d) *the valuable contribution of all stakeholder groups in their respective roles, as recognized in § 35 of the Tunis Agenda for the Information Society, to the evolution, functioning and development of the Internet;*

e) *that, as stated in the WSIS outcomes, all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the existing Internet and its future development and of the future internet, and that the need for development of public policy by governments in consultation with all stakeholders is also recognized;*

f) *Resolutions 101, 102 and 133 (Rev. Guadalajara, 2010) of the Plenipotentiary Conference,* resolves to invite Member States

1 to elaborate on their re
on international Intern
development and publ
mandate of ITU at vari
inter alia, the World Telecommunication/ICT Policy Forum, the Broadband Commission for Digital Development and ITU study groups;

2 to engage with all their stakeholders in this regard, instructs the Secretary-General

1 to continue to take the necessary steps for ITU to play an active and constructive role in the development of broadband and the multistakeholder model of the Internet as expressed in § 35 of the Tunis Agenda;

2 to support the participation of Member States and all other stakeholders, as applicable, in the activities of ITU in this regard.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Ein bißchen Multi-Stakeholder

Die Experten von ISOC und FCC rieten mit Blick auf die nächsten Schritte vor allem zu mehr Unterstützung und Werbung für das, was in der internationalen Netzpolitik als *Multi-Stakeholder*-Ansatz Karriere gemacht hat, mit wahlweise der ICANN oder dem *UN Internet Governance Forum (IGF)* als prominent zitierten Beispielen. In ihrer Erklärung zur Informationsgesellschaft beim UN-Weltgipfel in Tunis 2006 hat die Staatengemeinschaft die Regelung internationaler Netzfragen durch alle Interessengruppen aus allen Ländern im Grundsatz bejaht. Praktisch hat sich die US-Regierung des Konzepts nicht zuletzt dafür bedient, den Zugriff von Regierungen auf das ursprünglich komplett von den USA dirigierte *Domain Name System* zu begrenzen – die US-Regierung kontrolliert nach wie vor die zentrale *Rootzone*.

Doch der Multi-Stakeholder-Begriff hat durchaus Spuren hinterlassen, auch die WCIT-Konferenz zeigte das. Auf Druck von Öffent-
nen, aber auch einer Reihe demo-
en Nicht-Regierungsteilnehmer als
on Regierungsdelegationen teilneh-
urden ins Web übertragen – ein No-
ouré traf sich mit zivilgesellschaftlichen Gruppen vor Ort und tägliche Pressekonferenzen sollten für zusätzliche Transparenz sorgen. Vorab hatte man sogar in einer ersten weltweit abgehaltenen Online-Konsultation wenigstens die Kernvorschläge der neuen ITR zur Diskussion gestellt – mit freilich mäßigem Erfolg. Dass das Gros der Verhandlungsdokumente aber nur durch *Leaks* bekannt wurde und Nicht-Regierungsvertreter praktisch kein Rederecht haben, sichert der ITU allerdings nach wie vor den Vorwurf, eben nicht wirklich transparent und partizipationsbereit zu sein.

Auch in Deutschland lernt man noch, was der Begriff Multi-Stakeholder bedeutet. Zwar lud das BMWi vor und nach der WCIT zu kurzen Konsultationstreffen, Einladungen dazu ergingen aber nur an ausgewählte Unternehmen, Verbände und Organisationen, die Presse wurde nicht zugelassen. Von den 40 Teilnehmern beim Februar-Treffen kamen über 30 aus Ministerien, dem Parlament oder der Wirtschaft. Auf dem zivilgesellschaftlichen Auge ist man auch hierzulande noch beinahe blind – und könnte angesichts der bevorstehenden Debatten zur Netzkontrolle weltweit Unterstützung brauchen.

Björn Schembera

You are here – Privatsphäre der Positionsinformation

Es ist der 19. Februar 2011. Tausende machen von ihrem Grundrecht auf Versammlungsfreiheit Gebrauch und demonstrieren gegen einen jährlich stattfindenden Naziaufmarsch in Dresden. Weil ausgehend von den Gegenaktivisten Straftaten vermutet werden, führt die Polizei eine großangelegte Funkzellenauswertung durch, wodurch tausende sich in der Südstadt aufhaltende Personen unter Generalverdacht gestellt werden.

Dieses Beispiel zeigt, wie sensibel Positionsinformationen sind. Aus dem momentanen Aufenthaltsort lassen sich Rückschlüsse ziehen über das Sozialverhalten, persönliche Interessen und viele weitere Eigenschaften einer Person, wie z. B. deren politische Gesinnung. Diese Aspekte werden klassischerweise zur schützenswerten Privatsphäre gezählt. Ein zeitgemäßes Verständnis der Privatsphäre muss deshalb auch das Recht von Individuen, Gruppen oder Institutionen einschließen, „selbst bestimmen zu können, wann, wie und in welchem Ausmaß Information über ihre Position an andere weitergegeben wird.“[1]

Mit der Verbreitung von Smartphones ist heutzutage die Nutzung von Positionsinformationen fast schon zur Selbstverständlichkeit geworden: Wir teilen unsere Position über Dienste wie *Google Latitude* Freunden mit, Schüler kommunizieren zunehmend über *Facebook* und versehen Neuigkeiten, Bilder oder

Parties mit einer Positionsangabe, die in den sozialen Netzwerken erscheint.

Smartphones spielen dabei eine zentrale Rolle. In technischer Hinsicht stellen sie eine Erweiterung des klassischen Mobiltelefons dar, wobei sie es um mehrere Sensoren ergänzen, eine hochauflösende Kamera besitzen und auf mobilen Internet-Zugang ausgelegt sind. Hierfür ist natürlich eine wesentlich höhere Rechenleistung nötig. Durch den heute standardmäßig in Smartphones verbauten GPS-Sensor ist es möglich, jederzeit die eigene Position zu bestimmen. In Zusammenspiel mit dem Internet-Zugang, der heute meistens über Flatrates angeboten wird, führt dies zu standortbezogenen Diensten (*Location-based Services,* LBS), worunter Dienste verstanden werden, auf die von mobilen Geräten über ein mobiles Netzwerk zugegriffen wird und die von der Fähigkeit Gebrauch machen, die Position dieser Geräte zu bestimmen.[2]

Ein LBS benötigt ein Smartphone, ein Positionierungssystem, sowie einen *Location Server* (LS), um eine ortsbezogene Anwedung anbieten zu können, wie z. B. einen POI *(Point of Interest)*-Finder. Der LS verwaltet die Positionsdaten der mobilen Geräte und hat Informationen zumindest über den momentanen Aufenthaltsort, evtl. aber sogar über Bewegungsprofile des Nutzers.

Dobson und Fisher zeichnen bereits 2003 eine düstere Vision und nennen diese *Geoslavery*.[3] Eingebettet in ein Herr-Knecht-Modell besitzt der Überwacher Kontrolle über die Positionsinformation, d.h. Zeitpunkt, Position, Geschwindigkeit und Richtung eines oder mehrerer Überwachter. Die Technologie sei verfügbar, einige auf Freiwilligkeit basierende Produkte schon auf dem Markt.

Das oben genannte Beispiel mit *Google Latitude* ist insofern problematisch, da über ein spezielles Konto, den Google-Account, die Positionsinformation mit anderen Informationen verknüpft wird. An dieses Konto sind auch noch andere Dienste (E-Mail, Suchmaschinenergebnisse, Kalender, ...) angebunden. So kann einem Nutzer beispielsweise positionsbezogene Werbung eingeblendet werden, wenn aus seinem E-Mailkonto oder seinem Suchverhalten hervorgeht, dass er sich für ein gewisses Produkt interessiert.

Aufgrund der Komplexität von mobilen Anwendungen oder deren Nutzungsbedingungen kann dies im Hintergrund ohne explizite Einwilligung des Nutzers passieren. Zwar ist das gemäß §98 des Telekommunikationsgesetzes als Teil der informationellen Selbstbestimmung untersagt, kam jedoch in der Vergangenheit durchaus schon vor. So wurde 2011 bekannt, dass alle Apple-Produkte auf der iOS-Plattform lokal im Gerät die Positionsdaten speicherten.[4] Zu einem weiterern Vorfall bei Apple kam es im Februar 2012, bei dem Anwendungen ungefragt auf die Adressdaten zugriffen.[5]

Es handelt sich also bei jedem Teil eines LBS, vom mobilen Gerät über den Location Server bis zum Service um einen kritischen Punkt bezüglich der Privatsphäre. Die technischen Aspekte sollen nun beleuchtet werden, um im Folgenden einige Gegenmaßnahmen vorzustellen.

Mobiles Objekt (MO)

Das *Mobile Objekt*, sei es nun Smartphone oder Tablet, ist ein kritischer Punkt im System, weil es den Nutzer als digitaler Helfer ständig begleitet. Der Nutzer muss bewusste Kontrolle über Hard- und Software ausüben können, was insbesondere die Kontrolle über die Sensoren, die Kamera und die Internet-Verbindung umfasst.

Hier liegt die Problematik vor allem im Betriebssystem, das meist ein proprietäres ist. So sind die verbreitetsten Systeme *Symbian*, *iOS*, *Blackberry OS* und *Windows Mobile* allesamt Closed Source und den Herstellern muss vertraut werden – dass sie nicht immer als integer eingestuft werden können, zeigen die o.g. Beispiele von Apple.

Googles Betriebssystementwicklung für mobile Endgeräte, genannt *Android*, geht einen anderen Weg: Zwar ist das Betriebssystem Open Source, wirklich nutzen lässt sich dieses System jedoch nur mit einem Google-Account, was wieder die oben genannte Verknüpfung von personenbezogenen Daten auf verschiedenen Ebenen zur Folge haben kann. Ebenso lassen sich die Anwendungen oft nur über die hauseigene Vertriebsplattform *Google Play* herunterladen, wozu wiederum ein Google-Account Vorraussetzung ist.

Die Kampagne *Free your Android*, die vom FoeBud (heute digitalcourage) und FSF[6] initiiert wurde, gibt eine Hilfestellung, wie man das eigentlich freie Betriebssystem Android von Google *befreit*. Konkret wird die Nutzung von *CyanogenMod* empfohlen[7], einem Android-Abkömmling, der komplett ohne Google-Anwendungen auskommt und auf den meisten Android-Mobiltelefonen läuft. Zur Installation ist das *Rooten* des Geräts notwendig, wodurch die Garantie erlischt.

Eine weitere Entwicklung in Richtung freier Software auf mobilen Geräten machen die Ubuntu-Entwickler mit *Ubuntu for Phones*, welches auf der CES im Januar 2013 als Prototyp vorgestellt wurde. Das Projekt steht jedoch noch im Aufbau, lauffähige Versionen werden nicht vor 2014 erwartet und es ist

Björn Schembera

Björn Schembera ist Diplom-Informatiker und lebt in Stuttgart.

noch ungewiss, in welche Richtung sich das Projekt entwickeln wird.[8]

Location Server (LS)

Der *Location Server* verwaltet die Positionen aller auf ihm angemeldeten Benutzer. Dies macht ihn zu einem sensiblen Punkt, da dort die Informationen mehrerer Nutzer verfügbar sind. Neben den reinen Orts- und Zeitinformationen könnten hier auch Daten zwischen mehreren Nutzern korreliert werden.

Zwar beteuert beispielsweise Google für seinen Dienst *Latitude*, dass die Bewegungsprofile nicht gespeichert werden, aber es lässt sich auch eine Kompromittierung des Dienstes denken, oder ein Arbeitgeber, der Dienst-Handys an seine Belegschaft ausgibt und sie ohne ihr Wissen verfolgen lässt. Zur Absicherung des *Location Server* gibt es einige Konzepte, die hier in Kürze vorgestellt werden sollen:[9]

Eine grundsätzliche Absicherung des *Location Server* kann durch Zugriffskontrolle erfolgen, die aus anderen Bereichen wohlbekannt ist und wozu eine Zugriffsliste geführt wird, die besagt, welche Person welche Aktion auf den Positionsinformationen durchführen darf. Hierbei ist problematisch, dass die Kontrolle der Zugriffsliste sich nicht in der Hand des eigentlichen Nutzers befindet. Darüber hinaus können die Positionsinformationen verschlüsselt auf dem LS abgelegt werden, was jedoch dazu führt, dass räumliche Anfragen über mehrere Objekte unmöglich werden.

Ein anderes Verfahren ist *k-Anonymity,* wonach die eigene Position von der Position k–1 anderer Nutzer des LBS ununterscheidbar werden soll – eine Person wird durch eine Gruppe anonymisiert, wobei die Schwierigkeit darin liegt, eine Gruppierung zu finden, die ausreichend Sicherheit bietet. Des Weiteren lässt sich die exakte Position künstlich unscharf bzw. ungenau machen. Die Position entspricht dann einer Aufenthaltswahrscheinlichkeit innerhalb eines gewissen Radius. Mittels Kooradinatentransformation ließe sich die echte Position in ein anderes Koordinatensystem übertragen und so die Privatsphäre erhöhen.

Beide Ansätze lassen sich kombinieren zu einer Verteilung der Positionsinformationen auf mehrere unabhängige *Location Server.* Jeder Server beherbergt dann nur einen Teil der Informationen, was eine gewisse Sicherheit bei nicht vertrauenswürdigen *Location Servern* bringt.

Außer der Zugriffskontrolle existieren alle Konzepte nur prototypisch. Bis sie als Produkt zur Verfügung stehen, wird einige Zeit vergehen, außerdem muss dies gewollt sein sowohl von den Herstellerinnen und Herstellern als auch den Nutzerinnen und Nutzern.

Location-based Service (LBS)

Natürlich muss der Service selbst, der die auf dem LS abgelegten Positionsinformationen bezieht und verarbeitet, vertrauenswürdig sein. Er bekommt Zugriff auf alle von Nutzerin oder Nutzer zu Verfügung gestellten Daten.

Diesem Dienst muss ein grundsätzliches Vertrauen entgegengebracht werden, da er alle vom Nutzer autorisierten Daten verarbeitet. Die beste Möglichkeit, sich hier gegen Missbrauch zu schützen, ist die Nutzung von Freier Software. Nur wenn der Quellcode offen liegt, kann der Nutzer oder die Community nachvollziehen, was wirklich geschieht. Da die LBS jedoch meist auf entfernten Servern arbeiten, ist eine Kontrolle hier oft nicht möglich.

Grundsätzlich müssen LBS kritisch betrachtet werden, da diese mit den Positionsdaten von Individuen arbeiten und jene somit potenziell in deren Besitz sind. Für das mobile Objekt und den Location Server gibt es Konzepte, diese Teile abzusichern – so gibt es mittlerweile für Smartphones die Betriebssystem-Alternative CyanogenMod. Der kritische Punkt ist meist der LBS selbst, da dieser auf einer eigenen Infrastruktur die Positionsdaten verarbeitet und das Ergebnis dann an den anfragenden Nutzer schickt.

Neben den technischen Konzpten müssen auch die gesellschaftlichen Implikationen näher betrachtet werden. Zielführend kann es nicht sein, standortbezogene Dienste grundsätzlich abzulehnen – wichtig ist der kritische Umgang damit. Auf Firmen und deren Versprechungen in punkto Datensicherheit ist nur selten Verlass, wie viele Beispiele zeigen.

Ebenso wichtig ist es, dass wir wieder die bewusste Kontrolle über unser Handeln erlangen, worunter ich auch die bewusste Kontrolle von Geräten verstehe, die uns im Alltag zur Seite stehen sollen. Dafür muss bei einer großen Mehrheit jedoch erst ein Problembewusstsein geschaffen werden. Ebenso muss dieses Problembewusstsein auch im Bereich der Wissenschaft und der Industrie durchgesetzt werden. Technik ist per se weder gut noch schlecht, es kommt auf deren konkrete Nutzung an – wir müssen klare Trennlinien ziehen zwischen der Anwendung von Technik, die dem Menschen nützt, und Technik, die nur der Profitmaximierung oder anderen Partikularinteressen verpflichtet ist.

Um wieder auf das eingangs genannte Beispiel mit der Demonstration zu kommen: Dass man Technik auch meistens in der umgekehrten Richtung nutzen kann, zeigt sich exemplarisch an *Sukey*.[10] Dieses im Rahmen der britischen Studentenbewegung 2011 entwickelte Tool soll Demonstrantinnen und Demonstranten helfen, sich (meist illegalen) Polizeikesseln, die deren Bewegungsfreiheit einschränken, zu entziehen.[11] Dazu nutzt die App neben manuell eingegebenen textuellen Daten auch die vom GPS-Sensor gelieferten Daten, um eine interaktive Karte zu erstellen, wo gerade ein Polizeikessel entstehen könnte. Hier zeigt sich exemplarisch die produktive Nutzbarmachung einer Technologie.

Anmerkungen

1 *M. Duckham, L. Kulik. Location privacy and location-aware computing. In J. Drummond, R. Billen, D. Forrest, E. Joao, editors, Dynamic & Mobile GIS: Investigating Change in Space and Time, chapter 3, pp. 34–51. CRC Press, Boca Raton, FL, 2006.*

2 *K. Virrantaus, H. Tirri, J. Veijalainen, J. Markkula, A. Katanosov, A. Garmash, V. Terziyan. Developing GIS-Supported Location-Based Ser-*

vices. In Proc. of WGIS 2001, volume 2, p. 66. IEEE Computer Society, 2001.

3 J. E. Dobson, P. F. Fisher. Geoslavery. Technology and Society Magazine, IEEE, 22(1):47–52, 2003.

4 http://www.heise.de/tp/artikel/34/34601/1.html , Zugriff 31.1.2013

5 http://www.guardian.co.uk/technology/2012/feb/15/apple-iphone-address-book-privacy , Zugriff 31.1.2013

6 http://fsfe.org/campaigns/android/android.html , Zugriff 31.1.2013

7 http://www.cyanogenmod.org/, Zugriff 31.1.2013

8 O. Diedrich, J. Wirtgen. Smartphone-Underdogs. C't 4/13, S. 17, 2013

9 M. Duckham, L. Kulik., a.a.O.

10 http://www.opensukey.org , Zugriff 31.1.2013

11 http://www.heise.de/tp/blogs/6/149205, Zugriff 31.1.2013

Stefan Hügel

Log 1/2013

Ereignisse, Störungen und Probleme der digitalen Gesellschaft

Immer wieder gibt es Ereignisse, Verlautbarungen und Entscheidungen, die im Zusammenhang mit dem fortschreitenden Abbau von Bürgerrechten stehen. Wir dokumentieren hier einige davon. Die Aufzählung ist sicherlich nicht vollständig; mit einigen besonders bedeutsamen Ereignissen wollen wir aber auf die weiterhin besorgniserregende Entwicklung hinweisen.

November 2012

4. November 2012: Google löscht acht rechtswidrige Suchergebnisse, die auf das angebliche Vorleben von Bettina Wulff verweisen. Drei der Ergebnisse stammen von der umstrittenen christlichen Seite kreuz.net. Die Anwälte von Bettina Wulff hatten die Löschung von 3000 Einträgen aus dem Google-Suchindex und zusätzlich 80 Begriffen aus der automatischen Vervollständigung von Suchanfragen gefordert (Quellen: Spiegel, Heise).

5. November 2012: Die Federal Trade Commission der USA kritisiert die fehlende Möglichkeit des *Do Not Track* für Verbraucher und erhöht damit den Druck auf den W3C-Standardisierungprozess. Sie befürworte zwar grundsätzlich Selbstregulierung, denke aber angesichts des mangelnden Fortschritts über gesetzliche Regelungen nach (Quellen: Politico, Heise).

5. November 2012: Einem Bericht zufolge hat Skype Nutzerdaten an das private Sicherheitsunternehmen *iSight Partners* weitergegeben. Es handelt sich um Daten eines Niederländers, der 2010 im Alter von 16 Jahren an DDoS-Attacken der *Operation Payback* mitgewirkt haben soll. Kurz darauf wurde der Mann festgenommen. iSight Partners wurde danach von der Firma Paypal beauftragt, die ebenfalls Ziel der damaligen Attacken in Folge der Einstellung des Geschäftsverkehrs mit Wikileaks waren (Quellen: nu.nl, Heise).

6. November 2012: Vor dem Bundesverfassungsgericht in Karlsruhe beginnt die Verhandlung über eine Verfassungsbeschwerde gegen die Antiterrordatei, in der Informationen zu Terrorverdächtigen und ihrem Umfeld zentral zusammengeführt werden. Die Datei verletze nach Ansicht des Beschwerdeführers, eines pensionierten Richters, eine Reihe von Grundrechten, darunter das Grundrecht auf informationelle Selbstbestimmung. Ferdinand Kirchhof, Vizepräsident des Bundesverfassungsgerichts sieht bei der Antiterrordatei „verfassungsrechtliche Probleme". Bundesdatenschutzbeauftragter Peter Schaar sieht bei der Datei „erhebliche Kontrolldefizite" und verweist auf die verfassungrechtlich gebotene Trennung von Polizei und Nachrichtendiensten (Quellen: Bundesverfassungsgericht, Heise).

9. November 2012: Forschungsprojekte, an denen auch das Bundeskriminalamt (BKA) und die Bundespolizei beteiligt sind, haben das Ziel, mit Hilfe von multimodalen biometrischen Gesichtserkennungssystemen auf Basis von 3D-Bildern Personen aus Foto- und Videodateien zu identifizieren. Dies geht aus der Antwort auf eine kleine Anfrage des Bundestagsabgeordneten Andrej Hunko (Die LINKE) hervor. Gleichzeitig ist das Deutsche Forschungszentrum für künstliche Intelligenz (DFKI) in Saarbrücken am EU-Projekt *iCOP (Identifying and Catching Originators in P2P Networks)* beteiligt (Quellen: Andrej Hunko MdB, Heise).

9. November 2012: Der Teilnehmer der Demonstration *Freiheit statt Angst*, der 2009 von Polizeibeamten zusammengeschlagen wurde, erhält ein Schmerzensgeld von € 10.000. Aus Sicht des Anwalts des Opfers sei die Entschädigung im Vergleich zu ähnlich gelagerten Fällen ungewöhnlich hoch, aus Opfersicht aber eher bescheiden. Die verantwortlichen Beamten wurden bereits zuvor in einem Strafverfahren zu je 120 Tagessätzen verurteilt (Quellen: taz, Heise).

9. November 2012: Nach Ansicht des Leiters der deutschen Niederlassung des Überwachungstechnik-Spezialisten und Herstellers der Software *FinFisher, Gamma International,* rette dessen Software Leben und helfe dabei, Kriminelle zu fassen. Er nannte aber keine konkreten Beispiele. Gamma liefere keine Software an Diktaturen und sei auch nicht für die Überwachung in Ägypten und Bahrain verantwortlich. Im ersten Fall sei ein geplantes Geschäft nicht zustande gekommen, im zweiten Fall sei eine gehackte Demoversion verwendet worden (Quelle: Heise).

12. November 2012: Verantwortlichen des Projekts *INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment)* zufolge ziele das Projekt nicht auf eine Unterwanderung des Datenschutzes sondern vielmehr auf dessen Stärkung. Es würden auch Werkzeuge zum Schutz sensibler Daten vor Missbrauch entwickelt. Sicherheitsbehörden dürften aber persönliche Daten Verdächtiger und Krimineller ohne Wissen oder Einwilligung zur Strafverfolgung oder zur Gefahrenabwehr nutzen (Quellen: Andrej Hunko MdB, Heise).