenen Standort zu ermitteln, um sich zu beispielsweise zu verabreden oder sich auf öffentlichen Plätzen schnell zu finden. Mit ‚Meine Freunde

suchen‘ können Nutzer den Aufenthaltsort ihrer Freunde – solange diese die Übertragung nicht wieder sperren – permanent überwachen. Technisch wird die Position des Gerätes dazu periodisch und bei Anforderung durch einen ‚Freund‘ an Apple übertragen und weitergeleitet. Apple erhält somit ein Bewegungsprofil aller Teilnehmer. Abbildung 1 zeigt exemplarisch die Darstellung von Freunden und Karteninformationen auf meinem iPhone. Damit eng verzahnt ist die Funktion ‚Mein iPhone suchen‘, mit dessen Hilfe Nutzer ein abhanden gekommenes Mobiltelefon orten und notfalls aus der Ferne sogar sperren und die enthaltenen Daten löschen können.

Zudem ermöglichen internetfähige Mobiltelefone mit GPS-Funktion die Teilnahme an sogenannten Location-based Social Networks. Diese Netzwerke erlauben es dem Nutzer (wie auch bei ‚Meine Freunde suchen‘), seinen aktuellen Standort in Echtzeit mit Freunden zu teilen und bieten darüber hinaus weitere Interaktionsmöglichkeiten, wie beispielsweise die Möglichkeit ‚digitale Abzeichen‘ oder Gutscheine durch das Aufsuchen eines Restaurants, Hotels, Clubs etc. zu erstehen. Bekannte Vertreter sind die Netzwerke *Foursquare* (https://foursquare.com/), *Gowalla* (http://gowalla.com/) oder *Google Latitude* (http://www.google.de/latitude), welche sich derzeit steigender Popularität erfreuen. Den Reiz, die virtuelle Welt des Internets mit der realen Welt durch Standortdaten zu vermischen, haben auch die ‚klassischen‘ Social Networks wie Facebook oder der Kurznachrichtendienst Twitter erkannt. Beide bieten seit einiger Zeit ebenfalls Funktionen, um Nutzerbeiträge mit Ortsdaten zu versehen. Die Nutzungsszenarien dieser neuen Netzwerke sind vielfältig und liegen vorwiegend bei der Kontaktaufnahme (gezielt oder zufällig) zu in der Nähe befindlichen Personen oder Freunden, lokationsbasierten Spielen mit virtuellen oder realen Preisen sowie der Aufzeichnung des eigenen Tagesablaufs in einem automatischen virtuellen Tagebuch.[22]

Weitere beliebte Lokationsanwendungen sind das Verknüpfen von digitalen Fotos mit den Koordinaten des Aufnahmeortes (genannt ‚Geotagging‘) oder das ‚Geocaching‘ als eine Form der (elektronischen) Schnitzeljagd nach ‚Schätzen‘ oder Orten in unbekanntem Gelände. Allen Diensten gemein ist die Verknüpfung von Positionsangaben mit persönlichen Informationen oder Berichten, welche im Internet bzw. in Social Networks dabei zu einer ‚Währung‘ werden. Wie in jedem ökonomischen System steigt mit der Verfügbarkeit dieser Daten neben den Vorteilen auch die reale Gefahr ihrer nachteiligen kommerziellen Verwertung bis hin zu Missbrauchsszenarien wie Identitätsdiebstahl.[23] So ist es den Unternehmen als Betreiber der Plattformen möglich, aus

---

[22] Vgl. Marshall Kirkpatrick, „Why We Check In. The Reasons People Use Location-Based Social Networks“, Artikel vom 28.06.2010, auf: *ReadWriteWeb*, online unter: http://www.readwriteweb.com/archives/why_use_location_checkin_apps.php, zuletzt aufgerufen am 01.09.2011.

[23] Vgl. Steffan Heuer, „Sag mir, wo Du bist! – Geodaten werden zur neuen Währung im Web – mit zwiespältigen Folgen für Anbieter und Nutzer“, in: *Technology Review*, 7 (2010), S. 44-49.

den übertragenen Daten ein detailliertes Bewegungsprofil zu generieren, welches Rückschlüsse auf Tagesabläufe, Lebensgewohnheiten und soziale Kontakte zulässt. Die resultierenden weitreichenden Implikationen für die Privatsphäre der Nutzer stehen im direkten Gegensatz zur Erwartungshaltung bei der Teilnahme an sozialen Netzwerken. So geht der Nutzer nicht davon aus, dass alle seine Schritte ungewollt auf unbestimmte Zeit gespeichert, systematisch durch leistungsstarke Data-Mining-Algorithmen ausgewertet und zeitversetzt zweckentfremdet verwendet werden können. Das bestehende Gefahrenpotenzial verdeutlicht prägnant die Website bzw. das Projekt ‚Please Rob Me'. Der Algorithmus der Seite durchsuchte dabei 2010 permanent soziale Netzwerke nach persönlichen Informationen wie Privatadresse, Name und dem aktuellen Aufenthaltsort eines Nutzers. War dabei die geografische Distanz zwischen Wohnadresse und Standort über mehrere Tage genügend groß, wurden die Daten (Adresse und weitere gesammelte persönliche Informationen) auf der Seite als sogenannte ‚Opportunities' (Gelegenheiten zum Diebstahl) für jeden einsehbar veröffentlicht. Die Autoren wollen mit ihrem Projekt auf die Gefahren der Weitergabe von Standortinformationen an Social Networks hinweisen.[24] Derzeit können interessierte Nutzer durch Eingabe ihres Twitter-Benutzernamens erfahren, welche Lokationsdaten sie im Netz preisgeben.

Die Electronic Frontier Foundation (EFF), eine Bürgerrechtsorganisation in den USA, hat die Problematik unter dem Namen „locational privacy" zusammengefasst: „Locational privacy [...] is the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use."[25]

Das Paper definiert den Begriff als schützenswertes Gut, das nicht wiedererlangt werden kann, sobald die Daten einmal veröffentlicht wurden.

Allen lokationsbasierten sozialen Diensten gemein ist, dass sie Positionsangaben mit weiteren persönlichen Informationen der Nutzer verknüpfen. Während diese sich davon einen Mehrwert versprechen und erhalten, so werden doch im Gegenzug die Auswertungsmöglichkeiten für die Dienstanbieter drastisch erhöht. Sie erhalten frei Haus korrekte und detaillierte Informationen über den Lebensalltag ihrer Nutzer.

Selbstversuch

Das Spannungsfeld zwischen Daten, Privatheit (Privatsphäre) und Selbstreflexion stand im Mittelpunkt eines Selbstversuchs: Fünf Jahre habe ich jeden

---

[24] Vgl. Barry Borsboom/Boy van Amstel/Frank Groeneveld, „Please Rob Me – Raising Awareness about Over-Sharing". auf: *Please Rob Me*, online unter: http://pleaserobme.com/, zuletzt aufgerufen am 01.09.2011.

[25] Vgl. EFF – Electronic Frontier Foundation (Hg.), „On Locational Privacy, and How to Avoid Losing it Forever", Whitepaper (2009) , San Francisco, CA, auf: Electronic Frontier Foundation, online unter: http://www.eff.org/wp/locational-privacy, zuletzt aufgerufen am 01.09.2011.

meiner Wege im öffentlichen Raum aufgezeichnet. Ich wollte wissen, welche Rückschlüsse sich aus diesen Daten auf meine Kontakte und persönliche Lebensführung ziehen lassen, wie viele Datensätze und welcher Aufzeichnungszeitraum für Vorhersagen meiner künftiger Bewegungen notwendig sind und inwieweit die bewusste Aufzeichnung meinen Lebensalltag verändert. Zur Akkumulierung eines großen Datenbestandes und um alle Fortbewegungsarten möglichst lückenlos zu erfassen, habe ich unter anderem GPS-Empfänger als Navigationsgeräte im Auto, Mobiltelefone, Marine-Plotter sowie mobile Allzweck-GPS-Empfänger eingesetzt.

Am Ende eines jeden Tages wurden die gesammelten Daten aus den einzelnen Geräten exportiert und zu einer gemeinsamen Aufzeichnung zusammengeführt. Meine GPS-Empfänger[26] zeichneten die Positionsdaten intern in Form von Wegpunkten (engl. *waypoints*, ein einzelnes Kartendatum aus Längen-, Breitengrad, Höhe und Zeitstempel) auf, die logisch zu Tracks (Aufzählung von einander chronologisch folgenden Wegpunkten) gruppiert wurden. Dabei legten die Geräte bei jedem Neustart und beim Verlust des Satellitenempfangs für mehr als 30 Sekunden einen neuen Track an. Eine Positionsmessung erfolgte jede Sekunde, jedoch fand eine Aufzeichnung als Wegpunkt erst bei einem Mindestabstand von zwei Metern zum letzten Punkt mindestens aber alle fünf Sekunden statt. Ich habe versucht, diese Aufzeichnungsparameter – soweit möglich – auf allen Geräten einzustellen. Für die Zusammenführung der unterschiedlichen GPS-Datenformate wurde das kostenlose Programm GPSBabel (http://www.gpsbabel.org/) verwendet. Die so gewonnenen Tracks wurden anschließend zur besseren Auswertung in eine relationale Datenbank übertragen.

Diese Art der Speicherung ermöglichte detaillierte Analyseverfahren und eine zeitnahe Auswertung und damit einhergehende Reflexion des eigenen Verhaltens. Das Verhältnis von Aufzeichnung, Repräsentation und Reflexion war dabei keineswegs gleich. So nahm die bewusste Aufzeichnung einen großen Teil des Prozesses ein und war bestimmten Schranken unterworfen.

Technische, rechtliche und soziale Grenzen

Bei meinem Experiment zeigten sich u. a. pragmatische und technische Grenzen, die eine vollständige Erfassung in bestimmten Situationen verhinderten. So war es nicht immer möglich, die nach jedem Einschalten erforderliche Synchronisation des Empfängers mit den GPS-Satelliten abzuwarten. Nicht alle Empfänger verfügten über AGPS und benötigten in einigen Fällen mehrere Minuten bis zur ersten Positionsbestimmung. Oft erforderten Termindruck oder soziale Konventionen ein vorzeitiges Verlassen des Startpunktes, wo-

[26] Verwendete Geräte waren Garmin *eTrex Vista C*, Garmin *60CSX*, Garmin *Oregon 300*, Garmin *nüvi 765* und Apple *iPhone 3GS* mit selbstentwickelter Applikation zur Aufzeichnung.

durch die ersten 10 bis 500 Meter einer Wegstrecke nicht aufgezeichnet werden konnten. In diesen Fällen wurde die bewusste Aufzeichnung als eine zusätzliche Belastung empfunden.

Zusätzlich können die Funkwellen der Satelliten aufgrund ihrer Wellenlänge und geringen Sendestärke solide Objekte wie Wände nicht durchdringen. Daher war die Aufzeichnung innerhalb von Gebäuden nur in der unmittelbaren Nähe eines Fensters möglich, jedoch beeinflussten die Reflexionen der Wellen an den Gebäudewänden die Genauigkeit der ermittelten Position massiv. Eine genaue Bestimmung der Position innerhalb eines Gebäudes war in der Regel ausgeschlossen. In fast allen Fällen kam es daher im Gebäude zu mindestens einem Verbindungsabbruch. Der Empfangsverlust hatte den praktischen Vorteil, dass bei der Wiedererlangung des Satellitensignals durch Verlassen des Gebäudes ein neuer Track angelegt wurde. Somit wurden die einzelnen Reiseabschnitte automatisch logisch getrennt. Eine weitere Grenze bilden Gewässer, welche die Funkwellen nur bis zu einer Tiefe von ca. 2 Metern durchdringen können. Meine Position unter Wasser konnte bei absolvierten Tauchgängen daher nicht aufgezeichnet werden. Zudem waren die verwendeten Geräte nicht ausreichend wasserdicht. Bei Flugreisen konnten Start und Landung aufgrund geltender Bestimmungen, nach denen elektronische Geräte bei Start und Landung ausgeschaltet sein müssen, nicht aufzeichnet werden. Daneben verlangten des Öfteren Flugbegleiter das Ausschalten des Empfängers. Ein Empfang war auch hier in der Regel nur auf einem Fensterplatz möglich, die ermittelte Position war auf ca. 25 Meter genau. Letztlich sorgte die Verwendung des Mobiltelefons zur Daueraufzeichnung für einen hohen Batterieverbrauch. Der Akku musste dadurch schon innerhalb eines Tages aufgeladen werden. In der Regel wurden daher dedizierte GPS-Empfänger verwendet.

Trotz dieser Einschränkungen entstand ein umfangreiches, nahezu lückenloses persönliches Bewegungsprofil, welches im nächsten Schritt durch Anfragen an die erstellte Datenbank systematisch ausgewertet wurde.

Datenanalyse & -auswertung

Um über Standort hinausgehende Informationen zu inferieren, reichen bereits zwei aufeinanderfolgende Punkte. Diese ergeben einen Vektor, aus dem man die Bewegungsrichtung und – über die Differenz der beiden Zeitangaben – die Fortbewegungsgeschwindigkeit errechnen kann.

Aus Geschwindigkeit gepaart mit Informationen aus digitalen Geländekarten lässt sich zuverlässig ableiten, ob ich zu Fuß, auf dem Fahrrad, im Auto, auf einem Boot oder im Flugzeug unterwegs war (vgl. Abbildung 2). Ebenso zeigen die Häufung mehrerer aufeinander folgender Punkte oder eine Geschwindigkeit von null das Verweilen an einem Ort an. Aus dem ersten und letzten Punkt einer solchen Kette kann die Verweildauer an einem Ort abgele-

2 – Grafische Darstellung der ermittelten Fortbewegungsarten
Bahn, Bus, Schiff und zu Fuß am Kartenausschnitt San Francisco

sen werden. Ist diese größer als 15 Minuten[27], ist von einem signifikanten Aufenthaltsort, wie z. B. der Wohnung, dem Arbeitsplatz, einer Arztpraxis, einem Hotel- oder Restaurantbesuch auszugehen. Zur Identifikation solcher Orte in der Datenbasis habe ich die Clusteranalyse verwendet. Bei diesem Verfahren wird der Datenbestand als gerichteter Graph mit Knoten (Wegpunkt) und Kanten (Vektor zweier Wegpunkte) interpretiert. Als Cluster (Haufen) bezeichnet man in diesem Fall eine Menge von Wegpunkten von zeit- und räumlicher Nähe. Zur Identifikation dieser Cluster in einem Graph stehen in der Informatik mehrere effiziente und leistungsstarke Algorithmen zur Verfügung, welche zusätzlich semantische Verknüpfungen zwischen Clustern herstellen und eine Rangordnung erstellen können.[28] Für meine Datenbasis habe ich im ersten Schritt einen zeitbasierten Clustering-Algorithmus verwendet. Hierbei werden Cluster *s*ukzessive durch Hinzunahme des nächsten Wegpunktes erweitert. Der Mittelwert der Schnittpunkte aller Wegpunkte eines Clusters bildet dabei seinen Mittelpunkt (Ort). Die Trennung von Clustern erfolgt, wenn benachbarte Wegpunkte eine zu große zeitliche oder räumliche Distanz aufweisen. Cluster mit einer geringen Anzahl von definierbaren *n* Wegpunkten werden im Anschluss verworfen. Durch die Mittelung von Wegpunkten ist es auch möglich, einzelne, durch schlechten GPS-Empfang stark abweichende, Fehlmessungen zu erkennen und zu ent-

[27] Dieser empirisch bestimmte Wert bildete bei meinen Profildaten einen guten Kompromiss zwischen niedriger Falscherkennungsrate auf der einen und hoher Wahrscheinlichkeit der Erfassung von signifikanten Orten auf der anderen Seite. Bis auf wenige Ausnahmen (beispielsweise eine Zeitung am Kiosk kaufen) lag die Verweildauer an Orten, an denen eine Interaktion stattfand, bei mindestens 15 Minuten.

[28] Vgl. Xin Cao et al., „Mining Significant Semantic Locations From GPS Data“, in: *Proceedings of the VLDB Endowment* 3, 1 (2010), S. 1009-1020.

fernen.[29] Die so gebildeten Cluster stellen signifikante Orte für den Nutzer dar. Im nächsten Schritt wurde diesen Orten eine semantische Bedeutung (z. B. ‚Institut für Informatik, HU-Berlin, Rudower Chaussee 25') zugewiesen. Dies geschah mittels Anfragen an die Google- und die OpenStreetMap-Ortsdatenbank. Der semantische Kontext wurde im Anschluss für jeden Ort in der Datenbank gespeichert. Die Zeitinformationen zu jedem Cluster machen es zudem möglich, chronologisch geordnete Übergänge zwischen zwei Orten zu erstellen. Trägt man diese Daten in einen neuen Graph – bestehend aus Knoten von Clustern und Kanten aus chronologischen Übergängen – ein, so erhält man ein Bewegungsprofil. Durch Untersuchung u. a. der Häufigkeit von Übergängen lassen sich Wahrscheinlichkeitsmodelle anfertigen mit denen es möglich wird, Vorhersagen über meine zukünftigen Bewegungen zu treffen.[30]

Mittels des aus der Datenbasis errechneten Wahrscheinlichkeitsmodells konnte ich meine Bewegungen zu über 95 Prozent vorauszusagen. Daraus ließen sich weitere Gewohnheiten und Trends ableiten. Als letztes habe ich die verfügbare Datenmenge künstlich verringert. Damit konnte ich prüfen, wie viele Daten zur Vorhersage von Lebensgewohnheiten und künftigen Bewegungen notwendig sind. Bei einer angenommenen Treffsicherheit von 90 Prozent reichten bei meinen Bewegungsdaten Zeiträume von (im günstigsten Fall) drei bis vier Wochen aus. Im ungünstigsten Fall wurden die Daten von maximal drei Monaten benötigt. Bei Reduzierung der gewünschten Treffsicherheit lässt sich der Aufzeichnungszeitraum noch einmal deutlich verringern.

Selbstreflexion durch Selbstversuch

Die Auswertung meines Bewegungsprofils erlaubte es mir, abstrakte Gefährdungspotenziale praxisnah nachzuvollziehen und Gefahren bei der Nutzung von Lokationsdiensten zu benennen. Es war mir problemlos möglich, durch Anfragen an die Datenbasis meinen Tagesablauf komplett zu rekonstruieren und detaillierte Aussagen über Lebensgewohnheiten und soziale Kontakte zu treffen. Anfragen wie „Wann war ich das letzte Mal beim Arzt?", „Wie oft esse ich außer Haus?" konnten zuverlässig beantwortet werden. Eine Anfrage nach Orten mit einer Verweildauer zwischen 22 und 6 Uhr lieferte alle Orte, an denen ich übernachtet habe. Der Übernachtungsort mit der größten Häufigkeit war meine Wohnadresse. Anfragen nach Orten mit einer Verweildauer

---

[29] Für eine genaue informatische Beschreibung des Algorithmus vgl. Jong Hee Kang et al., „Extracting Places from Traces of Locations", in: *Mobile Computing and Communications Review* 9, 3 (2005), S. 58-68.

[30] Vgl. Alexander Gutjahr, „Bewegungsprofile und -vorhersage". Paper im Rahmen des interdisziplinären Forschungsseminars LBS/Location Awareness – Technische Hintergründe und juristische Implikationen (06.02.2009), Universität Freiburg, online unter: http://www.ks.uni-freiburg.de/download/papers/interdiszWS08/Alexander_Gutjahr.pdf, zuletzt aufgerufen am 01.09.2011.

von mindestens einer Woche außerhalb meines Wohnortes Berlin lieferten alle Orte von Urlaubs- oder Dienstreisen. Neben den genauen Zeiten konnte auch leicht der Standort des gebuchten Hotels, besuchte Sehenswürdigkeiten etc. ermittelt werden.

3 – Visualisierung der GPS-Rohdaten 2005-2011 im Programm Google Earth im Kartenausschnitt Berlin/Brandenburg

Mir war es sogar möglich, durch die Anfrage wie viel Fastfood ich konsumiere (definiert als das Aufsuchen eines Fastfood-Restaurants oder eines Imbissstands), meiner Ernährungsgewohnheiten gewahr zu werden und Veränderungen über den Erfassungszeitraum von fünf Jahren zu erkennen. Die Akkumulation der Daten erlaubte dabei immer detaillierte Anfragen zu stellen.

Diese einfachen Anfragen zeigen das hohe Missbrauchspotenzial und die datenschutzrechtliche Bedenklichkeit der Aggregation von Lokationsdaten.

Die bewusste Erfassung und regelmäßige Analyse bedingte auch eine Selbstreflexion mit bewussten (z. B. Einschränkung des Fastfood-Konsums), aber auch unbewussten Änderungen meines Verhaltens.[31]

So irritierte die bewusste Erfassung einspielte Tagesabläufe und führte zu Verzögerungen. Das Verlassen von Gebäuden wurde beispielsweise aufgrund der Wartezeit bis zur GPS-Signalakquise bewusster erlebt. Einerseits war die aktuelle Uhrzeit durch einen Blick auf den Bildschirm des Empfängers immer präsent. Andererseits wurde die unmittelbare Umgebung des Ortes durch die Zwangspause genauer beobachtet.

Die Datenanalyse erlaubte es, viele unbewusste Alltagsprozesse zu quantifizieren. Neben dem erwähnten Fastfood-Konsum konnte ich auch genau beziffern, wie viel Zeit ich im Monat im Auto, in der S-Bahn oder mit Spazierengehen verbringe. Dabei war es teilweise frustrierend zu sehen, wie viel Lebens-

[31] Vgl. Jens-Martin Loebel, „Aus dem Tagebuch eines Selbstaufzeichners. Laborgespräch mit Ute Holl und Claus Pias“, in: *Zeitschrift für Medienwissenschaft, Heft 4 – Menschen & Andere*, I (2011), S. 115-125.

zeit ich in Berlin im Stau verbringe. Durch die Datenbasis wurden diese Vorgänge überhaupt erst ‚greifbar'.

Hat man einmal den Zugriff auf seine eigenen Daten erlangt, so können diese ein mächtiges Werkzeug zur Selbsterkenntnis darstellen. Dabei geht es weniger um den Prozess der Aufzeichnung selbst, als um die Auswertungsmöglichkeiten und die bewusstere Verortung des Selbst in der Umwelt. Interessant ist hier die Verflechtung von Automatisierung, Automatismen der Aufzeichnung und der bewussten Reflexion: Die automatische Aufzeichnung erzeugt ein ‚Daten-Selbst', das Gewohnheiten und Routinen des Selbst sichtbar macht, die *vom Subjekt nicht bewusst gesteuert werden*. Der Prozess der Aufzeichnung ermöglicht, neben dieser Sichtbarmachung von Automatismen, die Reflexion des eigenen Verhaltens; sie kann in der Bewusstmachung zu einer Entautomatisierung führen.

In diesem Zusammenhang erwähnenswert ist die 2007 von Wolf und Kelly angestoßene ‚Quantified Self-Bewegung'.[32] Diese Gruppe von ‚Selbstaufzeichnern' benutzt die Technik der Datenaufzeichnung und -analyse als Spiegel zur Selbsterkenntnis und um effizienter in der Welt agieren zu können. Zum Einsatz kommen u. a. eine Vielzahl von (vorrangig biometrischen) Sensoren. Dabei können Puls, Blutdruck, Temperatur genau so erfasst werden, wie der Schlafrhythmus[33], der monatliche Zyklus der Frau, alle finanziellen Transaktionen oder die in regelmäßigen Abständen vermerkte eigene Stimmung.[34] Ziel ist immer, etwas über sich selbst und einen Aspekt seines Lebens zu erfahren. Dabei generieren erst die Analyseverfahren und die Verknüpfung eine Bedeutung aus dem Berg an quantifizierten Daten. Die einzelnen Datenpunkte für sich selbst sind nichtssagend. Hierin liegt, wie bei den GPS-Daten, die Mächtigkeit eines solchen Datenprofils begründet.

Ebenso wie bei GPS-Daten gibt es auch hier kritische Stimmen und Befürchtungen um Missbrauchsmöglichkeiten von online geteilten Datenprofilen. Neben der Privatsphäre und dem Datenschutz besteht zudem die Gefahr eines blinden Vertrauens in die aufgezeichneten Daten mit einem einhergehenden Verlust der gesunden Selbstwahrnehmung.[35]

---

[32] Vgl. http://www.webcitation.org/66TEY49wv, älteste Einträge des quantifiedself.com Blogs von Gary Wolf und Kevin Kelly, zuletzt aufgerufen am 25.06.2012.

[33] So gibt es beispielsweise für das iPhone ein Programm, das die Beschleunigungssensoren des Telefons benutzt, um Schlafphasen festzustellen. Dazu wird das iPhone mit ins Bett gelegt. Fortan wird jede Bewegung des Schlafenden (als Erschütterung) registriert und aufgezeichnet.

[34] Vgl. M. Hesse, „Bytes of Life. For Every Move, Mood and Bodily Function, There's a Web Site to Help You Keep Track", auf: *Washington Post Blog*, 09.09.2008,online unter: http://www.washingtonpost.com/wp-dyn/content/article/2008/09/08/AR2008090802681_pf.html; //www.washingtonpost.com/wp-dyn/content/article/2008/09/08/AR2008090802681_pf.html, zuletzt aufgerufen am 25.06.2012.

[35] Dieser Aspekt wurde treffend von Randall Munroe in xkcd karikiert. Vgl. „Decline", 2009, online unter: http://xkcd.com/523/, zuletzt gerufen am 25.06.2012.

Auf das ‚Daten-Selbst' haben also die Analyseverfahren sowie die Semantiken der Datenbanken einen entscheidenden Einfluss. So ist es wichtig, kritisch zu reflektieren, welche Daten überhaupt erfasst wurden und welche Aussagekraft sie tatsächlich besitzen. Hinzu kommt die Frage der Repräsentation. Wenn etwas nicht repräsentiert ist oder nicht werden kann, so existiert es in der Symbolwelt nicht – mit Implikationen für die reale Welt. Welche Restaurants und Tankstellen z. B. in meinem Auto-Navigationsgerät vom Hersteller einprogrammiert wurden, entscheidet maßgeblich, ob ich diese in einer fremden Stadt (z. B. im Urlaub) besuche. Ist ein Restaurant nicht im Gerät verzeichnet, so existiert es für die digitale Karte nicht. Eine Anfrage nach Restaurants in meiner Nähe würde diese Lokale dementsprechend nicht auflisten. Die Definitionsmacht liegt hier beim Hersteller des Geräts bzw. beim Anbieter der digitalen Karten.

Es ist die systematische, quantifizierte Aufzeichnung, welche umfangreiche Einblicke in meinen Lebensalltag ermöglicht. Das Wissen um diesen Vorgang aus meinem Selbstversuch hat mein Verhalten geprägt und zur Datensparsamkeit gegenüber Dritten ermahnt. Denn nach wie vor überwiegt die fremdbestimmte Auswertung des eigenen Profils. Zudem benötigt man unglaublich wenige Daten um Vorhersagen über Wege zu machen oder Rückschlüsse über die Tagesabläufe und Lebensgewohnheiten eines Menschen zu ziehen.

Vom Gefühl einer ständigen Beobachtung zu unterliegen geht die reale Gefahr aus, dass Menschen – z. B. aus Angst vor Sanktionen – ihr Verhalten ändern und zustehende Rechte nicht mehr wahrnehmen. Diese Gefahr hat auch die Rechtsprechung erkannt, wie 1983 im Volkszählungsurteil des Bundesverfassungsgerichts deutlich hervorgehoben.[36] Diese Rechtsauffassung wurde zuletzt 2010 bekräftigt, als das Gesetz zur sogenannten Vorratsdatenspeicherung für verfassungswidrig und nichtig erklärt wurde.[37] Durch dieses Gesetz sollten die Verbindungsdaten aller Bundesbürger für sechs Monate erfasst und gespeichert werden. Durch die Speicherung der aktuellen Funkzelle bei Mobiltelefonen wurde indirekt auch der Standort des Mobiltelefons erfasst. Der Zeitraum von sechs Monaten liegt dabei deutlich über dem von mir zur Erstellung eines kompletten Bewegungsprofils ermittelten Zeitraums von drei Monaten. Zusätzlich wäre es durch die Korrelation der Daten aller Bundesbürger möglich, eine Karte aller sozialen Kontakte zu erstellen.

Fazit

Tragbare GPS-Empfänger in Form von Mobiltelefonen oder Navigationsgeräten haben unseren Alltag durchdrungen und ermöglichen eine Vielzahl neuartiger Anwendungsszenarien. Eine ungewollte laufende Übertragung von

[36] Vgl. BVerfG, 1 BvR 209/83 vom 15.12.1983.
[37] Vgl. BVerfG, 1 BvR 256/08 vom 02.03.2010.

Standortdaten über einen Rückkanal sowie die Anreicherung von persönlichen Informationen um Standortdaten in digitalen sozialen Netzwerken bilden jedoch ein hohes Missbrauchspotenzial, mit konkreten Auswirkungen auf Privatsphäre und Datenschutz. In meinem Experiment konnte ich zeigen, wie leicht GPS-Daten zu erheben und systematisch zu verarbeiten sind. Oft ist den Nutzern das Ausmaß der Übertragung nicht bewusst, wodurch eine Kluft zwischen der technischen Realität der Auswertungsmöglichkeiten und der Bewertung der Daten durch den Nutzer entsteht. So ermöglicht die Clusteranalyse die Ermittlung von signifikanten Orten und die Erstellung von detaillierten Bewegungsprofilen inklusive Voraussage künftiger Bewegungen. Die Fülle der ableitbaren privaten Informationen und Lebensgewohnheiten ist dabei erstaunlich. Die bewusste Auseinandersetzung mit den Datenspuren sowie der Aufzeichnungsprozess selbst führten zu Verhaltensänderungen.

Wie von der EFF beschrieben, muss eine Aufklärung der Nutzer erfolgen und – wenn notwendig – zur Datensparsamkeit ermahnt oder zum kritischen Umgang mit den neuen Diensten angeregt werden. So lassen sich bereits heute bei vielen Diensten Einstellungen zur Privatsphäre vornehmen. Bei Telefonen mit dem Google- oder Apple-Betriebssystem kann der Zugriff auf GPS-Daten pro Applikation vom Nutzer eingestellt werden. Zusätzlich obliegt es dem Gesetzgeber das bestehende Datenschutzrecht an die neuen Anwendungsszenarien anzupassen und den Firmen – aber auch dem Staat selbst – gegebenenfalls Schranken bei der Erhebung und Auswertung von Lokationsdaten zu setzen.

Die Konsequenz des Versuchs soll dabei nicht der Verzicht auf Lokationsdienste und -anwendungen sein, da diese ebenfalls sehr viele Vorteile bieten. Dem Nutzer sollten Möglichkeiten geschaffen werden, sein eigenes Profil auszuwerten. Durch die Richtung des Blicks ‚nach innen' werden Reflexionsprozesse und eine bewusstere Verortung des Selbst möglich. Insbesondere die Diskrepanz zwischen der eigenen Selbstwahrnehmung und dem aus den ausgewerteten Daten erstellten Profil ist dabei von herausragender Bedeutung, stößt die Kluft zwischen ‚Daten-Selbst' und Selbstwahrnehmung doch einen Prozess der Selbsterkenntnis an. Erst durch die kritische Betrachtung der Semantik des Profils und der digitalen Repräsentation können wir neben der eigenen Selbstreflexion auch den Aufzeichnungsprozess und damit die Technologie an sich genauer verstehen.

Literatur

Allan, Alasdair/Warden, Pete, „Got an iPhone or 3G iPad? Apple is recording your moves", auf: *O'Reilly radar*, 20.4.2010, online unter: http://radar.oreilly.com/2011/04/apple-location-tracking.html, zuletzt aufgerufen am 01.09.2011.

Apple Inc. (Hg.), „Apple Datenschutzrichtlinie“, Teil der allgemeinen Geschäftsbedingungen, Stand vom 12. Oktober 2011, auf: *Apple*, online unter: http://www.apple.com/de/privacy/, zuletzt aufgerufen am 15.11.2011.

Barczok, Achim, „Kretschmann will satellitengestützte PKW-Maut“, Artikel vom 16.10.2011, auf: *Heise-Newsticker*, online unter: http://heise.de/-1361871, zuletzt aufgerufen am 15.10.2011.

Borsboom, Barry/van Amstel, Boy/Groeneveld, Frank, „Please Rob Me – Raising Awareness about Over-Sharing“, auf: *Please Rob Me*, online unter: http://pleaserobme.com/, zuletzt aufgerufen am 01.09.2011.

Cao, Xin et al., „Mining Significant Semantic Locations From GPS Data“, in: *Proceedings of the VLDB Endowment* 3, 1 (2010), S. 1009-1020.

Curtis, Sophie, „GPS Tracking Trojan Hidden In Android App“, 17.08.2010, auf: *eWeek Europe*, online unter: http://www.eweekeurope.co.uk/news/gps-tracking-trojan-hidden-in-android-app-9048, zuletzt aufgerufen am 15.10.2011.

Dodel, Hans/Häupler, Dieter, *Satellitennavigation*, 2. korrigierte und erweiterte Aufl., Berlin, 2010.

EFF – Electronic Frontier Foundation (Hg.), „On Locational Privacy, and How to Avoid Losing it Forever“, Whitepaper (2009), San Francisco, CA, auf: *Electronic Frontier Foundation*, online unter: http://www.eff.org/wp/locational-privacy, zuletzt aufgerufen am 01.09.2011.

Greene, Kate, „Staumeldung gegen Bewegungsprofil“, Artikel vom 25.11.2008. auf: *Technology Review* (Online Version), online unter: http://www.heise.de/tr/artikel/Staumeldung-gegen-Bewegungsprofil-275834.html, zuletzt aufgerufen am 01.09.2011.

Gutjahr, Alexander, „Bewegungsprofile und -vorhersage“. Paper im Rahmen des interdisziplinären Forschungsseminars *LBS/Location Awareness – Technische Hintergründe und juristische Implikationen* (06.02.2009), Universität Freiburg, online unter: http://www.ks.uni-freiburg.de/download/papers/interdiszWS08/Alexander_Gutjahr.pdf, zuletzt aufgerufen am 01.09.2011.

Heuer, Steffan, „Sag mir, wo Du bist! – Geodaten werden zur neuen Währung im Web – mit zwiespältigen Folgen für Anbieter und Nutzer“, in: *Technology Review*, 7 (2010), S. 44-49.

Horn, Sebastian, „Handy-Fahrschein: Von der Deutschen Bahn verfolgt“, 27.9.2011, auf: *Zeit Online*, online unter: http://www.zeit.de/digital/2011-09/bahn-fahrschein-berlin, zuletzt aufgerufen am 01.10.2011.

Johnson, Bobbie, „Researcher: ‚iPhone Location Data Already Used By Cops‘“, auf: *GigaOM Blog*, 21.04.2011, online unter: http://gigaom.com/2011/04/21/researcher-iphone-location-data-already-used-by-cops/, zuletzt aufgerufen am 01.09.2011.

Kang, Jong Hee et al., „Extracting Places from Traces of Locations“, in: *Mobile Computing and Communications Review* 9, 3 (2005), S. 58-68.

Kirkpatrick, Marshall, „Why We Check In. The Reasons People Use Location-Based Social Networks“, Artikel vom 28.06.2010, auf: *ReadWriteWeb*, online unter: http://www.readwriteweb.com/archives/why_use_location_checkin_apps.php, zuletzt aufgerufen am 01.09.2011.

Loebel, Jens-Martin, „Aus dem Tagebuch eines Selbstaufzeichners. Laborgespräch mit Ute Holl und Claus Pias“, in: *Zeitschrift für Medienwissenschaft, Heft 4 – Menschen & Andere*, I (2011), S. 115-125.

Meyer, Carsten, „Datenschutzbeauftragter warnt vor Missbrauch bei Handy-Ortung“, Artikel vom 30.05.2010, auf: *Heise-Newsticker*, online unter: http://heise.de/-1010712, zuletzt aufgerufen am 01.09.2011.

Sarno, David, „Apple Collecting, Sharing iPhone Users' Precise Locations“, Artikel vom 21.06.2010, auf: *Los Angeles Times* (Onlineversion), online unter: http://latimesblogs.latimes.com/technology/2010/06/apple-location-privacy-iphone-ipad.html, zuletzt aufgerufen am 01.09.2011.

Xu, Guochang, *GPS – Theory, Algorithms and Applications*, 2. Aufl., Berlin, 2007.