Arbeiterkammer Wien
Abteilung Konsumentenpolitik
Prinz-Eugen-Straße 20-22
A-1041 Wien
Tel: ++43-1-501 65/3136 DW
Fax: ++43-1-501 65/2693 DW
Internet: www.ak-konsumentenschutz.at
E-Mail: konsumentenpolitik@akwien.at

35/2012
Juli/2012

AKTUELLE FRAGEN DER GEODATEN-NUTZUNG AUF MOBILEN GERÄTEN

ENDBERICHT

ITA-PROJEKTBERICHT NR.: A63
ISSN: 1819-1320
ISSN-ONLINE: 1818-6556

INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
DER ÖSTERREICHISCHEN AKADEMIE DER WISSENSCHAFTEN

Projektleitung: Dr. Walter Peissl

Autoren: Robert Rothmann, MA
Jaro Sterbik-Lamina, MSc
Dr. Walter Peissl
Mag. Johann Čas

STUDIE IM AUFTRAG DER BUNDESARBEITSKAMMER

WIEN, JUNI 2012

IMPRESSUM

Medieninhaber:
Österreichische Akademie der Wissenschaften
Juristische Person öffentlichen Rechts (BGBl 569/1921 idF BGBl I 130/2003)
Dr. Ignaz Seipel-Platz 2, A-1010 Wien

Herausgeber:
Institut für Technikfolgen-Abschätzung (ITA)
Strohgasse 45/5, A-1030 Wien
www.oeaw.ac.at/ita

Die ITA-Projektberichte erscheinen unregelmäßig und dienen der Veröffentlichung
der Forschungsergebnisse des Instituts für Technikfolgen-Abschätzung.
Die Berichte erscheinen in geringer Auflage im Druck und werden über das Internetportal „epub. oeaw" der Öffentlichkeit zur Verfügung gestellt:
epub.oeaw.ac.at/ita/ita-projektberichte

ITA-Projektbericht Nr.: A63
ISSN: 1819-1320
ISSN-online: 1818-6556
epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a63.pdf

Inhalt

Tabellenverzeichnis

Zusammenfassung

Zwei Entwicklungen der letzten Jahre haben zu einem Problem geführt, dem bisher noch kaum Beachtung geschenkt wird: Die Analyse und Ausbeutung von Geodaten, die durch die zunehmende Ausstattung mobiler Geräte mit GPS-Sensoren ermöglicht werden, und die steigende Durchdringung des Marktes mit Smartphones, deren Funktionsumfang mit Apps erweitert werden kann.

Die heute selbstverständliche Verfügbarkeit von Geodaten sowie die genaue Zuordenbarkeit der einzelnen Geräte zu bestimmten Personen ermöglichen Werbetreibenden eine neue Dimension der Profilerstellung, die hohe Profite für die nächsten Jahre verspricht. Während NutzerInnen sich dessen bzw. der Folgen dieser Profiling-Prozesse kaum bewusst sind, und das Grundrecht auf Privatsphäre oft als vernachlässigbares Gut in Frage stellen, entledigen sich Hersteller und Service-Anbieter ihrer Verantwortung, und Datenschutzeinrichtungen sind oftmals nicht in der Lage, bestehendem Recht zur Durchsetzung zu verhelfen, was aber auf Grund der nationalen Zuständigkeiten, der unübersehbaren Menge an Apps und der hohen Dynamik in diesem Feld kaum gefordert werden kann.

Vor allem die hohe Verbreitung von Smartphones und geodatenbasierten Services unter Jugendlichen ist bedenkenswert. Während man als Kind und JugendlicheR als nicht voll geschäftsfähig gilt, scheint diese Altersgruppe in Bezug auf die Smartphonenutzung dem Streben nach Überwachung und/oder Profitmaximierung verschiedener Unternehmen hilflos überlassen zu werden. Aber auch insgesamt, über alle Altersgruppen, hat die Zahl der SmartphonebesitzerInnen so stark zugenommen, dass es hier eine sehr große Zahl Betroffener gibt.

An Hand von Apps, wie bspw. „Paper Toss“, einem einfachen Spiel, das Geodaten gar nicht benötigen würde, den Standort der AnwenderInnen aber gemeinsam mit deren eindeutiger Telefon-ID an fünf internationale Werbenetzwerke überträgt, oder „Text Plus“, einer App für Textnachrichten, die Geschlecht, Alter, Position und Telefon-ID an sieben internationale Werbenetzwerke weitergibt, oder „Best Alarm Clock Free“, das als Wecker Position und Telefon-ID an fünf Werbenetzwerke meldet, wird deutlich, dass die einzelnen Apps in manchen Fällen als Fassaden bezeichnet werden müssen, die den eigentlichen Zweck, nämlich das Datensammeln, verschleiern sollen.

Wer hätte die Ressourcen, um sich dieses Problems anzunehmen? Abgesehen von exemplarischen Musterprozessen vermutlich niemand, weil die Menge der zu überprüfenden Firmen und Anwendungen zu groß wäre. Letztendlich handelt es sich aus europäischer Sicht jedenfalls um ein Binnenmarktproblem, weil alle KonsumentInnen in Europa davon gleichermaßen nachteilig betroffen sind. Deshalb läge es wohl an der EU-Kommission, die als einzige die nötige Verhandlungsmacht haben dürfte, europäische Datenschutzstandards gegenüber den großen Hard- und Softwarefirmen durchzusetzen und von Betreibern wie Apple und Google eine Überprüfung ihrer zahlreichen Geschäftspartner zu verlangen.

In der vorliegenden Studie werden unterschiedliche Motivationen, Apps zu nutzen, ebenso beleuchtet, wie die Funktionsweise und die Konsequenzen, die sich aus der aktuellen Entwicklung ergeben. Letztendlich bleibt jedoch eine Frage unbeantwortet: Wohin entwickelt sich unsere Gesellschaft, welche Art neuer Abhängigkeitsverhältnisse entstehen in Zukunft, und wird es der/dem Einzelnen noch möglich sein, diesen Abhängigkeiten zu entgehen?

Um dieses und andere drängende Probleme in den Griff zu bekommen, wurden Empfehlungen an unterschiedliche Stakeholder entwickelt und im letzten Kapitel ausgeführt.

1 Einleitung

Im Jahr 2010 waren weltweit etwa 600 Millionen Smartphones im Einsatz, wobei einjährliches Wachstum von rund 20 Prozent prognostiziert wird, und der Verkauf von Smartphones die Zahl der PCs im Jahr 2012 endgültig übersteigen soll (vgl. Castelluccia 2012; Manyika et al. 2011). Mitunter wird bereits von *Post-PC Devices* gesprochen.

Worin besteht das Problem?

Über den Hardware-Verkauf hinaus eröffnen Smartphones als persönlicher Multimedia-Begleiter im Alltag eine enorme Wertschöpfung durch zusätzliche Servicefunktionen in Form von Software-Applikationen sowie der damit einhergehenden Generierung und Weiterverarbeitung detaillierter digitaler Informationen.

Gleichzeitig häufen sich Bedenken über den Umgang mit dieser Menge personenbezogener Daten. In den Medien wird diese Entwicklung mit teils besorgniserregenden Schlagzeilen wie „*Schnüffelsoftware konnte SMS abfangen*“[1], „*Aufregung um russische 'Stalking'-App*“[2] oder „*iPhone-Bug ermöglicht Zugang zu Adressbuch*“[3] kommentiert. Diese Besorgnis ist nicht unbegründet, wie sich an Beispielen datenhungriger Apps zeigen lässt, die Daten sammeln und sie an verschiedene Werbenetzwerke weitergeben, ohne die UserInnen darüber zu informieren und oft auch ohne die Daten tatsächlich zu benötigen.

Der hohen Dynamik des Feldes bewusst, versucht die vorliegende Studie dennoch, die sozialen und datenschutzrechtlichen Implikationen der Generierung personenbezogener Geo- bzw. Ortungsdaten über Smartphones zu analysieren. Dabei wird neben den technischen Aspekten und Funktionsweisen besonderes Augenmerk auf das systematische Sammeln und Weiterverarbeiten von Informationen für Marketingzwecke und serviceorientierte Überwachung der Bevölkerung gelegt. Die Diskussion mündet schließlich in der Formulierung von Empfehlungen für Smartphone-UserInnen, Politik, Wirtschaft und InteressensvertreterInnen.

1.1 Geodaten

Wie funktioniert die Ortung?

Zunächst werden die verschiedenen technischen Möglichkeiten und Verfahren zur geografischen Ortung (bzw. Positionsbestimmung) von Telefonen und der weiteren Objektverfolgung (Tracking) besprochen.

Dabei sei zuerst auf die sog. GPS-Technologie eingegangen. Das „Navigational Satellite Timing and Ranging – Global Positioning System“ (NAVSTAR GPS) ist ein globales Satellitensystem, das vom US-Verteidigungsministerium etwa seit den 1970er Jahren zum Zweck der Navigation und Positionsbestimmung sowie zur Zeitmessung entwickelt und 1995 offiziell in Betrieb genom-

[1] http://help.orf.at/stories/1691796/ (02.06.2012).

[2] http://orf.at/stories/2113256/ (02.06.2012).

[3] http://derstandard.at/1329870145613/Leck-in-iOS-501-iPhone-Bug-ermoeglicht-Zugang-zu-Adressbuch (02.06.2012).

men wurde.[4] Über die Laufzeit kodierter Radiosignale zwischen Satelliten und Beobachtungsobjekt (in unserem Fall das Smartphone) lassen sich Aufenthaltskoordinaten inkl. Höhenangaben errechnen. Eine Anzahl von 24 bis 30 Satelliten stellt sicher, dass die Empfangsgeräte möglichst konstant Signale von mindestens vier Satelliten gleichzeitig empfangen (drei Satelliten für Raumkoordinaten und ein Satellit zur Zeitkorrektur). Mittels satellitengestützter Zusatzsysteme, engl. Satellite-Based Augmentation Systems (SBAS), und der Aussendung von Korrekturdaten werden trotz diverser physikalischer Einflussfaktoren und dadurch bedingter Verzögerungen und Messungenauigkeiten mitunter zentimetergenaue Positionsangaben möglich.

Für die Lokalisierung von Smartphones kann GPS als Basisverfahren verstanden werden. Da jedoch Satellitensignale nicht immer stark genug sind, um Positionsangaben in geschlossenen Gebäuden zu ermöglichen, wird zur Smartphone-Ortung auch mit Zusatzinformationen über separate Datenverbindungen gearbeitet.[5] Das *Assisted Global Positioning System* (A-GPS) Modul eines Smartphones ermöglicht die Positionsbestimmung durch Triangulation der Zusatzdaten von *Wireless Local Area Network* (WLAN-) *Access Points* und Funkzellen des *Global Systems for Mobile Communications* (GSM) bzw. *des Universal Mobile Telecommunications Systems* (UMTS). Sowohl im Fall der WLAN Access Points als auch im Fall der Mobilfunkzellen werden zur Lokalisierung Datenbanken mit Positionsinformationen herangezogen. Diese Datenbanken werden z. B. von Anbietern wie *Skyhook* oder *Navizon* erstellt und gegen Bezahlung verfügbar gemacht. In diesen Fällen stellt der Sensor des Smartphones fest, welche Funkzellen und Access Points in seiner Umgebung sind, übermittelt diese Information an einen jener Datenbankbetreiber und erhält daraufhin die Standortdaten, wo sich das Gerät zurzeit befindet. Die Ortungsmethode über WLAN und GSM ermöglicht auch eine ungefähre Positionsbestimmung, wenn kein GPS Signal vorhanden ist. Zudem liefert sie eine schnelle Initial-Ortung, bis die Position über das etwas verzögert arbeitende GPS exakt bestimmt wird (vgl. Teufl und Dietrich 2010). Die ARTICLE 29 Data Protection Working Party (2011) verweist zudem darauf, dass die Exaktheit mit Informationen wie RSSI (Received Signal Strength Indicator) oder TDOA (Time Difference of Arrival) noch weiter erhöht werden kann.

Was sind Geodaten?

Je nach Form der Auswertung und Weiterverarbeitung inkludieren Ortungsdaten (location data) die folgenden Informationen:

- Längen und Breitengrad
- Postleitzahl (Bezirk bzw. Ortsteil, Stadt, Bundesland, Staat)
- Straße und Hausnummer.

Darüber hinaus sind die zeitliche Komponente und das durch wiederholtes Messen mögliche Erstellen raum-zeitlicher Datensets zu erwähnen. In diesem Zusammenhang wird von Bewegungsprofilen und sog. *Tracking* gesprochen.

---

[4] Das Konzept zur Entwicklung eines Satellitennavigationssystems geht in die 1960er Jahre auf Ivan A. Getting zurück. Neben den USA verfügen auch andere Staaten über Satellitennavigationssystem oder bauen derartige auf (z. B. Galileo/Europa, Glonass/Russland, Compass/China etc.).

[5] http://www.wi-fiplanet.com/tutorials/article.php/1487271 (02.06.2012).

Wer speichert Daten?

Immer mehr Unternehmen, speichern in ihren Systemen über Anwendungen (Apps) auf den Endgeräten Standortdaten und Bewegungen (vgl. Castelluccia 2012). In der Verwaltung dieser Daten können drei Typen von Einrichtungen als zentral herausgestellt werden:

- Inhaber und Netzbetreiber der Geolocation-Infrastruktur (insbesondere der Satellitensysteme, der WLAN Access Points sowie der GSM- bzw. UMTS-Funkzellen);
- Anbieter von Geolocation-Diensten und Softwareanwendungen (Apps);
- Entwickler von Smartphones und Smartphone-Betriebssystemen.

1.2 Smartphones

Unter einem Smartphone wird ganz allgemein ein Mobiltelefon mit erweiterten IT-Funktionen – insbesondere einem Internetzugang – verstanden. Smartphones sind zudem mit einer Reihe an Sensoren ausgestattet. Als weiteres Merkmal und Wendepunkt für den Smartphone-Markt gilt die Einführung des Multi-Touch-Screen am iPhone durch Apple im Jahr 2007.[6]

Was macht ein Phone smart?

Smartphones verfügen heute in den Regel über folgende Eigenschaften (vgl. Hogben and Dekker 2010):

- Größenfaktor (Hosen-)Taschenformat
- leistungsstarke Prozessoren (1 GHz und Dual-Core-Prozessoren) und Speicherplatz im Gigabyte-Bereich
- mehrere Netzwerkverbindungen (WAN, LAN, und PAN) und multiple Funk-Schnittstellen wie z. B. WiFi, GSM, UMTS, Bluetooth, etc.
- ein Set an Sensoren inkl. Mikrophon, Kamera, GPS, Akzelerometer (Beschleunigungssensor), Lagesensor (Kompass) sowie Licht- und Näherungssensoren, Magnetfeldsensoren und (häufig auch interne) Temperatursensoren
- funktionsreiches Userinterface, fähig zur Wiedergabe vollständiger Web-Seiten
- Application Marketplace (oder App-Store).

Smartphones können für eine Vielzahl von Aktivitäten genutzt werden und sind nicht zuletzt aufgrund von Größe und Mobilität als überaus persönliche Geräte zu bezeichnen (vgl. Düsseldorfer Kreis 2011). Im Gegensatz zu herkömmlichen PCs sind Mobiltelefone in der Regel konkreten Einzelpersonen zuzuordnen. Das Smartphone befindet sich meist in unmittelbarer Umgebung des Besitzers. Über das Touchpad erhält das Gerät zusätzlich eine sensitive Ebene. Es wird selten aus der Hand gegeben und nur ungern an (un-)bekannte Dritte verborgt. UserInnen sind sich dessen bewusst, dass das Smartphone ein höchst persönlicher Gegenstand ist, der in Form von E-Mails, Kurznachrichten (SMS), Fotos oder Kontaktlisten zahlreiche private, mitunter sogar intime Informationen speichert (vgl. ARTICLE 29 Data Protection Working Party 2011).

Wie wird mit den eigenen Daten umgegangen?

In starkem Widerspruch dazu steht die Praxis im Umgang mit den eigenen Daten auf digitaler Ebene. Im Kontext einer (ursprünglich nicht intendierter) Veröffentlichung und Weitergabe personenbezogener Informationen, z. B. im Fall eines Datenzugriffs durch Smartphone-Apps, wird von Privatpersonen

[6] http://de.wikipedia.org/wiki/Smartphone (02.06.2012).

gerne das Argument vorgebracht, *„sie hätten nichts zu verbergen und daher auch nichts zu befürchten“* (vgl. Solove 2008). Was auf analog-manueller Ebene als unangemessen gilt, wird auf digital-virtueller Ebene toleriert und oft unreflektiert zugelassen. Interessanterweise ändert sich dies jedoch rasch, sobald das Smartphone als Geschäftstelefon (Firmentelefon von EntscheidungsträgerInnen) genutzt wird. Hier wird der rechtliche Anspruch auf Geheimhaltung von Daten, Informationen und Kontakten unverzüglich geltend gemacht und von Dritten auch nicht weiter in Frage gestellt. Ungeachtet der grundrechtlichen Verankerung werden die eigene Privatsphäre und der Anspruch auf Datenschutz anscheinend erst dann verteidigt bzw. als legitim erachtet, wenn ökonomische Interessen und potentielle Wettbewerbsvorteile im Spiel sind. Die vorliegende Studie wird im weiteren Verlauf zeigen, dass eine derartige Auffassung von Privatsphäre zu kurz greift, und eine freiwillige Veröffentlichung der eigenen personenbezogenen Daten von diversen Organisationen monetär (aus-)genutzt wird und u. a. zu stereotypen Klassifizierungen von Einzelpersonen führen kann.

Die Veröffentlichung der Daten bringt anderen finanzielle Vorteile

1.2.1 Apps und Markets

Wie unterscheidet man Apps und Applications?

Smartphones werden ab Werk lediglich mit einem rudimentären Betriebssystem ausgestattet, wodurch die Funktionen auf wesentliche Dinge wie Telefonie, SMS und wenige andere Anwendungen begrenzt sind (vgl. Achten und Pohlmann 2012). In Verbindung mit entsprechender Zusatzsoftware (Software-Applikationen) von Drittanbietern eröffnet sich für SmartphonebesitzerInnen jedoch eine breite Palette von Anwendungsbereichen. Die im täglichen Sprachgebrauch als *App* (von engl. *application)* bezeichneten Anwendungsprogramme, die sich von Anwendungen auf Desktop-Betriebssystemen durch ihre geringere Komplexität deutlich unterscheiden[7], in der Regel über in das Betriebssystem integrierte Internet-Verkaufsportale (sog. Onlineshops) bezogen und so direkt auf dem Telefon installiert werden. Zu diesen Onlineshops zählen u. a. der Apple *App-Store*, der *Windows Phone Marketplace* von Microsoft, *Google Play* (früher Android Market), der *Nokia Store* (früher *Ovi Store*), *BlackBerry App World* von RIM (Research in Motion) sowie *PlayNow* von Sony Ericsson, *Amazon Appstore for Android* (nur USA) oder *Samsung Apps*.

Technisch gesehen gibt es Apps auf Mobiltelefonen bereits seit Jahren, doch erst das Erscheinen der Programmiersprache *Java* für Telefone (in der Version ME-Micro Edition) und die Eröffnung des Apple App-Stores im Juli 2008 brachten den Durchbruch (vgl. Thurm und Kane 2010). Heute bietet der App-Store mehr als 580.000 Applikationen zum Download an.[8] Andere Hersteller-

---

[7] Anwendungen, Applications, die auf sog. Desktop-Betriebssystemen, wie Microsoft Windows, MacOS u. ä., laufen, sind in der Regel eine relativ komplexe, aufwendig programmierte Software, die oft in einem eigenen Verzeichnis liegt, Systemressourcen mit anderen Programmen teilt, Konfigurationsdaten manchmal gesondert (im Fall von Microsoft Windows z. B. in der Registry) ablegt und sich oft in Firmennetzwerken zentral managen lässt. Apps, die auf Smartphone-Betriebssystemen laufen, sind in der Regel deutlich einfacher in ihrer Software-Architektur. Diese begriffliche Trennung hat sich im Englischen bis heute erhalten und wird möglicherweise erst durch die Einführung von Microsoft Windows 8 aufgeweicht, wo alle Programm, egal wofür sie geschrieben wurden, als „Apps“ bezeichnet werden sollen, um den plattformübergreifenden Charakter des Betriebssystems zu unterstreichen.

[8] Eric Slivka (07.03.2012): Live Coverage of Apple’s iPad 3 Media Event. In: *macrumors.com*. http://www.macrumors.com/2012/03/07/live-coverage-of-apples-ipad-3-media-event/ (20.03.2012).

firmen wie Research in Motion und Nokia folgten nach. Auch Googles Android Market (heute Google Play) eröffnete noch im Jahr 2008 und bot mit Februar 2012 rund 640.000 Apps zum Download an.

Mit Apps wird mehr Geld verdient als mit den Telefonen selbst

Das Anbieten von Apps als zusätzliches Service und potentielle Erweiterung der Funktionspalette des Telefons ist wesentlicher Teil des Geschäftsmodells der meisten Anbieter, weshalb es derzeit auch nur hersteller- bzw. systemspezifische Stores bzw. Markets gibt. So ist der Apple *App-Store* lediglich Verkaufsportal für iOS-Geräte (iPhone, iPod touch, iPad) und der *Windows Phone Marketplace* die einzige Möglichkeit, weitere Anwendungen auf ein Windows Phone zu installieren. Der *Google Play Store* (ehemaliger Android Market) ist wiederum eine Software, die nur auf Smartphones und Tablet-Computern mit Android-Betriebssystem ausgeliefert wird.[9]

Die in den Stores und Markets angebotenen Programme stammen zum Großteil von Drittfirmen und freien ProgrammiererInnen. In den meisten Fällen kann der Preis vom Entwickler bestimmt werden, je nach Verkaufsportal muss dieser jedoch etwa 30 bis 40 Prozent der Einnahmen an den Portal-Betreiber abgeben. Die Plattformen verfügen auch über eine große Auswahl an kostenlosen Programmen.[10] Die Portal-Betreiber behalten sich vor, die jeweilige App nach einer Prüfung abzulehnen. Google prüft die Apps in der Regel nicht, sondern ist der Meinung, dass die App-Produzenten selbst die Verantwortung für den Umgang mit Nutzerinformationen tragen. Bei Beanstandung durch KundInnen werden einzelne Apps jedoch geprüft und gegebenenfalls aus dem Sortiment genommen. Bei Apple wird ein restriktiverer Umgang mit Apps gepflegt, der mitunter auch Ansätze inhaltlicher Zensur enthält. Auch wenn Apple angibt, eine Prüfung der von Entwicklern hochgeladenen Programme vorzunehmen, findet diese auf Grund der großen Anzahl nicht gründlich statt. Unter anderem wegen des Preisdrucks am App-Markt und der geringen Hürden für Programmiereinsteiger zeichnen sich viele Apps durch schlechte Sicherheitseigenschaften aus (vgl. Heider und Khayari 2012).

Was können die Apps am Telefon finden?

Neben ihrer offiziellen Funktion haben Apps auch häufig Zugriff auf Gerätekennung, Standortdaten, E-Mail- und Telefonkontakte, Sim-Kartennummer sowie weitere personenbezogene Daten und Sensorinformationen, die sie mitunter ohne nähere Information der NutzerInnen an Gerätehersteller, Provider oder Anbieter von Analysediensten übermitteln (vgl. Heider und Khayari 2012). Auch wenn die eigentliche Zustimmung für den Datenzugriff erteilt wurde, sind sich Smartphone-UserInnen nicht immer über alle Funktionalitäten und den Umfang des Zugriffs auf die eigenen Daten durch die diversen Apps bewusst (vgl. Hogben und Dekker 2010).

Wozu brauchen Apps Geodaten?

Apps mit nötigem Zugriff auf Geodaten wären z. B. ein Dienst, der das Wetter für die nächsten Stunden in einer ganz bestimmten Region prognostiziert, eine App, die Informationen über Geschäfte, Kaffeehäuser oder Restaurants in der näheren Umgebung anbietet, ein Service, das hilft, das Mobiltelefon bei Verlust wiederzufinden, oder eine Dienstleistung, die den Aufenthaltsort von Freunden anzeigt (vgl. ARTICLE 29 Data Protection Working Party 2011). Auch Augmented-Reality-Apps oder Soziale Netzwerke greifen über Nachrichten (Microblog-Postings) auf Geodaten zu. Oft sind Standortdaten auch in Metadaten von Fotos enthalten. BenutzerInnen, die einer App Zugriff auf Bild-Dateien gestatten, könnten damit z. B. ungewollt ihre Aufenthaltsdaten offenlegen (vgl. Hogben und Dekker 2010).

---

[9] *Google Play Store* vereint die Portale *Google Music*, *Google Movies* und *Google Books*. Die entsprechende Umstellung erfolgte mit März 2012.

[10] http://de.wikipedia.org/wiki/Google_Play (02.06.2012).

2 Verarbeitung der Daten

In einer digitalisierten postindustriellen Informationsgesellschaft gilt die monetäre Verwertung personenbezogener Daten als ökonomischer Schlüsselfaktor. Die Verarbeitung und „Anreicherung" von Daten ist ein eigener Geschäftszweig. Den extrahierten Informationen wird marktrelevantes Potential zur Steigerung der Produktivität, der Wettbewerbsfähigkeit sowie zur Wertsteigerung von Unternehmen zugeschrieben. Auch der öffentliche Sektor sowie die EndverbraucherInnen profitieren von gezielt aufbereiteten Daten für logistische Entscheidungen oder Safety-Services (vgl. Čas und Peissl 2006; Manyika et al. 2011; Riederer et al. 2011).

Warum werden so viele Daten gesammelt?

Die Möglichkeit zur Nutzung personalisierter Geo- bzw. Standortdaten führte zu einer Reihe von Unternehmensgründungen und innovativen Geschäftsmodellen. Die Verwendung personenbezogener Standortdaten ist dabei nicht auf einen einzigen Sektor beschränkt, sondern in vielen Branchen, wie der Telekommunikation, dem Einzelhandel oder in den Medien angesiedelt. Das Consulting Unternehmen McKinsey[11]geht davon aus, dass durch die Vermarktung von (Geo-)Daten über die nächsten zehn Jahre eine enorme Wertschöpfung stattfindet. Es wird mit einem globalen Umsatz von mehr als 100 Milliarden US-Dollar auf Provider-Seite und etwa 700 Milliarden US-Dollar Umsatz auf Verbraucher- bzw. Anwenderseite gerechnet (Manyika et al. 2011).

Werbeausgaben für Werbung auf Mobiltelefonen wachsen schneller als der restliche Werbemarkt. Gerade dann, wenn diese geodatenbasiert funktionieren, gilt dies als innovatives und lukratives Marketing-Werkzeug, das bis zum Jahr 2020 mehr als fünf Prozent der weltweiten Gesamtausgaben für Werbung darstellen könnte (vgl. Manyika et al. 2011).[12] Als wesentlich gilt hierfür u. a. das Geschäftsmodell Werber mit App-Anbietern in Kontakt zu bringen. Viele Werbenetzwerke offerieren Software-Zusätze, die Werbung automatisch in Apps integrieren. Derartige Module verfolgen neben den Standortdaten z. B. auch die Zeitspanne, die KundInnen mit einer App verbringen (vgl. Hogben und Dekker 2010).

Das Sammeln der Daten wird forciert

In einer Studie des *Wall Street Journals* (Thurm und Kane 2010) wird davon berichtet, dass App-Produzenten mitunter dazu angehalten werden, mehr personenbezogene Daten zu erfassen. Max Binshtok, der Entwickler der Android App *DailyHoroscope* gibt an, dass Führungskräfte von Werbenetzwerken ihn dazu ermutigt haben, die Standortdaten der NutzerInnen zu übertragen, da Werbeanzeigen mit gezieltem Ortsbezug zwei- bis fünfmal so viel Geld bringen wie ungezielte Anzeigen.

---

[11] Neben geeigneten Organisationen braucht es dazu ausreichend Investitionen in Technologie, Infrastruktur und Personal sowie entsprechende Maßnahmen von Seiten der Regierungen; James Manyika et al., 'Big Data: The Next Frontier for Innovation, Competition, and Productivity', (McKinsey Global Institute, 2011).

[12] Als weiteres Beispiel für den Geldfluss im Smartphone Markt sei auf das Unternehmen eBay verwiesen, dessen Transaktionen über die eigene iPhone-App allein für das Jahr 2010 auf 1,3 bis 1,5 Milliarden Euro geschätzt werden (vgl. Hogben und Dekker 2010).

2.1 Service by Surveillance

Warum?

Das Sammeln und Verarbeiten von Daten (insb. großen Datensätzen mit personenbezogenen Informationen) generiert laut Manyika et al. (2011) durch folgende Prozesse ökonomischen (und politischen) Mehrwert:

- Schaffung von Transparenz und Überblick
- Bedürfnisse werden aufgedeckt bzw. entdeckt, Variabilität wird freigelegt und Leistung bzw. Effizienz wird gesteigert
- die Bevölkerung kann nach Kundenwünschen segmentiert werden
- menschliche Entscheidungsfindung kann von automatisierten Algorithmen abgelöst, ersetzt und/oder durch diese unterstützt werden
- die Hervorbringung neuer/innovativer Geschäftsmodelle, Produkte und Dienstleistungen wird gefördert.

Service versus Überwachung

Aus soziologischer Sicht handelt es sich bei den aufgelisteten Punkten – der Schaffung von Transparenz und Überblick, dem Aufdecken von Bedürfnissen oder dem Segmentieren der Bevölkerung – nicht nur um Serviceangebote sondern auch um Prozesse der Überwachung. Von gesellschaftstheoretischer Seite wird grundsätzlich davon ausgegangen, dass sich die digitale Informationsgesellschaft u. a. durch neue Formen technologischer Mobilität auszeichnet, wodurch herkömmliche Mechanismen der Überwachung und die „Physik" der Macht (Foucault 1994) zusehends auf einen direkten körperlich-physischen Zugriff verzichten (Lyon 1994). Bereits Ende der 1980er Jahre postulierte der französische Philosoph Gilles Deleuze (1993) das Auftauchen von neuen *„ultra-schnellen Kontrollformen mit freiheitlichem Aussehen"*, die die alten, innerhalb eines geschlossenen Systems operierenden Verfahren ersetzen werden. Smartphones scheinen eine nahezu idealtypische Materialisierung dieser neuen Mobilität. Durch das Auftauchen dieser Geräte ist eine technische wie inhaltliche Ausweitung und Diffusion der Überwachung auf diverse Alltagshandlungen zu beobachten. Das Phänomen der Überwachung ist nicht mehr ausschließlich auf strafrechtlich relevantes Verhalten und dessen Sanktionierung beschränkt. Mittels subtiler Verfahren auf abstrakter Datenebene werden nun auch diverse, scheinbar unwichtige, Situationen und Handlungsroutinen erfasst und analysiert. Überwachung tritt in diesem Sinne nicht mehr nur als bedrohliches Kontrollphänomen autoritärer Systeme auf, sondern zeigt sich vermehrt als Monitoring-Maßnahme mit Management- und Servicecharakter (vgl. Lyon 2005). Auf Grund des wohlwollenden und oft verspielten Charakters der verschiedenen Services empfinden UserInnen die Prozesse der Datensammlung nicht als externe Kontrollmaßnahmen. Die betroffenen Individuen sind nicht nur freiwillig dazu bereit personenbezogene Informationen preiszugeben, sondern die verschiedenen Prozesse der Überwachung sogar selbst auszuführen und mitunter für die Infrastruktur zur Gewährleistung der Datengenerierung und Übertragung obendrein zu bezahlen.

2.2 (Geodaten-)Anwendungen

In welchen Bereichen werden Geodaten eingesetzt?

In einem nächsten Schritt soll nun auf die verschiedenen Serviceangebote eingegangen werden, die in Teilen auch Kontroll- und Überwachungscharakter in sich tragen und auf Geodaten zugreifen. Diese können ihrer Funktion und Nutzung entsprechend in die folgenden Bereiche untergliedert werden:

- Freizeit, Freunde, Körper, Sport, Gesundheit und Ernährung,
- Handel, Marketing und Werbung,
- Soziale Dienste, Sicherheit und Strafverfolgung (Safety & Security),
- sowie Verkehr und Logistik.

Die Zuordnung in die Kategorien fällt nicht immer trennscharf aus. Besonders zwischen der unternehmensseitigen und der logistischen Nutzung sind die Grenzen fließend. Zudem funktionieren die diversen Services nicht immer nur auf Basis von Geodaten allein. Oft kommt eine Reihe an Sensoren zur Anwendung um Situationen und Verhalten zu interpretieren. Diese Entwicklung wird auch als *Urban Sensing* bezeichnet. Darunter versteht man allgemein eine Berücksichtigung sämtlicher Sensordaten im räumlichen Umfeld und Nahebereich, wobei Individuen bzw. SmartphonebenutzerInnen im System als Empfänger und auch Sender von Information partizipieren (vgl. Campbell et al. 2006).

Im Folgenden soll anhand einiger Beispiele etwas näher auf die einzelnen thematischen und funktionalen Bereiche zur Verwertung von Geodaten und anderen Sensorfunktionen eingegangen werden.

2.2.1 Freizeit, Freunde, Körper …

Warum ist digital ein Problem, was analog keines war?

Schon bevor Smartphones in der Lage waren, Ortungsdienste zu erbringen, gab es für EndverbraucherInnen verschiedene Geräte und Informationssysteme (z. B. GIS), die Geodaten in einem bestimmten Kontext zur Verfügung gestellt haben. Allen voran Navigationsgeräte, die im motorisierten Individualverkehr oder beim Sport (Wandern oder Joggen) Verwendung fanden, einerseits zur Orientierung im Gelände, andererseits aber auch, um den zurückgelegten Weg und die erbrachte Leistung zu dokumentieren. Durch diese Geräte kam es in weiterer Folge auch zu spielerischen Anwendungen wie Geo-Caching. Heute werden all diese Funktionen in unterschiedlicher Qualität auch von Smartphones erbracht.

Wie stolpert man in die „Geodaten-Falle"?

Eine andere, bereits etwas etabliertere Form der Geodatenanwendung ist das Speichern von Standortinformationen in den Meta-Daten digitaler Bilder (Georeferenzierung). Dabei werden die Bild-Dateien im Zuge der Aufnahme automatisiert getagged (mit den Koordinaten versehen). In anderen Fällen übernehmen das Taggen die UserInnen, die ihre Bilder im Internet zur Verfügung stellen. Mit Diensten wie z. B. *Google Maps* (gemeinsam mit Picasa), *FourSquare* (mit April 2011 mehr als 8 Millionen UserInnen), *Google Latitude* oder *Facebook Places*, werden Geo- und Bilddaten verknüpft (falls das nicht bereits bei der Aufnahme durch das Gerät mit GPS-Sensor erfolgt) und meist einem weiteren Personenkreis zugänglich, indem UserInnen sie auf Plattformen hochladen und mit Schlagworten versehen, oder sich einfach nur an bestimmten Orten „einchecken". In Social Networks werden diese Daten mit weiteren Statusangaben verknüpft. Auch *Loopt* ist einer dieser App-Dienste (mit April 2011 mehr als 5 Million UserInnen), der es seinen Mitgliedern erlaubt, Aufenthaltsstatus, Status-Message und Fotos in Echtzeit zu teilen. Den eigentlichen Gewinn generiert Loopt durch gezielte geodatenbasierte Werbung (vgl. Manyika et al. 2011). Da viele UserInnen des Fotodienstes *Flickr* Be-

denken entwickelten, weil über die mit dem Bild verknüpften Geodaten ihrer Fotos für Fremde erkennbar wurde, wo sie lebten oder ihre Kinder zur Schule gingen, lancierte die Webseite eine Funktion, die „Geofence“ genannt wurde und die Geodaten nur einem bestimmten Kreis von Kontakten zugänglich machte. Durch einen Designfehler in der Implementierung der Funktion verblieben die Geodaten jedoch im sog. Header des Bildes (Meta-Daten zu einem Bild, die bspw. GPS-Koordinaten, Gerätebezeichnung, Datum, Uhrzeit, Blende, Belichtungszeit u. ä. m. enthalten können; auch Exif (Exchangeable Image File Format) Daten genannt). Dadurch war es möglich, die Ortsinformationen auszulesen, nachdem das Bild auf den eigenen Rechner heruntergeladen worden war, was das Problem, das damit ursprünglich gelöst werden sollte, nicht zufriedenstellend beseitigte.[13] Das umso mehr, als das *iPhone*, das Bilder automatisch mit Geodaten speichert, das Gerät ist, mit dem die meisten Bilder erstellt werden, die auf *Flickr* veröffentlicht werden.[14]

Warum weiß Flickr wo ich war?

All diesen Diensten bzw. Kombinationen unterschiedlicher Dienste ist gemein, dass hier mehr Daten preisgegeben werden, als den UserInnen eventuell bewusst ist. Während nur ein Foto zur Ansicht für Freunde hochgeladen werden soll, lassen sich aus allen damit verknüpfbaren Daten Bewegungsprofile der Fotografierenden erstellen; mit Hilfe von Gesichtserkennung auch Profile über fotografierte Dritte. Ebenso sind Rückschlüsse auf Lebensgewohnheiten und -umstände möglich.

Teilweise wird durch die Anwendungen auch auf diverse andere Sensoren zurückgegriffen. Im Zusammenhang mit der verbraucherseitigen Nutzung zusätzlicher Sensoren wird auch von „Participatory Sensing“ gesprochen. Es handelt sich dabei um eine Form der technischen Selbstkontrolle bzw. Selbstüberwachung auf Basis einer Smartphone-App, die mit Hilfe diverser Sensoren des Telefons Verhalten und Aktivität eines Individuums (z. B. Schlaf- und Arbeitsrhythmus, Ausmaß und Art der körperlichen Bewegung, Essgewohnheiten etc.) ermittelt und für gesundheitsbezogene Services verarbeitet (vgl. Kang et al. 2012). Dabei können auch Umgebungsdaten wie Temperatur, Luftgüte, Lärmbelastung oder Ozonwerte berücksichtigt werden. Auch die Veränderungen des Magnetfelds (z. B. innerhalb der letzten 50 Sekunden) werden herangezogen (vgl. Hogben und Dekker 2010).[15] Das *Center for Embedded Networked Sensing* der University of California[16] verweist z. B. auf Services wie *cyclesense* um Radwege zu finden, Daten über deren Zustand (Verkehrsaufkommen, Luftgüte etc.) zu sammeln und diese wiederum anderen Radfahrern über eine Plattform zu Verfügung zu stellen. Die App *dietsense* dient zur Analyse und Kontrolle der Nahrungsaufnahme, die App *family dynamics* preist als Funktion an, Familien zu ermöglichen, ihre eigene Dynamik mit Mapping- und Coaching-Software kennenzulernen (vgl. Campbell et al. 2006; Castelluccia 2012; Miluzzo et al. 2008).

Haben Sie gewusst, dass Ihr Telefon Schlaglöcher vermessen kann?

Ähnliche Anwendungen gibt es auch um größere Bevölkerungsströme zu analysieren. In der App *CitySense* nutzt das New Yorker Unternehmen *Sense Networks* personenbezogene Geodaten, um die Frage zu beantworten, “*wo jeder gerade hingeht“*. Citysense zeigt die gesamte Aktivität der Stadt, die aktuellen Hotspots sowie Orte mit unerwartet hoher Aktivität in Echtzeit. Die

---

[13] http://blog.flickr.net/en/2011/08/30/introducing-geofences-on-flickr/ und http://thomashawk.com/2011/08/is-there-a-major-security-hole-in-flickrs-new-geo-fences-feature.html (18.05.2012).

[14] http://www.flickr.com/cameras/ (18.05.2012).

[15] http://metrosense.cs.dartmouth.edu/projects.html (02.06.2012).

[16] http://urban.cens.ucla.edu/projects/ (02.06.2012).

App verlinkt dann auf *Yelp* und *Google* um zu zeigen, welche Veranstaltungsorte sich in der jeweiligen Gegend befinden.

2.2.2 Einzelhandel und Werbung

Wo gibt's die nächste Pizza?

Manche *Location Based Services* offerieren Informationen über nahe gelegene Geschäfte, Restaurants oder den nächsten Taxistand. Derartige Services werden teils auch als *Geotargeted* Advertisements bezeichnet. VerbraucherInnen können sich bevorzugte Geschäfte (sog. Favoriten) speichern, um dann über automatisierte Werbung darauf aufmerksam gemacht werden, wenn sich eine Filiale in der Nähe befindet (Shop Alerts). Auch das Anbieten von Gutscheinen oder das Führen von Smartphone-UserInnen zum nächstgelegenen Bankomaten ist über derartige Services möglich.

Was nutzen Geodaten einem Supermarkt?

Der Einzelhandel kann personenbezogene Geodaten wiederum dazu nutzen, Shopping-Muster zu analysieren, indem Daten über die zurückgelegten Gehwege der KundInnen verarbeitet werden. Ein Beispiel ist die App *Shopkick*, die es Werbetreibenden ermöglicht, die KundInnen ab dem Zeitpunkt des Betretens des Geschäftslokals zu verfolgen. Dies geschieht mittels nicht hörbarer akustischer Signale, die einzelne KundInnen über Smartphones aussenden (vgl. Manyika et al. 2011). Dadurch wird es möglich zu sehen, wo KäuferInnen ihre Gehgeschwindigkeit verlangsamen oder bspw. als Reaktion auf Werbeinformationen den Schritt beschleunigen. Diese Muster können wiederum mit Daten über tatsächlich gekaufte Produkte und Informationen aus Kundenprofilen abgeglichen werden. Derart fein granuliertes Wissen kann bei einer Reihe von unternehmerischen Entscheidungen im Kontext von Werbung und Geschäftsgestaltung hilfreich sein. Verglichen mit traditionellen Werbe- und Marketingmethoden haben personenbezogene geodatenbasierte Kampagnen höhere Relevanz für KonsumentInnen, da sie direkt auf den Moment der Kaufentscheidung ausgerichtet sind. Werbetreibende wissen über diesen Effekt und sind dementsprechend auch bereit, höhere Preise für Services mit Geo-Target-Funktion zu zahlen (vgl. Manyika et al. 2011).

2.2.3 Safety and Security

Geodaten werden auch zur Verbesserung des Notfallmanagements herangezogen. Die steigende Verfügbarkeit personenbezogener Geodaten in Echtzeit bietet für Strafverfolgungsbehörden, Feuerwehr und Rettungsdienste die Möglichkeit, schneller an einer bestimmten Adresse zu sein. Zudem ist angedacht, Hilferufe über personenbezogene Geodaten präzisier verorten zu können (vgl. Manyika et al. 2011).[17] Derartige Services können auch unter Einbeziehung von anderen Privatpersonen in der näheren Umgebung stattfinden. In Notfällen würde die Alarminformation automatisch an die nächstgelegenen Smartphone-NutzerInnen gesendet (vgl. Braun et al. 2011). Im Handel sind verschiedene

[17] Auch bei der Änderung des Sicherheitspolizeigesetzes (SPG) in Österreich im Jahr 2007 wurde vom damaligen Innenminister angeführt, dass man vermisste Bergsteiger nach einem Unfall schneller orten könnte, wenn die Sicherheitskräfte Zugriff auf die Standortdaten hätten
http://www.heise.de/newsticker/meldung/Neues-oesterreichisches-Sicherheitspolizeigesetz-in-der-Kritik-171122.html (22.04.2012),
http://derstandard.at/3141872 (22.04.2012).

Systeme dieser Art erhältlich.[18] So gibt es auch Services, die bei einem Autounfall automatisch eine Notfallmeldung inkl. Standortdaten versenden (meist per SMS). Auf diese Weise werden Einsatzkräfte verständigt, wenn die Insassen nicht (mehr) in der Lage sind, die genaue Position per Telefonanruf durchzugeben. Eine niederländische Initiative verfolgt wiederum den Ansatz eines digitalen Community Policings. Dabei werden Bewohner einer Gegend von den Behörden mittels SMS über sicherheitskritische Ereignisse in ihrem Umfeld informiert (vgl. Korteland und Bekkers 2007). Auch zum Thema Emergency-Management bei Großveranstaltungen (Fußball, Konzerte etc.) unter Bezugnahme auf *Mobile Social Media* wird geforscht. Dabei sollen Besucher einer Großveranstaltung im Falle eines sicherheitskritischen Ereignisses über ihr mobiles Endgerät mit Verhaltensempfehlungen oder Informationen über den besten Fluchtweg informiert werden (vgl. Roßnagel und Zibuschka 2011). Das *Joint Research Center* der europäischen Kommission hat zudem ein sog. *Global Disaster Alert and Coordination System* (GDACS) ins Leben gerufen. Dieses System hat zum Ziel, Informationen über Naturgewalten wie Erdbeben, Wirbelstürme, Vulkaneruptionen oder Überschwemmungen per SMS oder E-Mail zeitnah zur Verfügung zu stellen (vgl. European Communities 2008).[19]

Wie funktioniert ein virtueller Zaun?

Zudem gibt es Applikationen, die es ermöglichen virtuelle räumliche Grenzen zu ziehen. Diese unter dem Begriff *Geofencing* (nicht zu verwechseln mit der unter 2.2.1 erwähnten Funktion „Geofence“ der Fotoplattform Flickr) bekannte Funktion definiert ein geographisch-räumliches Areal mittels virtueller Perimeter im Sinne eines Zaunes. Entfernt sich eine Person mit ihrem Gerät aus einem definierten Umkreis und überschreitet die digitale Begrenzung erfolgt eine Alarmierung, z. B. mittels SMS. Diese Funktion wird u. a. zur Überwachung von Kindern am Schulweg und Spielplatz verkauft. Auch zur Kontrolle und Betreuung älterer oder orientierungsloser Personen wie z. B. Demenzkranker kann Geofencing eingesetzt werden.[20] Für Tiere gibt es ebenfalls entsprechende Produkte. Geofencing ist zudem auch im Handel und der Logistik zu finden. So gibt es Fahrzeuge die nur auf einer bestimmten Strecke oder einem vordefinierten Gebiet fahren dürfen (z. B. Verleih von PKW’s nur im Inland, sicherheitskritische Werttransporte etc.). Auch das Einrichten raum-zeitlicher Checkpoints ist möglich. Weiters können diese Funktionen bei Abrechnungssystemen von Mautgebühren verwendet werden.

Ein weiterer Nutzen wird in der Ortung gestohlener Fahrzeuge gesehen. Da das Fahrzeug nicht erkennen kann, ob der rechtmäßige Besitzer oder jemand anderer hinter dem Steuer sitzt, muss der Eigentümer nach Entdecken des Diebstahls die Firma informieren, die die Ortungsdaten verwaltet. Diese leitet die Daten dann an die Strafverfolgungsbehörden weiter. Dafür ist es jedoch erforderlich, dass das Fahrzeug regelmäßig seinen Standort meldet, auch wenn es noch nicht als gestohlen gemeldet ist, weil ja nicht bekannt ist, wann das Fahrzeug gestohlen wird, und dann der letzte Aufenthaltsort für die Polizei interessant sein kann. Dies insbesondere, wenn die Diebe versuchen, als erstes die GPS-Ortung lahmzulegen. Dadurch wird aber ein komplettes und jeder-

---

[18] Beispielhaft sei hier das Produkt „Satalarm“ der österreichischen Firma Dolphin Technologies angeführt: http://www.dolphin-technologies.com/produkte/gps-ortung/satalarm-metasat-ortung-tracking/33-74.htm (22.04.2012).

[19] http://www.gdacs.org/ (02.06.2012).

[20] https://de.wikipedia.org/wiki/Geofencing (02.06.2012).

zeit abrufbares Bewegungsprofil des Fahrzeugs bei der Firma, die diesen Dienst anbietet, gespeichert.[21]

Was macht die Polizei mit all den Daten?

Ganz allgemein hat der Einsatz von Geodaten und Geografischen Informationssystemen (GIS) in der Kriminalanalyse seit den 1990er Jahren stark an Bedeutung gewonnen. Das österreichische Bundeskriminalamt arbeitet bspw. mit Geodaten, um Personen zu verfolgen oder bestimmte Delikte räumlich darzustellen (vgl. Kampitsch et al. 2008). Die Forschungsschwerpunkte in diesem Feld liegen in der Entwicklung von Analyse- und Modellierungsmethoden zur Identifikation von *Hot Spots* (vgl. Eck et al. 2005) sowie der Untersuchung von Zusammenhängen zwischen Tatorten, sozial-ökonomischen Merkmalen der Bevölkerung und der physischen Struktur einer Stadt (vgl. Lawton und Schulenburg 2007). Gefördert wird diese Entwicklung durch Softwareprodukte wie z. B. *CrimeStat* zur räumlichen Analyse und Modellierung (vgl. Levine 2007).

Was ist ein IMSI-Catcher ...?

Im Kontext von Mobiltelefonie und polizeilicher Nutzung von Ortungsdaten ist auch auf sog. IMSI-Catcher zu verweisen. Strafverfolgungsbehörden und Nachrichtendienste nutzen diese Geräte um Mobiltelefone bzw. Personen über die *International Mobile Subscriber Identity* (IMSI) z. B. für einen polizeilichen Zugriff zu orten und/oder Gespräche abzuhören. Dabei simuliert der IMSI-Catcher eine reguläre Funkzelle eines beliebigen Providers. Mobiltelefone im Einzugsbereich des Catchers loggen sich dann automatisch in die simulierte Basisstation ein, da die Endgeräte dort ein Login versuchen, wo die Sendeleistung am stärksten ist. Vereinfacht wird dieser Angriff dadurch, dass sich Funkzellen gegenüber Telefonen nicht authentifizieren müssen. Gegenüber der echten Basisstation des Netzbetreibers gibt sich der IMSI-Catcher als Mobiltelefon aus und leitet die vom observierten Telefon ausgehenden Datenpakete weiter („Man-in-the-middle"-Angriff). Im Gegensatz zu herkömmlichen Funkzellen, die in ihrem Durchmesser einige Kilometer betragen können, kann auf Grund der geringeren Leistung des IMSI-Catchers und der dadurch reduzierten Ausdehnung der simulierten Funkzelle der Standort eines Mobiltelefons relativ genau bestimmt werden. Von der Herstellerfirma Rhode & Schwarz wird zudem auch technisches Equipment zur Peilung eines Handys über drei Messungen von verschiedenen Standorten angeboten. Die Ortungsfunktion eines IMSI-Catchers setzt in jedem Fall voraus, dass das von der observierten Person genutzte Mobilfunknetz und die IMSI bekannt sind, sich das Mobiltelefon der observierten Person im Stand-by-Betrieb befindet, und der IMSI-Catcher das Mobiltelefon der observierten Person „eingefangen" hat, wozu der Aufenthaltsort der observierten Person auf wenige Kilometer genau bekannt sein muss und je nach Größe und Auslastung der Funkzelle die richtig IMSI aus einer größeren Anzahl herausgefiltert werden muss. Ohne Vorabkenntnis der IMSI des benutzten Mobiltelefons und einer groben Kenntnis des Aufenthaltsortes der gesuchten Person ist eine Ortung mittels IMSI-Catcher daher nicht möglich (vgl. Fox 2002).

... was macht man damit ...?

... und wie erkennt man ihn?

Der Einsatz von IMSI-Catchern kann aber auch Störungen (von einigen Sekunden bis zu 5-10 Minuten) im Netzbetrieb verursachen und im Einzugsgebiet das Empfangen von Gesprächen ebenso wie den Aufbau von Verbindungen blockieren. Dies inkludiert auch Notrufdienste. Zudem postuliert Fox (2002) in seinem Artikel, dass der Aufbau eines UMTS-Netzes eine gegenseitige Authentifizierung der Geräte im Funkverkehr mit sich brächte, und der Einsatz eines IMSI-Catchers, dessen Funktion darauf basiert, sich nicht zu identifizieren, damit erschwert würde.

[21] Die regelmäßige Aufzeichnung der Fahrzeugnutzung kann auch dazu genutzt werden, ein elektronisches Fahrtenbuch zu führen.

Durch die Novellierung des Sicherheitspolizeigesetzes mit 1. Januar 2008 wurde in Österreich die Verwendung des IMSI-Catchers auch ohne richterliche Erlaubnis möglich. Aus der Beantwortung einer Parlamentarischen Anfrage geht hervor, dass innerhalb der ersten vier Monate nach Inkrafttreten der Novelle insgesamt 3.863 Auskunftsbegehren auf Name, Anschrift und Teilnehmernummer eines Anschlusses gem. § 53 Abs. 3a SPG durchgeführt wurden.[22]

Wie werden Geodaten zu Vorratsdaten?

Im Zusammenhang mit der kriminalistischen Verwendung von Smartphone-Geodaten ist zudem darauf hinzuweisen, dass diese auch als Verkehrsdaten im Sinne der Vorratsdatenspeicherung gelten. Bei jeder Kommunikation des Telefons, gleich ob von NutzerInnen direkt gestartet (etwa bei einem Telefonanruf) oder durch die Nutzung von Betriebssystemfunktionen oder Apps ausgelöst, fallen Verkehrsdaten an, die im Sinne der Umsetzung der Richtlinie zur Vorratsdatenspeicherung in den meisten EU-Staaten (seit 1. 4. 2012 unter bestimmten Voraussetzungen auch in Österreich) von den jeweiligen Mobilfunknetzbetreibern mindestens sechs Monate lang zu speichern sind. Dies erlaubt es den Behörden exakte raumzeitliche Profile inkl. soziometrischer Beziehungen von Personen anzulegen.[23]

Darüber hinaus kann es durch das Offenhalten der Verbindung einer App zu „ihrem“ Server dazu kommen, dass mehr Vorratsdaten zu einem bestimmten Gerät/User anfallen (die wiederum die Standortdaten enthalten, die sich aus der Position des Telefons in der Schnittmenge benachbarter Funkzellen ergeben), als es sonst der Fall gewesen wäre, weil nicht nur der periodische Kontakt zwischen Telefon und Netz stattfindet, sondern auch noch die Verkehrsdaten der Datenkommunikation zu einem bestimmten Server mitprotokolliert werden. Das Profil wird dadurch detaillierter.

2.2.4 Verkehr und Logistik

Geodaten und Handlungsreisende

Eine der häufigsten Anwendungen von Geodaten liegt im Bereich Verkehrsmanagement und Logistik. Abgesehen von Vermessungszwecken und Geoinformationssystemen (GIS), war das Fuhrparkmanagement großer Kurierdienste ein früher Einsatzbereich. Mittlerweile sind bestimmte Funktionen in diesem Prozess automatisiert. Verschiedene Algorithmen versuchen die kürzesten bzw. schnellsten Wege zwischen den unterschiedlichen anzufahrenden Punkten zu berechnen (mathematisches „Problem des Handlungsreisenden“ bzw. mit mehreren „Handlungsreisenden“, wenn man eine ganze Flotte betrachtet[24]). Wo sich früher FahrerInnen per Funk nach jeder Zustellung gemeldet haben, wird jetzt automatisch übertragen, wo sich die Fahrzeuge gerade aufhalten, und über zusätzliche Geräte die Statusinformation der einzelnen Sendung erhoben und bei einer Änderung (bspw. Zustellung) übermittelt. Dadurch weiß die zentrale Leitstelle, wann sich welches Auto wo aufhält, und auch welche

---

[22] http://derstandard.at/3391080/Handy--und-Internetueberwachung-Durchschnittlich-32-Anfragen-pro-Tag?sap=2&_pid=9882745 (02.06.2012)

[23] http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten (02.06.2012).

[24] http://de.wikipedia.org/wiki/Problem_des_Handlungsreisenden (22.04.2012).

Sendung sich wo befindet[25]. Die persönliche Freiheit der Angestellten in der Erfüllung ihrer Zustellaufgaben wird dadurch natürlich eingeschränkt.

Je mehr Geodaten mit Verkehrsbezug über Smartphones oder andere Navigationsgeräte generiert werden, desto besser lässt sich der Verkehr ganz allgemein analysieren. Im Jahr 2010 waren etwa 20 Prozent aller Mobiltelefone mit GPS-Funktionen ausgestattet. Manyika et al. (2011) gehen davon aus, dass dieser Anteil bis ins Jahr 2020 auf etwa 70 Prozent steigen wird. Zudem wächst auch die Zahl an Fahrzeugen mit integrierten GPS-Navigationssystemen. In Situationen wie Unfällen, Baustellen und Staus kann auf dieser Basis die Situation in Echtzeit dargestellt werden. Für einzelne Straßen können Frequenz und durchschnittliche Geschwindigkeit ermittelt werden, die z. B. je nach Tagesabschnitt und Uhrzeit variieren (vgl. ARTICLE 29 Data Protection Working Party 2011). In Singapore wird für Bedarfsprognosen im öffentlichen Verkehr bereits seit mehr als zehn Jahren auf personenbezogene Standortdaten zurückgegriffen. Auch niederländische Verkehrsagenturen prognostizieren Verkehrsstaus unter Verwendung personenbezogener Standortdaten von Mobiltelefonen (vgl. Manyika et al. 2011).

Was macht eine Versicherung mit meinen Geodaten?

Die Verwendung personenbezogener Geodaten im Verkehr ist auch für Versicherungen interessant, wenn es darum geht das Fahrverhalten ihrer KlientInnen (Versicherten) genauer zu kontrollieren. Auf dieser Basis wäre es den Versicherungsunternehmen möglich, ihre Preise exakter dem tatsächlichen Risikoverhalten anzupassen, statt auf grobe soziodemographische Indikatoren zurückgreifen zu müssen. Es wird auch gehofft, dass dies in weiterer Folge zu einer Reduktion von Unfällen führt, wenn sich die FahrerInnen über ein derartiges Monitoring bewusst sind. Versicherungen könnten aber auch Informationen über die aktuelle Wetterlage oder unsichere Parkplätze und Tiefgaragen zuspielen. GPS-fähige Handys wären zudem dazu geeignet, die Maut-Abrechnung zu übernehmen. So könnte bspw. das Smartphone Fahrzeug und Mautstelle lokalisieren und die Maut über die Telefonrechnung zahlen, wodurch separate Geräte, Transponder und das zusätzliche Zahlen von Rechnungen wegfielen. Ein anderes Anwendungsbeispiel aus dem Straßenverkehr kommt aus Boston. Dort wurde eine App mit der Bezeichnung *Street Bump* entwickelt, die personenbezogene Geodaten dazu nutzt, Schlaglöcher ausfindig zu machen. Dabei nutzt *Street Bump* die im Smartphone integrierte Sensor-Technologie, GPS-Funktion und Beschleunigungsmesser, um Größe und Ort der Schlaglöcher zu detektieren (vgl. Manyika et al. 2011).

2.2.5 Sonstige Anwendungen

Wie funktioniert Augmented Reality?

Neben den erläuterten Anwendungsbereichen von Smartphone-Geodaten gibt es noch zahlreiche weitere Funktionen und Services. Zum Beispiel arbeitet auch *Augmented Reality* (Erweiterte Realität) oft mit Geodaten. Azuma (1997) definiert Augmented Reality über die folgenden drei Merkmale:

- Die virtuelle Realität und die Realität sind miteinander kombiniert (teilweise überlagert)
- Interaktivität in Echtzeit
- Reale und virtuelle Objekte stehen 3-dimensional zueinander in Bezug.

[25] Viele kleinere Zustelldienste verwenden aus Kostengründen hierfür Mobiltelefone, womit durch die oben beschriebenen Maßnahmen zur Umsetzung der Vorratsdatenspeicherung auch hier der Mobilfunkprovider ein lückenloses Bewegungsprofil der BotenfahrerInnen speichert.

Augmented Reality kann grundsätzlich alle menschlichen Sinnesmodalitäten ansprechen, häufig wird darunter aber die visuelle Darstellung von Informationen verstanden, also die Ergänzung von Bildern oder Videos mit computergenerierten Zusatzinformationen, Einblendung und Überlagerung virtueller Objekte. So kann beim Betrachten der Sehenswürdigkeiten einer Stadt durch das Smartphone eingeblendet werden, um welche Sehenswürdigkeit es sich handelt und diese z. B. um weitere historische Details ergänzen. Augmented Reality kommt in zahlreichen weiteren Apps zu Anwendung. Zur virtuellen Präsentation von Bauprojekten ebenso wie zur Interpretation von Sternbildern am Nachthimmel. Durch die verschiedenen Sensordaten (A-GPS und Kompass) ist für das Gerät erkennbar, in welche Richtung geblickt wird. Durch einen Abgleich mit einer digitalisierten Karte lassen sich die gewünschten Informationen erkennen und einblenden.

Das Telefon weiß, was ich mir gerade ansehe

Eine weitere Anwendung ist das Erkennen von Personen. Das leistet z. B. die App *Recognizr* der Firma TAT (The Astonishing Tribe) aus Schweden, die 2010 von Research in Motion (BlackBerry) gekauft wurde. Wenn eine Person mit der Kamera des Smartphones betrachtet wird, die auf dem Server der Firma Informationen über sich selbst hinterlegt hat, werden diese Informationen allen NutzerInnen der App angezeigt. Zur Gesichtserkennung wird eine Technik der Firma Polar Rose verwendet, die mittlerweile von Apple gekauft wurde. Auch andere große Player in dem Bereich haben Know-How zur Gesichtserkennung zugekauft (Google kaufte *NevenVision*, *Riya* und *PittPat*, Facebook lizenzierte *Face.com*, beide implementierten Gesichtserkennung auf den Seiten ihrer sozialen Netzwerke und Foto-Webseiten). Im Unterschied zum ersten Beispiel wird die Erkennung hier bislang nicht über Geodaten sondern die Gesichtserkennung durchgeführt. Es ist jedoch denkbar, dass in Zukunft nicht klar zuordenbare Personen durch die Information, wo sie sich gerade befinden, eindeutig zu identifizieren sein werden, und bspw. nicht nur die explizit von ihnen freigegebenen Informationen eingeblendet werden, sondern auch Links zu anderen Informationen, die sie im Internet zu irgendeinem Zeitpunkt veröffentlicht haben (z. B. in ihrem facebook-Profil).

Smartphones für Entdecker

Smartphones können auch dazu genutzt werden die Infrastruktur im physischen Nahbereich des Mobiltelefons zu orten und diverse Daten zu sammeln. Im Fall der systematischen Ortung von WLAN Access Points wird dies allgemein (unabhängig von Smartphones) als *war-driving* bezeichnet (vgl. Hogben und Dekker 2010: 31). Ursprünglich waren dabei Personen mit Entdeckertrieb in Autos unterwegs. Der Beifahrer hatte einen Laptop mit einer extra WLAN-Antenne in Betrieb. Beim langsamen Abfahren der Straßenzüge wurden so automatisch die sichtbaren WLANs kartographiert. In weiterer Folge hatten die Geräte auch GPS-Sensoren, um die Verortung genauer vornehmen zu können. In den Anfangszeiten wurden in verschiedenen Städten die gefundenen offenen Netzwerke an Hauswänden mit Kreide angezeichnet; dies wurde als „warchalking“ bezeichnet. Dadurch wurden offene Netzen mit gutem Empfang für andere gekennzeichnet. Durch einen höheren Automatisierungsgrad und immer mehr Daten werden die erstellten Karten heute meist im Internet zur Verfügung gestellt und aktualisiert. Das so gefundene Material wird auch bei der Lokalisierung eines Smartphones mittels A-GPS genutzt. Umgekehrt werden Smartphones oft verwendet, um diese Daten „nebenbei“ zu erheben, wodurch die NutzerInnen unfreiwillig zu „Wardrivern“ werden; Google hat beim Erstellen der Street View Bilder durch die mit Kameras ausgerüsteten Fahrzeuge ebenfalls diese Daten erhoben. Zusätzlich jedoch auch den Netzwerkverkehr der WLANs mitgeschnitten, was für viel Aufregung sorgte (vgl. Lischka und Volkery 2012).

2.3 Profiling and Sorting

Die deskriptive Aufarbeitung der Anwendungsbereiche zeigt eine überaus heterogene Ansammlung an Services und einen inhaltlich-funktionalen Spagat zwischen gesellschaftlichem Nutzen und der Erosion persönlicher Freiheit und privater Lebensgestaltung. Im Bereich der Logistik und Navigation handelt es sich bspw. um Funktionen, die heute kaum jemand missen will. Im Fall des Monitorings von Familienmitgliedern und der Kontrolle von Kindern und älteren Personen handelt es sich jedoch um ethisch sensible Bereiche. Dabei stellen sich pädagogische Fragen über gegenseitiges Vertrauen, und es stellt sich die Frage nach dem gesellschaftlichen Selbstverständnis im Umgang mit sozial benachteiligten Personen und Bevölkerungsgruppen.

Wie kam es dazu?

Die Verwendung von GPS-Daten war anfangs mit einem konkreten Nutzen verbunden. Die Geodaten der Betroffenen wurden nicht zweckfremd ausgewertet, die datenschutzrechtlichen Ansprüche der NutzerInnen waren nicht gefährdet. Es fand lediglich eine Weiterentwicklung und Automatisierung bestehender Aufgaben statt (wie z. B. sich mit Kompass und Karte zurechtzufinden, aufschreiben, wann und wo ein Foto aufgenommen wurde oder Freunden mitteilen, wo man gerade ist).[26] Heute zeigt sich eine wesentlich größere Heterogenität an Verwendungszwecken und ein reger Datenhandel mit Drittanbietern als gängige Praxis. Geodaten sind eine wichtige Variable zur Erstellung von detaillierten Profilen und neuen darauf aufbauenden (App-)Services (vgl. Castelluccia 2012). Während die großen Vorteile verschiedener Anwendungen unbestritten sind, stellen viele auch einen Eingriff in die Privatsphäre (*Location Privacy*) der Betroffenen dar (vgl. Blumberg und Eckersley 2009).

Was lässt sich aus Geodaten erkennen …?

Geodaten eines Smartphones können durchaus sensible personenbezogene Informationen und alltägliche Handlungsroutinen offenlegen (z. B. wann jemand zu Hause ist, oder ob jemand wiederholt ein Krankenhaus oder einer religiöse Einrichtung besucht etc.). Auch eine Kombination scheinbar harmloser Sensordaten (z. B. Magnetfeld und Acceleration bzw. Beschleunigungssensor) könnte dazu verwendet werden, um persönliche Informationen über (Standort-)Umfeld und körperliches Befinden abzuleiten. Je nachdem welche Magnetfeldänderungen in einem bestimmten Zeitraum geortet werden, und mit welcher Häufigkeit bzw. Intensität der Bewegungssensor aktiviert wird, kann bspw. abgeleitet werden, ob eine Person am Arbeitsplatz sitzt, sich zu Hause aufhält oder gerade mit Fahrrad oder Auto unterwegs ist (vgl. Hogben und Dekker 2010).

(Geo-)Daten werden zwar auch von staatlicher Seite gesammelt, wie die Auflistung der diversen Anwendungsbereiche zeigt, jedoch sind es in der überwiegenden Zahl der Fälle privatwirtschaftlich organisierte Unternehmen mit ökonomischen Interessen. Eine wachsende Branche beschäftigt sich damit, Profile von Mobiltelefon-NutzerInnen mit diversen anderen Datensätzen zu verknüpfen. Neben legitimen technischen und ökonomischen Gründen (wie etwa zu Abrechnungszwecken) geht es vor allem um das Sammeln, Aufbereiten, Zusammenführen, Analysieren und Weiterverkaufen zusätzlicher Daten

[26] Dass diese Informationen nun Unternehmen zur Verfügung stehen, die all das ermöglichen, war vorerst eine technikbedingte Konsequenz dieser Entwicklung, weil eine einzelne Person mit ihrem Smartphone das nicht leisten konnte. Diese Funktionalität wäre jedoch jedenfalls heute auch technisch machbar, ohne im Gegenzug zu ermöglichen, dass sehr viele Firmen Profile über Einzelpersonen anlegen können. Ein Umdenken in der Konstruktion der Dienste und Netzwerke wäre dazu ebenso erforderlich wie die Etablierung anderer Geschäftsmodelle, die nicht auf der Verwertbarkeit dieser Daten basieren (Privacy by Design).

für Marketingzwecke. Auf diese Weise werden monetär verwertbare Informationen für Werbeagenturen in Form von Verbraucherkategorien und Kundensegmenten gebildet.

… und welche Werbenetzwerke interessiert das?

Neben den eigentlichen Smartphoneherstellern und den Erhaltern der Infrastruktur werden (Geo-)Daten auch von App-Produzenten selbst gespeichert und/oder an Dritte übermittelt. Als derartige Informationssammler (3rd Party Information Aggregators) lassen sich exemplarisch die folgenden Unternehmen anführen: *AdMarvel, AdWhirl* (ehemals *Adrollo*), *Apple iTunes, Apple Quyattro, AppRupt, Fluent Mobile, Flurry* (ehemals *Pinch Media), Jumptap, Geocade, Google AdMob, Google AdSense, Google Analytics, Google DoubleClick, Microsoft, Millennial Media, Mobclix, Ngmoco, OpenX, Smart AdServer, TapjoyAds* usw. (vgl. Cortesi 2011; Thurm und Kane 2010). Weitere (österreichische und deutsche) Unternehmen, die im Bereich Geo-Marketing und der Verarbeitung von Geodaten aktiv sind, sind bspw. *Acxiom, BGIS, GeoMarketing Datenverarbeitungs & Dienstleistungsgesellschaft* sowie *ProfileAddress, Schober Group* oder *WIGeoGIS*.

Die Analyse und Aufbereitung der Informationen erfolgt im wesentlichen durch quantitativ-statistische Verfahren (z. B. Klassifikation, Korrelation, Regression, Assoziationsanalysen, Cluster Analysen, Data Mining, Dichte- und Trackinganalysen, Mobile Crowdsourcing, Simulation und Visualisierung).

Wie wird gesammelt?

Eines der größten Werbenetzwerke ist das von Google 2010 aufgekaufte *AdMob*, das man neben den beiden großen Plattformen iOS und Android auch auf webOS und Windows Phone 7 findet. AdMob sammelt auch besonders viele Datenkategorien. So erklärt AdMob in seinen Datenschutzbestimmungen, dass auch Geo-Informationen, Telefon-IDs und, wenn vom Netzbetreiber übermittelt, die Telefonnummern erfasst werden. Anwender müssen also damit rechnen, dass Apps, die AdMob verwenden, konkrete personenbezogene Daten übermitteln. Das Unternehmen Mobclix verbindet wiederum Werbetreibende mit App-Produzenten. Es wird die ID von Telefonen erhoben und nach Kriterien wie z. B. welche Apps Personen herunterladen, wie viel Zeit sie mit einer App verbringen, etc. den verschiedenen Interessengruppen zugeordnet. Als Modul zum Tracken der App-Nutzung ist unter den App-Entwicklern Flurry besonders beliebt. Neben allgemeinen Funktionen kann Flurry auch GPS-Daten übermitteln oder über eine Facebook-Connect-Anbindung Informationen wie Alter und Geschlecht auslesen. Außerdem überprüft das Modul, ob der Anwender das Gerät für die Installationen nicht autorisierter Software freigeschalten hat (Jailbreak bei iOS, Root-Zugriff bei Android) oder eine Raubkopie der App einsetzt (vgl. Kolla-ten Venne et al. 2012). Auf Basis der verfolgten Telefon-Standortdaten eruiert bzw. schätzt das Unternehmen Mobclix dann auch den Wohnort einer Person und gleicht diesen wiederum mit anderen zugekauften (demographischen) Daten ab. Innerhalb einer Sekunde kann Mobclix Smartphone-UserInnen einem von 150 Verbraucher-Segmenten für Werber zuordnen, die vom „Grünen Enthusiasten“ bis hin zur „Vorstadt-Mutter“ reichen. So enthält die Kategorie „Die Hard Gamer“ bspw. 15 bis 25-jährige Männer mit mehr als 20 Apps auf ihrem Telefon, die eine App im Schnitt mehr als 20 Minuten am Stück nutzen (vgl. Thurm und Kane 2010). Das Unternehmen Millennial Media unterscheidet wiederum elf Typen von Information über Personen, die Entwickler dann weiterverarbeiten. Diese beinhalten u. a. Variablen wie Alter, Geschlecht, Einkommen, Ethnie, sexuelle Orientierung und politische Einstellung.

Wissen sie meinen Namen?

Darüber hinaus steigt die Zahl an Unternehmen deren Geschäftsmodell darauf basiert Daten zu personalisieren. So betreibt bspw. das US-Unternehmen *RapLeaf* Profiling von EndverbraucherInnen mit deren echten Namen und

handelt mit diesen Daten ohne weitere Zustimmung oder Vergütung der Betroffenen (vgl. Riederer et al. 2011).

Ganz nach dem Motto „Wissen ist Geld“ wird auf diese Weise versucht, möglichst genaue, umfassende und aktuelle personenbezogene Detailinformation zu sammeln, zu verknüpfen und je nach Bedarf nach Mustern zu durchsuchen, um Konsumentengruppen zu identifizieren, zu klassifizieren und nach diversen Kriterien zu selektieren. In der Analyse der Daten geht es z. B. darum Verhalten vorherzusagen, Informationen über die potentiell „besten“ KundInnen und Märkte zu identifizieren und nach räumlichen Strukturen aufzubereiten. Ziel ist es, Werbung gezielt dort abzusetzen, wo sie am ehesten angenommen wird. In diesem Zusammenhang wird auch von *location based direct marketin*g gesprochen.

Worin besteht das Problem maßgeschneiderter Werbung?

Im Gegensatz zu Kundenrabatten nach wiederholtem Konsum, wird es durch diese Form der Klassifizierung auch möglich, Angebote und Preise für verschiedene Kundensegmente selektiv zu errechnen um den Profit zu maximieren. Profiling und die personenbezogene Selektivität von Werbung stellen einen großen Mehrwert für Unternehmen und deren Kundenkommunikation dar. Ab einem gewissen Punkt wird aus dieser Selektivität der Werbung jedoch Kundenmanipulation (vgl. Clarke 1993).

Was ist „Social Sorting“?

Die über die diversen Apps generierten Datensätze werden mit weiteren Informationen angereichert, über die eigentliche Smartphonekommunikation und Werbung hinaus gehandelt und verarbeitet. Die subtilen Prozesse des Datensammelns und Verarbeitens zielen darauf ab, Personen möglichst detailreich in Form von sog. *datadoubles* (vgl. Haggerty und Ericson 2000) nachzubilden und das erstellte Profil marktgerecht einzusetzen. Die Folgen dieser Datenverarbeitungsprozesse treten oft erst viel später ein als die Verletzung selbst und sind für die Betroffenen nicht immer klar erkenntlich, z. B. wenn Bewerbungen abgelehnt oder schlechte Konditionen bei Bank- oder Versicherungsgeschäften geboten werden (vgl. Čas und Peissl 2006). Nach Deleuze (1993) besteht die Sprache postmoderner Kontrolle aus numerischen Chiffren, die den Zugang zu oder den Ausschluss von Informationen (oder Services) kennzeichnen, wodurch es weniger um physische Einschließung als um gesellschaftliche Positionierung geht. Man könnte auch sagen, es geht um die digitale Positionierung in der Klasse eines Datensatzes. Der kanadische Soziologe David Lyon betitelt das daraus entspringende Phänomen plakativ als „Social Sorting“. Gemeint ist damit eine stereotype Kategorisierung und Segmentierung der Bevölkerung. Besonders im Fall einer falschen Interpretation oft inhaltlich facettenreicher Daten und einer nicht gerechtfertigten Lesart des Profils kann dies zu unangenehmen Nachteilen, Verwechslungen, Verdächtigungen und Formen der Diskriminierung führen (vgl. Bowker und Star 2000; Lyon 2003).

3 Technik

Woher weiß mein Telefon, wo ich bin?

Apps auf Smartphones haben unterschiedliche Möglichkeiten Geodaten zu verarbeiten. Abhängig von der gewünschten Funktion und dem Wunsch der Entwickler, Daten unabhängig von der Funktion der App zu sammeln, können die Programme auf die von WLAN, UMTS und GPS-Empfänger produzierten Daten entweder nur dann zugreifen, wenn das Programm läuft und die Datenabfrage zur Erbringung des gewünschten Services nötig ist, oder immer wenn sie vom User gestartet werden, oder permanent, indem ein Modul der App im Hintergrund läuft und die Daten erfasst. Auch das Aufzeichnen der Daten durch Komponenten, die dann bei jedem Start abgefragt werden, ist möglich. Ebenso kann die Verarbeitung (und Übermittlung) der Daten bei Erbringung des Dienstes in regelmäßigen Abständen erfolgen. Da Smartphones in der Regel nicht leistungsfähig genug sind, um jede Funktion der unterschiedlichen Apps lokal zur Verfügung zu stellen, wird oft der Server der Firma kontaktiert, die die App vertreibt. Dort finden die nötigen Berechnungen statt (Daten von anderen Diensten werden abgefragt, kombiniert u. ä.). Danach wird das Ergebnis wieder an das anfragende Telefon übermittelt. So müssen Smartphones selbst meistens nur die Darstellung des Ergebnisses leisten.

Kann man das abdrehen?

Die meisten Smartphones bieten Möglichkeiten zur Steuerung, wie und wann Ortungsdaten übertragen werden. Bei iPhones werden in den Einstellungen auch jene Apps aufgelistet, die auf Geodaten zugreifen oder zugreifen wollen.[27, 28] BenutzerInnen können über diese Funktion den Datenzugriff steuern. Bei Android besteht die Möglichkeit in den Einstellungen zwischen GPS-Ortungsdaten und der Ortung über Funkzellen und WLAN Access Points zu differenzieren. Zudem kann der Datenverkehr im Hintergrund abgestellt werden, wodurch grundsätzlich die Interaktion und Datensynchronisation durch Apps ohne Zustimmung der BenutzerInnen unterbunden wird. Viele UserInnen sind sich dessen aber nicht bewusst, dass Daten übertragen werden, geschweige denn wissen sie von der Funktion, mit der die Privatsphäre-Einstellungen kontrolliert werden können. Zudem gibt es auch Apps, die sich nicht an die individuellen Einstellungen der BenutzerInnen halten. Bei iOS5 können Notrufe die Ortungsdienste auch dann verwenden, wenn diese eigentlich deaktiviert sind, was für NutzerInnen nur in der Support-Datenbank des Herstellers nachzulesen ist. Das Deaktivieren der Ortungsfunktion bietet also grundsätzlich keine Garantie, dass die Ortungsfunktion tatsächlich inaktiv ist. Für KonsumentInnen ist letztlich unklar, mit welchen Daten das Telefon auf Ortungsanfragen durch Dritte reagiert.[29, 30]

---

27 http://support.apple.com/kb/HT1975?viewlocale=de_DE&locale=de_DE (20.05.2012).

28 http://support.apple.com/kb/HT4995?viewlocale=de_DE&locale=de_DE (20.05.2012).

29 http://www.computerbild.de/artikel/cb-Ratgeber-Handy-Sicherheitsrisiko-iPhone-Ortungsdienste-deaktivieren-Geotagging-5401554.html (02.06.2012).

30 Zur teilweisen Anonymisierung kann zurzeit auch auf den Anbieter yesss! zurückgegriffen werden, da dieser Prepaids ohne Registrierung anbietet.

Warum dürfen Apps alles?

Bei der Installation einer App verlangt diese in der Regel den Zugriff auf diverse Daten und Funktionen, den die AnwenderInnen gestatten müssen, damit die App in vollem Umfang eingesetzt werden kann. Eine Verweigerung der Zustimmung zur Datennutzung führt oft dazu, dass die Installation abgebrochen wird, oder die App nicht, oder nur schlecht, mit zahlreichen Abstürzen funktioniert (obwohl sie die Daten oft nicht brauchen würde). Auf diese Art und Weise empfinden NutzerInnen das Verweigern des Zugriffs als Problem und erteilen die Zustimmung regelmäßig, um die App sicher nutzen zu können.

Je nach Betriebssystem gibt es Unterschiede, wie die Apps auf Daten und Funktionen zugreifen. Im Gegensatz zu Android haben am iPhoneApps bspw. von vornherein Zugriff auf das Adressbuch (vgl. Eikenberg 2012). Bei Apple steht jeder installierten App der Zugriff auf die meisten Systemressourcen frei. Apple sagt, iPhone-Apps können Daten nicht ohne Einholung der Zustimmung der BenutzerInnen übertragen. Laut Kolla-ten Venne et al. (2012) senden iPohne Apps deutlich seltener Positionsdaten, die sie nicht benötigen. Viele Anwendungen, die in der Studie des Wall Street Journals (Thurm und Kane 2010) getestet wurden, haben aber den Standort an Werbenetzwerke übertragen, ohne die BenutzerInnen darüber zu informieren (siehe hierzu auch Kapitel 4).

Es gibt Unterschiede, aber keine Gewinner …

Es lässt sich feststellen, dass sich die Betriebssysteme der verschiedenen Anbieter in Bezug auf den Umgang mit Apps und deren Datenhunger unterscheiden. Allerdings ist für KonsumentInnen nicht nur der Rahmen unklar, in dem die Betreiber der verschiedenen Plattformen den Apps gestatten, auf Daten am Telefon zuzugreifen, es ist auch nicht ersichtlich, ob sich die Programme an die Vorgaben halten, bzw. auf technischem Weg dazu gezwungen werden, sich an die von den NutzerInnen bei der Installation gesetzten Vorgaben zu halten. So lassen sich die Unterschiede bspw. in der Art, wie eine Zustimmung eingeholt wird, erkennen, eine aus Datenschutzsicht akzeptable *Best Practice* ist aber – vor allem auf Grund der Intransparenz in diesem Bereich – bei allen Herstellern noch in weiter Ferne.

3.1 Gefahrenpotenzial und Bedrohungsszenarien

Wie hilft das Datenschutzgesetz?

Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit (gem. §14 ff DSG 2000) zu treffen. Dabei ist je nach Art, Umfang und Zweck der Verwendung der Daten, sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit, sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt, und dass die Daten Unbefugten nicht zugänglich sind. Insbesondere ist die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln (gem. §14 Z 5 DSG 2000). Diese Forderungen aus dem DSG stecken einen Rahmen ab, der in der Praxis kaum eingehalten wird, wie sich anhand der folgenden Beispiele veranschaulichen lässt.

Was weiß mein Telefon?

Auf Smartphones werden oft wertvolle Informationen gespeichert – wertvoll sowohl in finanzieller als auch ideeller Hinsicht. Das ergibt sich einerseits aus der ständigen Verfügbarkeit, weil Smartphones in der Regel immer mitgeführt werden, und andererseits auch aus den zahlreichen Funktionen. So werden Adressdaten gespeichert, Erinnerungsfotos angefertigt, und die gesamte Kommunikation protokolliert und über das Telefon festgehalten. Falls es sich

um ein beruflich genutztes Smartphone handelt, finden sich darauf oft auch Firmenmails, für die z. T. besondere Speicherungspflichten gelten, und in diesen Mails Dokumente und Firmendaten, die ebenfalls geheime oder wertvolle, sowie personenbezogene Daten enthalten können. In manchen Fällen ermöglichen die Geräte auch den Zugriff auf das Firmennetzwerk, wodurch im Falle eines Verlustes oder Diebstahls auch von dieser Seite Gefahr für schützenswerte Firmendaten droht (vgl. Hogben und Dekker 2010).

Durch die Erweiterbarkeit des jeweiligen Smartphone-Betriebssystems und die Möglichkeit, Applikationen beliebig selbst zu installieren, sind Smartphones anfällig für Schadsoftware wie Computerviren, Trojaner etc. Von der so installierten Zusatzsoftware geht u. a. die Gefahr aus, dass darin enthaltene Schwachstellen von Angreifern genutzt werden um unberechtigten Zugriff auf Daten zu gewähren (vgl. Heider und Khayari 2012).

Letztlich begünstigen auch App-Stores neue Formen des Phishings, indem Apps mit betrügerischen Funktionen ohne nähere Qualitätskontrolle in den virtuellen Markt eingeschleust werden (vgl. Hogben und Dekker 2010).

Eine weitere Schwachstelle ist die Tatsache, dass auf dem iPhone der Keyboard-Cache für alle Apps zugänglich ist. Der (iPhone) Keyboard-Cache beinhaltet all die Wörter, die jemals über das Keyboard eingegeben wurden (mit der Ausnahme von Passwort-Eingabefeldern). Dies hat den Sinn die automatische Komplettierung bei der Eingabe zu verbessern, letztlich führt dies aber auch zu einer umfangreichen Ansammlung privater Information und vertraulichen Daten (vgl. Hogben und Dekker 2010).

Was passiert, wenn diese Daten in falsche Hände geraten?

Die unbeabsichtigte Preisgabe von Standortdaten kann auch dazu führen, dass Angreifer diese für Stalking, Raub oder bspw. die Entführung von Lastkraftwagen mit wertvoller Fracht missbrauchen (vgl. Hogben und Dekker 2010).

3.2 Informationssicherheit in Unternehmen

Wie gehen Unternehmen damit um?

Die IT-Infrastruktur von Unternehmen ist seit jeher ein beliebtes Angriffsziel für Sabotage und Industriespionage, weil sie, was die Informationen betrifft, sozusagen das Nervensystem einer Firma darstellt. Ein Informationssicherheitsmanagement, das den Wert der Informationen berücksichtigt und daher deren Schutz ermöglichen soll, muss also jede Art von Informationsspeicher berücksichtigen. Das sind einerseits die MitarbeiterInnen selbst, und andererseits die Geräte, auf denen Informationen verarbeitet werden. Der klassische Ansatz war es, Informationssicherheit auf IT-Sicherheit zu beschränken, und dort alle Geräte hinter einer Firewall von außen unerreichbar zu machen. Im Laufe der letzten 20 Jahre musste dieses Konzept aber überdacht werden. Zunächst wurden immer mehr Firmennetze für immer mehr von außerhalb erreichbare Dienste mit dem Internet durch eine zunehmend weniger restriktive Firewall verbunden. Das führte zu mehrstufigen Netzwerksystemen, in den von außen erreichbare Server bspw. in eine so genannte DMZ (Demilitarized Zone) gestellt wurden, wo ein überwinden der Sicherheitsmechanismen noch keine Katastrophe darstellte, weil die unternehmenskritischen Daten in einem weiteren Netzwerksegment verarbeitet wurden, für das zusätzliche Sicherheitsmaßnahmen etabliert wurden.

Mit zunehmend mobileren ArbeitnehmerInnen wurden aus diesem sicheren Bereich immer öfter Geräte hinaus- und wieder hineingetragen (z. B. Notebooks). Damit wurde es nötig, diese ebenfalls gegen all diese Angriffe zu sichern, denen sie außerhalb des Firmennetzwerks ausgesetzt waren, weshalb

bald auf jedem PC eine eigene Firewall eingerichtet wurde, die bspw. Verbindungen nur mit dem Firmennetzwerk zuließ und die Kommunikation dorthin über einen sicheren, d. h. verschlüsselten, Tunnel abwickelte. Weiters musste beim Wiederanschließen im sicheren Bereich des Firmennetzes überprüft werden, ob sich trotz der Sicherheitsmaßnahmen in der Zwischenzeit Schadsoftware auf dem Rechner einrichten konnte – etwa über einen USB-Stick. Daher wurden/werden die Geräte automatisiert überprüft, bevor der Zugriff auf das Netz gewährt wurde.

Mittlerweile sind aber auch die Mobiltelefone, die Firmen ihren Angestellten zur Verfügung stellen, informationsverarbeitende Geräte, die oft mehr Speicher bieten als Desktop-Systeme noch vor einigen Jahren. Somit müssen auch diese gemanaged werden. Dem wird besonders von Herstellern wie Research in Motion (RIM/BlackBerry) Rechnung getragen, die ihre Geräte ursprünglich auf die Nutzung im Unternehmenskontext ausgelegt haben, indem hier bspw. Funktionen zur Fernlöschung angeboten werden, sowie weitere Tools, die das Sicherheitsmanagement erleichtern sollen.

BYOD und Sicherheit

Zusätzlich setzt sich ein Trend fort, der vor einigen Jahren seinen Anfang genommen hat: BYOD – Bring Your Own Device[31]. Seitdem Mobiltelefone immer leistungsfähiger wurden und immer mehr persönliche Informationen über uns speichern konnten, ist die Grenze zwischen privater und Firmennutzung verschwommen. Die wenigsten NutzerInnen verwenden hierfür unterschiedliche Geräte. Unternehmen, die entweder aus Kostengründen, um nicht allen Angestellten ein Telefon zur Verfügung zu stellen, oder um ein einfacheres Arbeiten von unterwegs zu ermöglichen, dieses Konzept verfolgen, sehen sich zunehmend vor dem Problem, diese Geräte nicht kontrollieren zu können.

Selbst wenn es firmeneigene Geräte sind, die zur mobilen Kommunikation und Datenverarbeitung genutzt werden, gehen die wenigsten Unternehmen so weit, dass sie nur die Nutzung freigegebener Apps ermöglichen (was auch nicht auf allen Plattformen möglich ist). D. h., dass auch hier von schlecht oder mutwillig bösartig programmierten Apps eine Gefahr für die Informationssicherheit des Unternehmens ausgeht; und was Geodaten betrifft, eventuell auch für die NutzerInnen der Telefone selbst – entweder weil sie selbst, oder ihre Geräte Informationen bereithalten und/oder den Zugang dazu ermöglichen können.

3.3 Betriebssysteme

Alle aktuellen Betriebssysteme (wie bspw. iOS, Android, Windows Phone, Symbian, BlackBerry BBX …) für Smartphones ermöglichen eine Erweiterung mit Apps, die von den NutzerInnen nach dem Kauf des Telefons installiert werden können. Darin besteht für die meisten Betreiber ein Teil des zugrunde liegenden Geschäftsmodells, weshalb es zuzeit auch nur herstellerspezifische Shops[32] für Apps gibt.

---

[31] http://en.wikipedia.org/wiki/Bring_your_own_device (02.06.2012).

[32] Eigentlich systemspezifisch, weil Google nur ein Betriebssystem, aber keine Hardware herstellt, und für das Google-System Android auch Amazon und Mobiltelefonhersteller, wie bspw. Samsung, Apps vertreiben.

Gibt's Apps bald überall?

Bei immer geringeren Unterschieden in der Hardware zwischen den einzelnen Geräteklassen, zwischen mobil und stationär (Mobiltelefon → Smartphone → Tablet → Netbook → Ultrabook → Notebook → Desktopersatz → Desktop), wird auch versucht, Bedienkonzepte und Betriebssysteme zusammenzuführen. Eine intuitive, herstellertypische Bedienung soll über Gerätegrenzen hinweg erkennbar und für UserInnen erlernbar sein.

Alles eins ...

Das bringt Vorteile für Hersteller, die aus der IT-Produktion kommen, und in den letzten Jahren die etablierten Mobiltelefonhersteller zunehmend vom Markt verdrängten. Bisher haben die Hersteller ihre Systeme auf ein bestimmtes Hardwaresegment, das sich in der Regel durch ähnliche Komponenten auszeichnet, zugeschnitten. So gibt es bspw. Apples iOS nur für die Smartphones und Tablets aus dem eigenen Haus. Für die Notebook- und Desktopgeräte gibt es MacOS. Den Spagat jede Art von Hardware unter einem Betriebssystem vereinen zu können, versucht zuzeit Microsoft. Für Herbst 2012 ist die neue Version des Windows Betriebssystems angekündigt, Microsoft Windows 8, das sowohl auf geeigneten Smartphones, Tablets, Notebooks als auch Desktops laufen soll – natürlich in unterschiedlichen Versionen, jedoch immer mit derselben Basis. Dadurch wird es Software geben, die sowohl auf Windows Phones als auch Windows Desktops läuft. Ein erklärtes Ziel Microsofts ist es, Apps aus dem Windows Phone Marketplace auf allen Windows-Geräten benutzen zu können. Auch ein App-Store für MacOS[33] ist online und stellt den ersten Schritt in Richtung Integration von MacOS und iOS dar. Google hat ebenfalls angekündigt, Android und ChromeOS in Zukunft verschmelzen zu wollen. Diese Entwicklung ist im Zusammenhang mit der Geodaten-Nutzung vor allem insofern beachtenswert, als damit das Verhalten wiedererkennbarer UserInnen über eine App eines Herstellers auf unterschiedlichen Geräten mitverfolgt werden könnte, wodurch es auch kleineren App-Herstellern und nicht nur großen Firmen, wie etwa Google[34], möglich wäre, ein noch ausgeprägteres Kundenprofiling zu betreiben, das die Gewohnheiten der NutzerInnen in verschiedenen Lebensbereichen und verschiedenen Dimensionen über Geräte- und Dienstegrenzen hinweg berücksichtigt.

---

[33] http://www.apple.com/at/macosx/whats-new/app-store.html (14.06.2012).

[34] http://futurezone.at/netzpolitik/7748-googles-datenschutzerklaerung-tritt-in-kraft.php (20.4.2012).

4 Studien und App-Analysen

Was sagt die Statistik?

Im Juni 2010 ließ das Software Security Unternehmen Webroot in Großbritannien und den Vereinigten Staaten einen Online Survey mit insgesamt 1.645 RespondentInnen durchführen. Rund 39 Prozent der Befragten gaben an, auf ihrem Smartphone App-Services mit Geodatenzugriff zu nutzen. Grund für die Nutzung dieser Apps ist für rund 67 Prozent der allgemeine Wunsch geographische Informationen (z. B. zur Navigation) zu erhalten. Weitere 43 Prozent der Befragten gaben an sie nutzen dieses Services um Freunde zu treffen, was auf einen Social Network Dienst verweist. Etwa 27 Prozent der jungen männlichen Erwachsenen (im Alter von 18 bis 29) teilen ihren Standort ihren Freunden täglich mit, und rund 10 Prozent aktualisieren diesen, wenn sie an einem neuen Ort ankommen. Frauen scheinen mehr über die mit Geolocation-Tools verbundenen Risiken nachzudenken. Während nur 32 Prozent der Männer sich besorgt äußerten, gaben rund 49 Prozent der weiblichen Befragten an, dabei Bedenken zu haben, ihren Standort preiszugeben. In der Studie wird zudem davon berichtet, dass ältere Smartphone NutzerInnen (ab 40 aufwärts) mehr über potentielle Risiken nachdenken als die Vergleichsgruppe junger NutzerInnen im Alter von 18 bis 39 Jahren.[35]

Darüber hinaus konnten im Zuge der Recherche drei Analysen, eine des *Wall Street Journals* (vgl. Thurm und Kane 2010)[36], eine Analyse der Zeitschrift *c't* (vgl. Kolla-ten Venne et al. 2012) sowie eine Analyse des Programmierers und Security Consultants Aldo Cortesi (2011)[37] gefunden werden, die sich auf technischer Eben mit der Datenübertragung von Apps auseinandersetzen.[38] Bei den Tests im Zuge dieser Analysen wird die Verbindung des Telefons mit dem Mobilfunkanbieter blockiert, und der gesamte Datenverkehr für die Analyse über eine eigene WLAN-Verbindung umgeleitet. Die Nutzung des Telefons wurde dabei immer auf nur eine App beschränkt, um die Kommunikation ohne etwaige Störeinflüsse in einer isolierten Netzwerkumgebung betrachten zu können. Zum Mitlesen und Entschlüsseln der Daten werden verschiedene sog. *man-in-the-middle* Open-Source-Tools wie *Mallory* oder *mitmproxy* verwendet. (Für nähere technische Ausführung zur Kontrolle des Netzwerkverkehrs von Smartphones siehe Eikenberg 2012).[39]

Das *Wall Street Journal* analysierte im Oktober 2010 jeweils 50 Apps für das iPhone- und das Android-Betriebssystem (sowie die App des Journals selbst), um zu sehen, welche Informationen die Apps im Hintergrund über Telefone, NutzerInnen und Standort an den eigenen Server und außenstehende Dritte für weitere Verarbeitungszwecke versenden. Die Apps wurden aus den „most popular"-Listen auf Apples App Store und Googles Android Market (heute

---

[35] http://www.webroot.com/En_US/pr/threat-research/cons/social-networks-mobile-security-071310.html (15.06.2012).

[36] http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html (15.06.2012).

[37] http://corte.si/posts/security/apple-udid-survey/ (15.06.2012).

[38] http://corte.si/posts/security/apple-udid-survey/ (15.06.2012).

[39] Es sei darauf hingewiesen, dass einige der getesteten Apps ihre Nutzungsbedingungen, Funktionen sowie die Datenschutzrichtlinien ihrer Apps u. a. aufgrund der unerwarteten Aufmerksamkeit durch die Studien nachgebessert bzw. nachträglich geändert haben.

Google Play) gewählt. Für die Analyse wurden die Telefone iPhone 3G und Samsung Captivate herangezogen.

Mehr als die Hälfte der Apps überträgt die Telefon-ID

Die Analyse zeigte, dass 56 der 101 untersuchten SmartphoneApps die eindeutige Geräte-ID des Telefons an andere Unternehmen übertragen, ohne dass BenutzerInnen der Übertragung zugestimmt hätten. Insgesamt 47 Apps übermittelten die Geodaten des Telefons, und weitere fünf übertrugen Informationen wie Alter, Geschlecht und andere persönliche Daten an Dritte.

Als eine der Apps, die besonders viele Informationen übermittelten, wurde auf *textPlus*, eine iPhone-App für Textnachrichten, verwiesen. Diese versendete die eindeutige ID des Telefons an acht Werbeunternehmen und an zwei dieser Unternehmen zudem die Postleitzahl, das Alter und das Geschlecht des Benutzers/der Benutzerin.

Sowohl die Android- als auch die iPhone-Version der Musik-App *Pandora*-übermittelten Alter, Geschlecht sowie Standortdaten und die ID des Telefons an diverse Werbenetzwerke. *Grindr*, eine iPhone-App zum Treffen homosexueller Männer, schickte Geschlecht, Geodaten und Telefon-ID an drei Werbenetzwerke. Sogar im Fall der App *PaperToss*, einem Spiel, bei dem es darum geht, Papierknäuel in einen Mistkübel zu werfen, konnte die Übertragung der Telefon-ID und der Positionsdaten an fünf verschiedene Werbenetzwerke offengelegt werden.

Die folgende Auflistung (Tabelle 4-1) zeigt einen Auszug der datenhungrigsten Apps der WSJ-Studie in alphabetischer Reihung:

Tabelle 4-1: Apps und die Datenweitergabe an Drittfirmen

App	Daten	Drittfirmen
Angry Birds (iPhone) **Kategorie:** Spiel **Typ:** Bezahlt **Hersteller:** Rovio Mobile Ltd.	**Bei iPhone:** Kontakte, Location (Längen und Breitengrad), Telefon ID Benutzernamen und Passwort	**Bei iPhone:** Google Chillingo und Flurry
Best Alarm Clock Free (iPhone) **Kategorie:** Productivity **Typ:** Kostenlos **Hersteller:** MyNewApps Inc.	**Bei iPhone:** Location (Längen- und Breitengrad, Stadt) und Telefon ID	**Bei iPhone:** Geomint, Tapjoy, Open X, Google AdMob, Appredeem, Apple iTunes
Dictionary.com (iPhone, Android) **Kategorie:** Auskunft **Typ:** Kostenlos **Hersteller:** IAC/Interactive Corp.	**Bei iPhone:** Location (Längen- und Breitengrad, Stadt) und Telefon ID **Bei Android:** Telefon ID	**Bei iPhone:** Millenial Media Google DoubleClick Flurry Apple Quattro Apple iTunes AdMarvel **Bei Android:** Google DoubleClick
Grinder (iPhone) **Kategorie:** Social Network **Typ:** Kostenlos **Hersteller:** Grindr	**Bei iPhone:** Alter, Geschlecht, Location (Längen und Breitengrad, Stadt, Postleitzahl) und Telefon ID	**Bei iPhone:** Apple iTunes, Apple Quattro, Flurry, Google Admob, Google DoubleClick, Jumptap, Millennial Media und Mobclix.

App	Daten	Drittfirmen
Groupon (iPhone, Android) **Kategorie:** Lifestyle **Typ:** Kostenlos **Hersteller:** Groupon	**Bei iPhone:** Telefon ID und Benutzernamen und Passwort. **Bei Android:** Location und Telefon ID.	**Bei iPhone:** Facebook, Flurry und Google Analytics **Bei Android:** Fluent Mobile, Flurry und Google Analytics.
Movies by Flixster (Android) **Kategorie:** Entertainment **Typ:** Kostenlos **Hersteller:** Flixster	**Bei Android:** Location (Postleitzahl), Telefon ID, Benutzernamen und Passwort	**Bei Android:** Facebook, Google Analytics, Google DoubleClick und Google AdSense.
Paper Toss (iPhone, Android) **Kategorie:** Spiel **Typ:** Kostenlos **Hersteller:** BackFlip Studios	**Bei iPhone:** Location (Stadt, Längen u. Breitengrad, Postleitzahl) und Telefon ID Bei **Android:** Location (Längen und Breitengrad) und Telefon ID	**Bei iPhone:** Apple iTunes, Apple Quatro, Flurry, Geocade, Google AdMob, Google AdSense, Google DoubleClick. **Bei Android:** AdWhirl, Flurry, Geocade, Google AdMob, Google AdSense und Microsoft.
Pandora (iPhone, Android) **Kategorie:** Musik **Typ:** Kostenlos **Hersteller:** Pandora Media Inc.	**Bei iPhone:** Alter, Geschlecht, Location (Stadt, Postleitzahl) und Telefon ID. **Bei Android:** Alter, Geschlecht, Location (Postleitzahl) und Telefon ID	**Bei iPhone:** Apple Quattro, Google DoubleClick, Medialets, Facebook, Google AdSense, Google Analytics, Weeklyplus, Yahoo. **Bei Android:** AdMarvel, Google DoubleClick, Medialets, Mylife.com.

Text Plus (iPhone) **Kategorie:** Textnachrichten **Typ:** Kostenlos **Hersteller:** GOGII	**Bei iPhone:** Alter, Geschlecht, Location (Postleitzahl) und Telefon ID	**Bei iPhone:** AdMarvel, Apple iTunes, Apple Quattro, Fluent Mobile, Google AdMob, Millennial Media, Ngmoco, OpenX, Tapjoy.
Shazam (iPhone, Android) **Kategorie:** Entertainment **Typ:** Kostenlos **Hersteller:** ShazamInc	**Bei iPhone:** Location (Längen- und Breitengrad, Postleitzahl) und Telefon ID **Bei Android:** Location (Längen- und Breitengrad, Stadt), Telefon ID, Benutzernamen und Passwort	**Bei iPhone:** Mobile Interactive Group, Flurry, Apple Quattro, Apple iTune **BeiAndroid:** Mobile Interactive Group, Google, Goolge DoubleClick, Flurry, Facebook

Auch das Computermagazin *c't*, aus dem Heise-Verlag, hat über 500 iPhone Apps getestet und hinsichtlich unintendierter Datenzugriffe analysiert (vgl. Kolla-ten Venne et al. 2012). Dabei zeigte sich, dass etwa jede fünfte App auf das Adressbuch zugreift. Darunter waren auch Apps (wie *Angry Birds*, *Keynote*, der *DB-Navigator* oder *Runkeeper*), bei denen auf den ersten Blick nicht klar ist, wozu sie diese Daten brauchen. So übertrug *Path*, eine App mit dem Motto „stay connected with family & friends" bis vor kurzem beim Start noch alle Daten des Adressbuchs, einschließlich Mailadressen, Telefonnummern und sogar Postanschriften der gespeicherten Kontakte. Auf Rückfragen zur Zustimmung wurde verzichtet.

Im Zuge der *c't*-Studie wurden auch die Protokolle von 60 Apps der iTunes-Store-Kategorie „Top Gratis-Apps" analysiert. Anwendungen wie *eBay* oder *PayPal*, die als Ergänzung zu Desktop oder Webdiensten dienen, sind meist frei von Zusatzmodulen. Viele andere dieser Gratis Apps kontaktieren jedoch einen oder mehrere Server von Werbenetzwerken. Gerade einfache Apps verwenden oft gleich mehrere Module zur Datenübertragung. So kontaktiert die Taschenlampen-App von *Intellectual Flame* gleich fünf Werbenetzwerke. Neben iPhone-Modell, iOS-Version, Netzbetreibername und MAC-Adresse des WLAN-Chips überträgt die App auch den Jailbreak-Status. Sogar das kostenlose iPhone Tool *Protect My Privacy*, eine App, die verspricht den Datenzugriff der diversen Apps zu kontrollieren, kommuniziert ohne jegliches Nachfragen oder Informieren der AnwenderInnen mit dem eigenen Server und überträgt zusammen mit der eindeutigen ID die jeweiligen Entscheidungsdaten darüber, welche App vom User freigeschaltet oder blockiert ist (vgl. Kolla-ten Venne et al. 2012).

„Protect My Privacy" spioniert die UserInnen aus

Weitere Ergebnisse mit Apple-Bezug liefert der Programmierer und Security Consultant Aldo Cortesi aus Neuseeland.[40] Er analysierte den Datenverkehr

Wer sammelt das Meiste?

[40] http://corte.si/posts/security/apple-udid-survey/appdomains.html (15.06.2012).

von insgesamt 94 iPhoneApps, und fand heraus, dass 84 Prozent der getesteten Apps im Zuge ihrer Nutzung eine oder mehrer Domains kontaktierten. Als Extremfall verweist er auf das Spiel *iDestroy*, das im Zuge der Nutzung mit 14 Domains, davon drei verschiedene Werbenetzwerke, Kontakt aufnimmt. 74 Prozent der getesteten Apps senden die Gerätekennung (UDID) zu einer oder mehreren Domains. 46 Prozent der analysierten Apps, die die UDID übertragen, tun dies unverschlüsselt. Als die drei großen Daten- bzw. UDID Sammler im Hintergrund identifizierte er *Apple*, *Flurry* und *OpenFeint*, die wiederum die UDID mit diversen weiteren Informationen und Datensätzen verknüpfen. Neben diesen drei Großen verweist Cortesi noch auf verschiedene kleinere Werbenetzwerke, Analysefirmen, individuelle Entwicklerseiten und Online-Services wie z. B. :
ads.mp.mydas.mobi, analytics.localytics, api.dropbox, bayobongo, bbc.112.2o7.net, beatwave.collect3, catalog.lexcycle, data.mobclix, init.gc.apple, msh.amazon, notifications.lexcycle, promo.limbic, soma.smaato, chimerasw, phasiclabs, trainyard, twitter, ngpipes.ngmoco, npr.122.2o7.net oder *ws.tapjoyads.*

Eine weitere Studie zum Thema Informations-Flow-Tracking, veröffentlicht im Jahr 2010 auf dem *9th USENIX Symposium on Operating Systems Design and Implementation,* hat herausgefunden, dass von insgesamt 30 Android-Apps zwei die Rufnummer, IMSI und ICC-ID, sieben die Geräte-ID und 15 Apps die Standortdaten an fremde Server und Werbenetzwerke übertragen haben. In keinem Fall wurden die BenutzerInnen nach ihrer Zustimmung gefragt (vgl. Enck et al. 2010; Hogben und Dekker 2010).

In den angeführten Studien und App-Analysen war unter allen getesteten Apps das am häufigsten übertragene Detail die eindeutige ID des Telefons. Als zweithäufigste Datenkategorie werden die verschiedenen Formen von Standortdaten übertragen. Hierzu zählen GPS-Daten aber z. B. auch die Postleitzahl.

Was wird am häufigsten gesammelt?

Der Mitbegründer von Mobclix Inc., Vishal Gurbuxani, spricht bei der Telefon-ID von einer Art „Supercookie“ für den Informationsaustausch unter Werbetreibenden (vgl. Thurm und Kane 2010). Über diese ID (UDID bei Apple, IMEI bei anderen Herstellern) ist es möglich, das Userverhalten zu tracken und verschiedene Datensätze zusammenzuführen (siehe auch Smith 2010). Wie der Programmierer und Security Consultant Aldo Cortesi demonstriert, kann die UDID auch de-anonymisiert und mit den „echten“ Daten (Name, Adresse usw.) der betroffenen Personen verknüpft werden.[41] Zudem gibt es, wie oben bereits erwähnt, Unternehmen wie *RapLeaf*, deren Geschäftsmodell darauf basiert Daten zu personalisieren (vgl. Riederer et al. 2011).[42]

Weiters zeigen die (Sekundär-)Analysen, dass vor allem kostenlose Apps als Datenübermittler fungieren. So kann man z. B. bei allen Diensten, die kostenlosen SMS-Ersatz versprechen, davon ausgehen, dass sie das Telefonbuch der jeweiligen NutzerInnen an den Betreiber senden (vgl. Kolla-ten Venne et al. 2012).

---

[41] http://corte.si//posts/security/openfeint-udid-deanonymization/index.html (15.06.2012).

[42] Wie die rechtlichen Klagen gegen Apple zeigen, sind sich Smartphone-Erzeuger und App-Hersteller durchaus über die datenschutzrechtliche Relevanz im Umgang mit der Telefon-ID im Klaren.
(http://www.infosecurity-magazine.com/view/15643/apple-faces-second-lawsuit-over-udid-disclosure-to-third-parties/ (15.06.2012)).

5 Privacy

Das Recht auf Privatsphäre ergibt sich aus Artikel 12 der Allgemeinen Erklärung der Menschenrechte[43], sowie aus Artikel 8 der Europäischen Menschenrechtskonvention[44], welche in Österreich im Verfassungsrang steht.[45] Darüber hinaus ist das Recht auf Privatsphäre in Form des Datenschutzgesetzes (DSG 2000) spezifiziert.[46]

5.1 Definitionen

Was ist Privatsphäre und wozu braucht man sie?

Zum rechtlichen Schutzbereich des Privaten zählen neben der Verfügung über den eigenen Körper, das Sexualverhalten sowie die körperliche und geistige Befindlichkeit auch private Tätigkeiten, Beziehungen mit engen Bezugspersonen und die persönliche Identität. Auch berufliche Kontakte und Tätigkeiten sind dem Privatleben zuzurechnen (vgl. Berka 1999). In einer Entscheidung des VfGH wird ausgeführt, dass der Schutzbereich des Privatlebens im Sinn des Art. 8 der EMRK auch das Recht umfasst, die Gestaltung des Privatlebens dem Blick der Öffentlichkeit und des Staates zu entziehen. In einer von der Achtung der Freiheit geprägten Gesellschaft, brauchen BürgerInnen niemandem ohne triftigen Grund Einblick gewähren, welchem Zeitvertreib sie nachgehen, welche Bücher sie kaufen, welche Zeitungen sie abonnieren, was sie essen und trinken, und wo sie die Nacht verbringen.[47]

Gem. § 2 Abs. 1 bietet das Datenschutzgesetz rechtliche Kompetenz in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr. Laut DSG hat jedermann ganz allgemein Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten. Damit wird der Schutzbereich der Privatsphäre auf der etwas abstrakteren Ebene der Daten nochmals spezifiziert.

Im Zusammenhang mit Mobiltelefonie gilt festzuhalten, dass die Telefon-ID (IMEI, UDID etc.) nicht lediglich als Kennziffer des Geräts, sondern auch als *personenbezogenes Datum* im Sinne des DSG § 4 Z 1 gesehen werden kann. Nur dann, wenn der Personenbezug der Daten derart ist, dass die Identität des Betroffenen nicht mit rechtlich zulässigen Mitteln bestimmt werden kann, spricht das Datenschutzgesetz von indirekt personenbezogenen Daten.

---

[43] http://www.un.org/depts/german/grunddok/ar217a3.html (15.06.2012).

[44] http://www.echr.coe.int/NR/rdonlyres/F45A65CD-38BE-4FF7-8284-EE6C2BE36FB7/0/GER_CONV.pdf (15.06.2012).

[45] Bundesverfassungsgesetz vom 4. März 1964, mit dem Bestimmungen des Bundes-Verfassungsgesetzes in der Fassung von 1929 über Staatsverträge abgeändert und ergänzt werden, Art. 2 Zi. 7.

[46] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), § 1 Abs. 1, ebenfalls im Verfassungsrang.

[47] Vgl. VfGH 14.03.1991, VfSlg 12689.

Smartphones speichern sensible personenbezogene Daten

Zudem ist auf die Kategorie der *sensiblen Daten* im Sinne des § 4 Z 2 hinzuweisen. Als sensible Daten gelten per Definition alle Daten über Personen, die Rückschlüsse auf ihre rassische oder ethnische Herkunft, ihre politische Meinung, ihre Gewerkschaftszugehörigkeit, ihre religiöse oder philosophische Überzeugung, ihre Gesundheit oder ihr Sexualleben zulassen. Bei der raumzeitlichen Verfolgung von Geodaten und der Rekonstruktion von Handlungen über Mobiltelefone (Tracking) kann daher ebenfalls von sensiblen Daten gesprochen werden, weil damit erfasst wird, wenn z. B. wiederholt ein Krankenhaus, eine Arztpraxis oder eine religiöse Einrichtung besucht wird. Auch die Teilnahme an politischen Demonstrationen kann getracked werden. Zudem kommen persönliche Beziehungen und Rückschlüsse auf das Sexualleben. Geodaten (Ortungsdaten) von Mobiltelefonen sind daher jedenfalls als sensible Daten zu behandeln.[48] Das Erstellen von Profilen auf Basis von Geodaten kann Wissen generieren, das je nach Handhabe tief in das Leben der Betroffenen eingreift.

5.2 Rechtliche Prinzipien

Nach § 1 Abs 3 DSG hat jedermann, soweit ihn betreffende personenbezogene Daten verarbeitet werden, das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet und insbesondere auch, an wen sie übermittelt werden. Zudem hat jedermann das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

Das Prinzip der Zweckbindung und Datensparsamkeit gem. § 6 Abs 1 Z 2 besagt weiters, dass Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden dürfen (siehe *function creep*). Auch die Datenschutzvereinigung Düsseldorfer Kreis (2011) mahnt im Zusammenhang mit Smartphones zur Einhaltung des Grundsatzes der Datensparsamkeit. Zudem müssen Zweck und Inhalt der Datenanwendung gem. § 7 (1) DSG von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sein.

Kein Computer sollte über mich entscheiden, sondern ein Mensch

Im Zusammenhang mit Profiling und Phänomenen wie *Social Sorting* auf Basis digitaler personenbezogener Daten ist zudem auf das Verbot automatisierter Einzelentscheidungen gem. § 49 DSG zu verweisen. Demnach darf niemand einer für ihn rechtliche Folgen nach sich ziehenden oder einer ihn erheblich beeinträchtigenden Entscheidung unterworfen werden, die ausschließlich auf Grund einer automationsunterstützten Verarbeitung von Daten zum Zweck der Bewertung einzelner Aspekte seiner Person ergeht, wie beispielsweise seiner beruflichen Leistungsfähigkeit, seiner Kreditwürdigkeit, seiner Zuverlässigkeit oder seines Verhaltens.

Ein weiteres datenschutzrechtliches Prinzip ist jenes, über die bewusste Zustimmung der Betroffenen zur Verwendung der Daten. Diese sog. informierte Zustimmung soll im Folgenden etwas eingehender diskutiert werden.

[48] Vgl. WP185, Opinion 13/2011 on Geolocation services on smart mobile devices.

5.2.1 Freiwilligkeit der Zustimmung

Die schutzwürdigen Geheimhaltungsinteressen einer betroffenen Person werden laut § 9 DSG nicht verletzt, wenn der/die Betroffene die Daten offenkundig selbst öffentlich gemacht hat, oder die Daten in nur indirekt personenbezogener Form verwendet werden.

Zudem liegt kein grundrechtlicher Eingriff vor, wenn der/die Betroffene zur Verwendung der Daten seine/ihre ausdrückliche Zustimmung erteilt hat. Ein Widerruf der Zustimmung, der die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, ist rechtlich jederzeit möglich.

In der aktuellen Fassung des Datenschutzgesetzes ist diese Zustimmung (informed consent) nach §4 Z14 definiert als *„gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt."*

Wann ist man informiert genug, um zustimmen zu können?

Eine wichtige Rolle spielt die informierte Zustimmung bspw. im medizinischen Kontext, wo PatientInnen über die Folgen und Risken eines Eingriffs aufgeklärt werden, und ihre Zustimmung dazu geben müssen. David Finkelhor etablierte den Begriff ursprünglich in der Debatte um sexuellen Missbrauch Minderjähriger. Grundsätzlich gilt, dass sowohl Kinder und Jugendliche, aber auch Erwachsene, zustimmen können, sich deshalb aber der Tragweite der Entscheidung dennoch nicht bewusst sein müssen.[49] Dies gilt auch für KonsumentInnen von Smartphone-Apps, die nicht immer über die Tragweite der Zustimmung und die weitere Verwendung ihrer Daten informiert sein können.

Als Beispiel für datenschutzrechtlich problematische Smartphone-Anwendungen verweist die ARTICLE 29 Data Protection Working Party (2011) auf Geolocation-basierte Services, die für Eltern als Supervisionswerkzeug zur Kontrolle ihrer Kinder dienen (siehe *Geofencing*). In der Stellungnahme 2/2009 über den Schutz personenbezogener Daten von Kindern hielt die ARTICLE 29 Data Protection Working Party (2011) daher fest: „*It should never be the case that, for reasons of security, children are confronted with over-surveillance that would reduce their autonomy. In this context, a balance has to be found between the protection of the intimacy and privacy of children and their security.*[50] Die Rechtslage sieht vor, dass Eltern für den Schutz der Privatsphäre ihrer Kinder verantwortlich sind, ebenso wie für deren Sicherheit. Wenn Eltern zu dem Entschluss kommen, dass die Anwendung einer derartigen App für eine bestimmte Situation notwendig ist, so sind die Kinder darüber zu informieren und so bald wie möglich in den Entscheidungsprozess über die Anwendung der App einzubeziehen.

Kann man sich der Datensammlung im Arbeitsalltag entziehen?

Ein Fall fragwürdiger Zustimmung zur Verwendung personenbezogener Daten findet sich bei der geschäftlichen Nutzung von Mobiltelefonen durch Angestellte. Die Zustimmung kann in diesem Kontext möglicherweise unter Befangenheit und sozialem Druck erfolgen. Die ARTICLE 29 Data Protection Working Party (2011) hält hierzu fest: „*If it is not possible for the worker to refuse it is not consent. (…) An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent, but*

---

[49] http://de.wikipedia.org/wiki/Informed_consent#Informed_consent_in_der_Debatte_um_den_sexuellen_Missbrauch (20.4.2012).

[50] WP160, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools).

the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid. "[51]

Die Komplexität der rechtlichen Grundlagen für die Verarbeitung von Geodaten bzw. die Probleme der Wirksamkeit einer informierten Zustimmung zeigen sich deutlich am Beispiel der Nutzung der Navigationsgeräte und Zusatzdienste der niederländischen Firma TomTom. In der Regel wird bei standalone-Navigationsgeräten, wo die Dienstleistung der Navigation von einem eigenen Gerät erbracht wird, und nicht von Software auf einem Smartphone, der aktuelle Aufenthaltsort nicht an einen Diensteanbieter übertragen, da die Ortung ausschließlich auf GPS-Signalen beruht, die Routenberechnung findet lokal am Navigationsgerät mit den darauf gespeicherten Kartendaten statt. Hersteller solcher Geräte bieten jedoch Zusatzdienste an, die einerseits erfordern, dass eine Datenverbindung zum Hersteller/Diensteanbieter aufgebaut werden kann, und es andererseits mit sich bringen, dass Nutzungs- und Positionsdaten des Gerätebesitzers an das Unternehmen übermittelt werden. Einer dieser Zusatzdienste ist lt. Hersteller bspw. die Übermittlung von Stauinformationen.

TomTom-Daten für die Polizei

Die daraus gewonnenen Nutzungsdaten hat die Firma TomTom 2011, als Einbußen im finanziellen Ergebnis des Unternehmens erwartet wurden, an die niederländische Regierung verkauft. Diese hat die Daten über das Fahrverhalten der TomTom-NutzerInnen an die Polizei weitergegeben, die daraus erkennen wollte, wo es am lohnendsten wäre, Radargeräte zur Geschwindigkeitsmessung aufzustellen.[52]

Obwohl der Datenverwendung durch das Unternehmen generell zugestimmt werden muss, bevor man diese Zusatzdienste nutzen kann, weshalb sich das Unternehmen anfangs auch keiner Schuld bewusst schien, führten empörte Reaktionen zahlreicher NutzerInnen dazu, dass der Chef der Firma sich letztendlich bei den KundInnen entschuldigte und eingestand, hier einen Fehler gemacht zu haben.

Aus der Empörung lässt sich jedoch auch schließen, dass die BesitzerInnen der Navigationsgeräte eben nicht das Gefühl hatten, genau dieser Verwendung ihrer Daten zugestimmt zu haben. Insofern lässt sich hier beispielhaft erkennen, dass nicht jeder vermeintliche Akt der Zustimmung, durch oftmals vielleicht allzu schnelles Weiterklicken am Bildschirm eines (Geodaten verarbeitenden) Geräts die Anforderungen an eine Zustimmung i. S. des „informed consent" erfüllt, und es erhebt sich die Frage, ob es sich die datenverarbeitenden und -nutzenden Unternehmen hier nicht zu leicht machen.

Ein großes Ungleichgewicht zwischen KonsumentInnen und Anbietern

Auch wenn es sich nicht um Unmündige oder Befangene handelt, haben voll geschäftsfähige KundInnen oft zu wenig Fachkenntnis und Transparenz darüber, wie die Daten in weiterer Folge verwendet werden, wo sie gespeichert werden, wer darauf Zugriff hat, und auf welche Art und Weise damit Geld gemacht werden kann. Die VerbraucherInnen sind darauf angewiesen, Informationen von den beteiligten Unternehmen zu erhalten und befinden sich daher in einem Abhängigkeitsverhältnis. Obendrein kann nicht erwartet werden, dass sich jeder einzelne Konsument und jede einzelne Konsumentin technisch und juridisch damit befassen, wie Apps funktionieren, und welche Daten sie verarbeiten und übermitteln. Diese strukturelle Unterlegenheit des/der einzelnen ist in vielen Bereichen Ausgangspunkt für Regelungen zum Konsumentenschutz. So müsste auch in diesem Geschäftsfeld regulatorisch und durch

---

[51] WP48, Opinion 8/2001 on the processing of personal data in the employment context.

[52] http://news.orf.at/stories/2055504/ (22.04.2012).

Aufklärungsarbeit sichergestellt werden, dass Unternehmen die KonsumentInnen nicht übervorteilen können.

Zusätzlich stehen KonsumentInnen vor der Entscheidung, zwischen der Einhaltung abstrakter datenschutzrechtlicher Konstruktionen und dem schnellen Komfortgewinn durch die App. Auch die spürbare Ausgrenzung im näheren sozialen Umfeld (wenn man auf bestimmten Kommunikationskanälen nicht erreichbar ist oder bei bestimmten Kommunikationsformen nicht mitmacht) spielt eine wichtige Rolle. Kommunikation über Mobiltelefone wird bei jungen Menschen immer häufiger dazu benutzt, ein Zusammengehörigkeitsgefühl zu vermitteln und immer weniger dazu, inhaltliche Informationen auszutauschen. Ausgrenzung kann gerade im jugendlichen Alter eine Motivation darstellen, den Preis in Form der Herausgabe personenbezogener Daten zu bezahlen, besonders dann, wenn die Konsequenzen dieses Handelns nicht gut abgeschätzt werden können.

5.2.2 Informationelle Selbstbestimmung

Kann ich kontrollieren, wer was mit meinen Daten macht?

Die Diskussion um die Zustimmung hängt auch mit dem Begriff der informationellen Selbstbestimmung zusammen. Der Verlust informationeller Selbstbestimmung meint den Verlust der Kontrolle über Informationen die eigene Person betreffend, bzw. den Verlust der Kontrolle über die eigene Selbstdarstellung (vgl. Rössler 2001). Im Kontext digitaler Kommunikation haben Betroffene immer weniger Kontrolle über die eigenen Informationen, wodurch die Möglichkeit einer Zustimmung oft gar nicht gegeben ist. Die NutzerInnen müssten eigentlich in der Lage sein, die diversen Datenübermittlungen nachvollziehen zu können. Sie müssten für eine Beurteilung der Zulässigkeit einer Datenverarbeitung auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden (vgl. Düsseldorfer Kreis 2011). Die Entkoppelung der personenbezogenen Daten von den betroffenen Individuen ist Merkmal einer Neukonstituierung und Abstraktion gesellschaftlicher Abläufe auf einer digitalen Metaebene. Die Informationsgesellschaft ist schlicht über die zunehmende Relevanz diverser Daten und deren Verarbeitung definiert. Die Datenmenge, der Umgang mit den Daten und die Dynamik des Marktes führen dazu, dass betroffene Personen keine Kontrolle mehr über die diversen Angaben und Informationen zur eigenen Person haben: „*The ratio of what individuals know about themselves (or are capable of knowing) versus what outsiders and experts can know about them has shifted away from the individual."* (Marx 1998: 172). Diese Entkoppelung der Betroffenen von ihren eigenen Daten und die digitale Konstituierung sog. *Data Doubles* (vgl. Haggerty und Ericson 2000) in den Händen von Drittfirmen wird von Beate Rössler (2001) aufgrund der folgenden drei Prozesse als ethisch bedenklich gesehen:

- Daten werden gegen den eigenen Willen weitergegeben.
- Daten werden ohne das eigene Wissen (an unbestimmte bzw. unbekannte Dritte) weitergegeben.
- Betroffene Personen werden systematisch darüber getäuscht, welche Daten in welchem Ausmaß/Umfang und an wen weitergebenen werden.

In diesem Sinne ist die Verbreitung digitaler Informations- und Kommunikationstechnologie insofern diskussionswürdig, weil Personen in vielen Fällen gegen ihren Willen gewissermaßen „entprivatisiert" werden (vgl. Rössler 2001). Zudem sind die betroffenen Personen aber auch immer mehr dazu bereit, die Dimensionen ihrer Privatsphäre um anderer Güter willen zu reduzieren. Datenmissbrauch und unangemessene De-Anonymisierung in diesem Kontext zu diskutieren ist schwierig, da viele Betroffene zunehmend geneigt sind, je nach

Kosten-Nutzen Verhältnis ihre Privatheit im Sinne eines empfundenen Trade-Offs zwischen Privatsphäre und Komfort von sich aus zu verhandeln, zu „verkaufen“ bzw. aufzugeben. Es scheint, als würde man sich gerade bei computergestützten Dienstleistungen daran gewöhnen, bestimmte Formen der Privatheit nicht mehr für gesichert aber auch nicht mehr für wichtig anzusehen (vgl. Rössler 2001; Tichy und Peissl 2001).

Wann wird das Sammeln zum Problem?

Auch auf der Herstellerseite muss Datensammeln grundsätzlich nicht mit böswilligen Motiven verbunden sein, sondern entsteht vielmehr aus dem Interesse an Rationalisierung, Effizienz und letztlich ökonomischer Profitorientierung. Problematisch wird diese Form der Sammlung personenbezogener Daten insbesondere dann, wenn die Motivation der Verwendung von ökonomischer Effizienz in Kontrolle und Macht umschlägt (vgl. Rössler 2001). Gefährdungen entstehen auch dort, wo das Sammeln und Verarbeiten personenbezogener Daten zu Klassifikationen von Personen und im weiteren zu Formen der Diskriminierung führen wie dies bereits unter dem Begriff des *Social Sorting* diskutiert wurde.

Derartige Entwicklungen könnten sich auch auf den Freiheitsbegriff und das demokratische Selbstverständnis der Gesellschaft auswirken. Wer nicht mehr weiß oder beeinflussen kann, welche Informationen über die eigene Person und das eigene Verhalten gespeichert und vorrätig gehalten werden, wird sein Verhalten aus Gründen der Vorsicht mehr oder weniger anpassen. Nicht nur die individuelle Handlungsfreiheit sondern auch das Gemeinwohl einer freien demokratischen Gesellschaft, die letztlich auf der selbstbestimmten Mitwirkung der Bevölkerung aufbaut, wird davon beeinflusst. Die Bedingungen moderner Datenverarbeitung wirken sich letztlich auf die Entfaltung einer selbstbestimmten Persönlichkeit aus (vgl. Peissl 2003; vgl. Rössler 2001).[53]

5.3 Privatsphären-freundliche Geräte

Was am Smartphone-Markt zurzeit fehlt, ist ein explizit Privatsphären-freundliches Gerät. Gängige Funktionen des Selbstdatenschutzes und *DoNotTrack*-Funktionen müssen gefördert und standardisiert zu Verfügung gestellt werden, nicht zuletzt deshalb, weil die ökonomische Nutzung der (Geo)Daten oft die Basis der in diesem Markt agierenden Unternehmen darstellt.

Fehlende Einflussmöglichkeiten für NutzerInnen

Bedrohungen ergeben sich natürlich nicht nur durch die Nutzung der Ortsdaten, sondern auch durch Auslesen der Kontaktdaten, die Möglichkeit Spyware am Gerät zu installieren, das Speichern von Daten in fremdkontrollierten Speicher- und Verarbeitungsnetzen (Clouds) u. v. m. Generell geht es um das Unterbinden der Möglichkeiten zur Überwachung eines höchst persönlichen Geräts, das die AnwenderInnen i. d. R. immer in unmittelbarer Reichweite bei sich haben, das fast immer eingeschaltet ist und zudem als zentraler Hub (sensibler) personenbezogener Daten fungiert.

Smartphones sind oftmals darauf reduziert, Apps lediglich pauschal, während der Installation der Anwendung, den Datenzugriff zu verbieten. Den Nutze-

[53] Siehe auch: Volkszählungsurteil des deutschen Bundesverfassungsgerichts vom 15. Dezember 1983 als Herleitung der informationellen Selbstbestimmung aus dem deutschen Grundgesetz, das die Unantastbarkeit der Menschenwürde und die freie Entfaltung der Persönlichkeit garantiert, womit auch ein Übertritt des Begriffs der informationellen Selbstbestimmung aus der Rechtssprechung in den wissenschaftlichen Diskurs und die gesellschaftliche Diskussion einsetzte.

rInnen müssen Möglichkeiten gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden, und an wen sie übermittelt werden. Es fehlt die Einflussmöglichkeit, Datenspuren zu vermeiden, zu reduzieren und ggf. zu löschen. Zudem sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen (vgl. Düsseldorfer Kreis 2011).

Was kann man tun?

Diese Überlegungen waren vermutlich auch für den US-Nachrichtendienst NSA (National Security Agency) ausschlaggebend für die Entwicklung einer eigenen Android-Version. Die Sicherheitserweiterung des Android-Betriebssystems soll nun einen Einsatz des Gerätes ohne Abhören ermöglichen.[54] Zurzeit füllt die NSA damit ihre eigene Nische am Markt, vielleicht kann das Beispiel aber als Vorbild für weitere Entwicklungen im Consumer-Bereich dienen.

Um Risiken von Malware zu reduzieren haben einige Smartphone-Betriebssysteme eine Funktion integriert, die es möglich macht, unerwünschte Software extern vom Mobiltelefon zu entfernen. Diese Funktionalität wird manchmal auch als *Remote-Kill-Switch* bezeichnet (vgl. Hogben und Dekker 2010). Eine andere Möglichkeit bietet die Android-App *aSpotCat* die installierte Apps nach den erteilten Rechten sortiert und so Überblick und Kontrolle fördert. Mac-NutzerInnen können sich z. B. von dem kostenlosen Tool *AdiOS* anzeigen lassen, welche der von iTunes gespeicherten iPhone-Apps Aufrufe von API-Funktionen wie ABAdressBookCopyArrayOfAllPeople enthalten, um auf das Adressbuch zuzugreifen (vgl. Eikenberg 2012).

5.4 Gütesiegel und Vertrauen

Wie erhält man Vertrauen?

Wenn sich der Privacy-by-Design-Ansatz in der App-Entwicklung nicht durchsetzen kann, bedarf es entweder anderer Geschäftsmodelle, die nicht darauf abzielen, durch das Verwerten der User-Daten einen finanziellen Vorteil für das Unternehmen zu erwirtschaften, oder regulativer Vorgaben, um einen verbesserten Schutz der Privatsphäre zu erreichen. Ob es nun eine gesetzliche Forderung ist, oder ein alternatives Geschäftsmodell, das Beispiel des Europäischen Datenschutzgütesiegels (EuroPriSe – European Privacy Seal)[55] zeigt, dass der Schutz der Privatsphäre der KundInnen auch einen finanziellen Nutzen für ein Unternehmen mit sich bringen kann. So wäre es in einem ersten Schritt denkbar, dass Firmen, die Apps programmieren, diese einer derartigen Prüfung unterziehen, um die danach zertifizierte, somit wertvollere App zu einem höheren Preis verkaufen zu können, der wiederum die Zertifizierungskosten abdeckt. Obendrein könnte so eine Zertifizierung etwaigen strengeren Ausschreibungskriterien genügen, z. B. wenn es darum geht, bestimmte Funktionen in staatlichen Einrichtungen und dem öffentlichen Dienst nutzen zu wollen.

Zudem existieren bereits erste Reputations-Systeme zur Beurteilung einzelner Apps. *Web Of Trust (WOT)* und *WhatApp* sind Beispiele von Seiten, die

---

[54] http://futurezone.at/produkte/6912-nsa-verbessert-sicherheit-bei-android.php (22.04.2012).

[55] https://www.european-privacy-seal.eu/ (15.06.2012).

Ratings von Apps nach verschiedenen Aspekten anbieten. Derartige Services sollten weiter ausgebaut und für die sicherheitstechnische Beurteilung von Privatsphäre und Datenschutzaspekten professionalisiert werden (vgl. Wetherall et al. 2011).

6 Schlussfolgerungen

Da Smartphones und Tablet-Computer aufgrund ihrer Mobilität unmittelbar mit ihren BesitzerInnen verbunden sind, bieten die Bewegungsmuster der Geräte einen sehr intimen Einblick in das Privatleben der EigentümerInnen. Über diese Geräte generierte Geodaten sind personenbezogene Daten, die es erlauben, sensible Inhalte zu rekonstruieren. Mit der Hilfe von Geodaten, wie GPS-Koordinaten oder WLAN Access Points, können mobile Endgeräte von verschiedenen Akteuren getracked werden. Die Zwecke reichen von Logistik und Verkehrsmanagement über Direct Marketing bis zur Kontrolle der Kinder auf dem Schulweg. Dabei wird in vielen Fällen das Grundrecht auf Privatsphäre und Datenschutz zum Zweck des Profits missachtet. Möglichkeiten der informationellen Selbstbestimmung sind oft nicht gegeben. Ein großes Risiko besteht vor allem auch darin, dass sich die Betroffenen dessen nicht bewusst sind, dass ihre (Positions-)Daten an Dritte übermittelt werden. Ein weiteres Problem besteht in der ungültigen Zustimmung, wenn Informationen über die Verarbeitung der Daten nicht oder nur unvollständig offengelegt werden (vgl. ARTICLE 29 Data Protection Working Party 2011). Betroffene sollten Kontrolle über ihre personenbezogenen Daten haben und entscheiden können, was veröffentlicht wird, und was nicht. Die Information sollte vollständig, klar und für ein breites, nicht technisch versiertes Publikum leicht verständlich und dauerhaft zugänglich gemacht werden (vgl. ARTICLE 29 Data Protection Working Party 2011).

In einer kapitalistischen Gesellschaft sollte grundsätzlich alles, was gratis angeboten wird, bei den KonsumentInnen ein gewisses Maß an Skepsis hervorrufen. Generell muss man feststellen, dass fast alle Geräte, in die ein GPS-Sensor passt, auch ohne dass dazu eine Notwendigkeit besteht, geortet werden (können), weil es jemand gibt, der hofft, mit diesen Daten Geld zu verdienen.

Betroffenen wird zum Teil empfohlen, ihre Erwartung hinsichtlich der Geheimhaltung personenbezogener Daten im Zuge der Smartphone-Kommunikation zu senken (vgl. Castelluccia 2012). Mitunter wird auch die Meinung vertreten, dass die Abstinenz bzw. der Rückzug aus der Online-Welt die einzige Methode sei, die wirklich noch Datenschutz garantiert (vgl. Conti 2009). Das ist jedoch ein Luxus, den sich viele heute nicht mehr leisten können, wo bspw. in verschiedenen beruflichen Umfeldern erwartet wird, jederzeit erreichbar und in Sozialen Netzen vertreten zu sein. Der Erhalt der eigenen Privatsphäre wird so immer mehr zu einer Art Privileg und elitärem Gut. Gerade auch im Hinblick auf die steigende Marktrelevanz von Geodaten wäre eine klare rechtliche Regelung, die auch durchgesetzt wird, für alle Beteiligten wünschenswert.

Dies scheitert oft schon an der fehlenden Transparenz der Datenverarbeitungsprozesse. Wenn Anbieter von Geolocation-Apps den Standort eines Geräts mehr als einmal berechnen, so haben sie ihre KundInnen darüber zu informieren wie lange bzw. wie oft Standortdaten verarbeitet werden. Sie müssen ihren KundInnen außerdem ermöglichen, ihre Zustimmung zu widerrufen. Um dies zu erreichen, sollten die Anbieter von Anwendungen enger mit den EntwicklerInnen des Betriebssystems kooperieren. Die EntwicklerInnen sind technisch in der besten Position, eine permanent sichtbare Funktion zu integrieren, die darüber informiert, dass Standortdaten verarbeitet werden. Die EntwicklerInnen sind auch in der besten Position, zu kontrollieren, dass keine Anwendungen am Smartphone in Verwendung sein können, die heimlich den Aufenthaltsort mobiler Geräte mitverfolgen. Die verschiedenen App-Anbieter und

Datensammler müssen sicherstellen, dass BesitzerInnen eines mobilen Endgeräts ausreichend über die wichtigsten Elemente der laufenden Datenverarbeitung informiert sind. Dazu zählen bspw. der Zweck der Datenverarbeitung, die Dauer, der Umfang und Typ der verwendeten Daten, sowie die Möglichkeit für die Betroffenen, ihre Rechte auf Auskunft, Richtigstellung und Löschung ihrer Daten geltend zu machen. Wetherall et al. (2011) argumentieren, dass der Umgang mit und die bewusste Verwaltung der Datenschutzstandards bei den NutzerInnen steigen würden, wenn das Betriebssystem eine Übersicht darüber böte, welche Apps persönliche Daten in welchem Umfang verarbeiten und weitergeben. Die Form der Bereitstellung dieser Informationen sollte auf ein breites Publikum ausgerichtet sein. Hersteller und Datensammler dürfen nicht davon ausgehen, dass ihre KundInnen technisch versierte Personen sind, nur weil sie im Besitz eines Smartphones sind. Gerade bei älteren und jüngeren Bevölkerungsteilen handelt es sich um ein systematisches Informations- und Verantwortungsdefizit zur Beurteilung der technischen Verarbeitungsprozesse der diversen App-Softwaremodule (vgl. ARTICLE 29 Data Protection Working Party 2011). Datenhandel ist generell ein Geschäft, das von einem großen ökonomischen Ungleichgewicht und fehlender Transparenz geprägt ist. Die Rechtslage bietet zwar grundsätzlich Schutz vor überbordendem und den Einzelnen beeinträchtigendem Datenhandel, die Kontrolle der bestehenden Regelungen scheint allerdings schwer, wobei auch das Unrechtsbewußtsein gering ausgeprägt ist (vgl. Čas und Peissl 2006).

Am 23. Februar 2012 wurde bekannt, dass sich die sechs größten Anbieter von App-Stores, unter anderem auch Apple, auf eine Datenschutz-Kooperation geeinigt haben. Apps sollen demnach nicht mehr unkontrolliert Daten sammeln dürfen.[56] Man wird sehen welche Auswirkungen diese Kooperation haben wird.

6.1 Handlungsempfehlungen

Im Lichte der Ausführungen dieser Studie drängen sich Empfehlungen auf, die zu einer Verbesserung der Situation führen könnten. Klar ist jedoch, dass diese in einem hochdynamischen Umfeld, das hauptsächlich von der Weiterentwicklung technischer Möglichkeiten und ökonomischen Profitstreben geprägt ist, nicht leicht umzusetzen sein werden. In Folge finden sich Empfehlungen an unterschiedliche Gruppen, die sich aus den hier erworbenen Erkenntnissen ergeben.

6.1.1 Politik allgemein

Vertrauen der KonsumentInnen in die Gesetze

Der permanente Verstoß gegen die Grundsätze des europäischen Datenschutzes und der in Unkenntnis erfolgte oder vielleicht sogar billigend in Kauf genommene Verstoß gegen europäisches Datenschutzrecht, der sich hinter dem Feigenblatt dessen, was als „informed consent“ bezeichnet wird, verbirgt, sollte nicht nur aus rechtspositivistischer Sicht ein Ende haben, sondern untergräbt

[56] Apple, Google und Co.: Datenschutzrichtlinien bei Apps werden Pflicht Netzwelt.de, 23. Februar 2012.

auch die Wirksamkeit und gesellschaftliche Akzeptanz der missachteten Regeln. Hier erscheint es dringend geboten, Datenschutzeinrichtungen mit den nötigen Ressourcen auszustatten, damit diese ihrer Aufgabe nachkommen und dem bestehenden Recht zur Durchsetzung verhelfen können.

Anreizsysteme für Hersteller

Der Bedeutung eines Smartphones als zentraler Ort (sensibler) personenbezogener Daten (die NutzerInnen sind identifizierbar über UDID/IMEI, Telefonnummer, Name, Browser-Fingerprint, Bilddaten, soziales Netzwerk, Zeit-Weg-Profile, diverse Login-Daten und Kombinationen daraus) wird derzeit kaum Rechnung getragen. Die gesellschaftliche Praxis ist weit von den Vorstellungen des Gesetzgebers entfernt, weshalb es angebracht erscheint, dass über Sanktionen oder Anreizsysteme nachgedacht wird, die bei der Herstellung des gewünschten Datenschutzstandards begleitend wirksam werden.

Grundlagen des Staates

Die Akzeptanz der Tatsache, dass die Entfaltung der eigenen Persönlichkeit und der dafür nötige Schutz der Privatsphäre eine conditio sine qua non in einem demokratisch organisierten Staat sind, der nur funktionieren kann, wenn die BürgerInnen freie Willensentscheidungen treffen und uneingeschränkt ihre Rechte ausüben können, ist die Grundlage bzw. der Rahmen für alle Maßnahmen in diesem Bereich. Weitere Forschung und bewusstseinsbildende Maßnahmen erscheinen nötig, um den Themenkomplex einerseits breit diskutieren zu können und andererseits weitere konkrete Vorgaben in der Politikberatung machen zu können.

6.1.2 Datenschutz

Neue Dimension der Überwachung

Der Übergang von der Überwachung fester Orte (bspw. mittels Videoüberwachung) zur Überwachung einzelner Objekte und Menschen verläuft anscheinend nur getrieben von technischen Möglichkeiten. Ein breiter gesellschaftlicher Diskussionsprozess wäre hier anzustreben, um solche schrittweisen Veränderungen rechtzeitig zu bedenken.

Vollzugsdefizit bestehender Regeln

Im Wettbewerbsrecht hat die Europäische Kommission schon öfter bewiesen, dass es durchaus möglich ist, gegen große internationale Konzerne vorzugehen, wenn diese sich nicht an die Regeln halten. Die Prozesse haben auch Beispielwirkung auf andere Firmen entwickelt. So wäre vielleicht eine einmalige Durchsetzung des Datenschutzrechts in diesem Bereich ausreichend, um alle Marktteilnehmer davon zu überzeugen, dass die Einhaltung der Datenschutzstandards in Europa nicht optional ist. Dazu ist die Zusammenarbeit der nationalen Daten- und Konsumentenschutzorganisationen notwendig, vermutlich unter Einbeziehung der EU-Kommission.

Transparenz

Unternehmen sollten dazu verpflichtet werden, klar darüber zu informieren, welche Daten sie sammeln, und wie sie diese nutzen. Im Falle von personenbezogenen Daten bspw. durch einen jährlichen Bericht über die über sie gespeicherten Daten an alle NutzerInnen/KundInnen.

Zukunft?

Kann es in Zukunft als zumutbar gelten, sich selbst einer Überwachung zu unterwerfen, wenn damit bspw. günstigere Versicherungsbedingungen einhergehen? Ansätze dazu sind bereits heute zu erkennen. Einem allzu schnellen Tausch persönlicher und gesellschaftlicher Freiheiten gegen ökonomische Vorteile einzelner sowie die Aushöhlung des Solidaritätsprinzips sollte jedoch ein Riegel vorgeschoben werden.

6.1.3 Hersteller, Betreiber, Privatwirtschaft

Bessere Steuerungsmöglichkeiten

Die geforderte informierte Zustimmung im Einzelfall ist schon alleine dadurch nicht gegeben, dass eine Zustimmung, wenn überhaupt, nur ein einziges Mal (nämlich während des Installationsprozesses) pauschal eingeholt wird. Hier wären feiner abgestufte Eingriffsmöglichkeiten für die NutzerInnen anzustreben.

Privacy by Design

Schon bei der Entwicklung von Telefonen und anderen Geräten, die Ortsdaten erheben und verarbeiten können, sowie bei der Entwicklung von Software für diese Geräte, sollte darauf geachtet werden, dass es Möglichkeiten für KonsumentInnen gibt, ihre Rechte in Bezug auf die über sie vorhandenen Daten auszuüben.

Anzeige

Wie von der Article 29 Working Party vorgeschlagen, würde ein sichtbares Zeichen am Display eines Smartphones, das jedes Mal, wenn Geodaten verarbeitet werden, zu sehen ist, viel zu der Schaffung eines öffentlichen Problembewusstseins beitragen, und darüber hinaus wieder ein gewisses Maß an Kontrolle an die NutzerInnen zurückgeben (vgl. ARTICLE 29 Data Protection Working Party 2011). Zusätzlich würden Monitoring Tools den Betroffenen helfen, zu sehen und zu kontrollieren, was mit ihren Daten passiert (z. B. die App *Taintdroid*).

Datenschutzgütesiegel

Wenn NutzerInnen sicher sein könnten, dass Apps nur das tun, was man von ihnen erwartet, wären sie vermutlich auch dazu bereit, für dieses Service mehr zu zahlen. Insofern könnte eine kontrolliertere Art der Software-Distribution dazu beitragen, die „schwarzen Schafe“ unter den Apps loszuwerden (vgl. Hogben and Dekker 2010). Dieses Transparenz- und Vertrauensproblem könn-

ten auch Zertifizierungen beheben, bspw. mit dem europäischen Datenschutzgütesiegel „EuroPriSe“[57].

6.1.4 KonsumentInnen

Automatisierte Falscheingaben und Kontrolle

Wie von Wetherall et al. empfohlen (vgl. Wetherall et al. 2011), könnten UserInnen von Smartphones, sobald eine kritische Masse das tut, die Datensammlungen relativ wertlos machen, indem ein Software-Layer (bspw. in Form einer anderen App) zwischen Betriebssystem, Sensor und datenhungriger App bei Anfrage durch ein Programm falsche Daten produziert und diese an die App weitergibt. Das funktioniert natürlich nur dort, wo die Daten nicht für die Funktion benötigt werden. Eine ad hoc-Entscheidung durch die NutzerInnen wäre also bei jeder Abfrage erforderlich. Die Umsetzung einer vergleichbaren Idee bietet bspw. „MockDroid“[58].

Darüber hinaus kann nur empfohlen werden, vorsichtig alle Möglichkeiten zur Kontrolle der Datenkommunikation zwischen einer App und „deren“ Server auszunutzen.

[57] http://www.european-privacy-seal.eu (02.06.2012).

[58] http://www.cl.cam.ac.uk/research/dtg/android/mock/ (02.06.2012).

Literatur

Achten, Oliver M. and Pohlmann, Norbert (2012), Sichere Apps, *Datenschutz und Datensicherheit*, 36/3/2012, S. 161-64.

Apple (2012), iOS 4: Grundlagen zu den Ortungsdiensten. <http://support.apple.com/kb/HT1975?viewlocale=de_DE&locale=de_DE>.

Apple (2012), iOS 5: Grundlegende Informationen zu den Ortungsdiensten.

Azuma, Ronald T. (1997), A Survey of Augmented Reality, *Presence: Teleoperators and Virtual Environments 6*, 355-85.

Berka, Walter (1999), *Die Grundrechte. Grundfreiheiten und Menschenrechte in Österreich.*, ed. Springers Handbücher der Rechtswissenschaft. (Wien. New York.).

Blumberg, Andrew J. and Eckersley, Peter (2009), On Locational Privacy, and How to Avoid Losing it Forever, in Electronic Frontier Foundation (ed.).

Bowker, Geoffrey and Star, Susan Leigh (2000), *Sorting things out. Classification and its consequences.* , ed. The MIT Press (Cambridge, London).

Braun, Markus, Khan, Dominik, and Özmü, Eray (2011), Mobile Zivilcourage – Mobile Community-Dienste für ortsbezogene Unterstützung von Menschen in Notlagen. <http://www.user.tu-berlin.de/komm/CD/html/ws615.html>.

Campbell, A. T., et al. (2006), People-centric urban sensing, *Second ACM/IEEE International Conference onWireless Internet* (Boston, MA, U.S.A.).

Castelluccia, Claude (2012), Behavioural Tracking on the Internet: A Technical Perspective, in S. Gutwirth et al. (ed.), *European Data Protection: In Good Health?* (Springer Science+Business Media B.V.).

Communities, European (2008), Global Disaster Alert and Coordination System (GDACS).

Conti, Greg (2009), *Googling Security – How much does Google know about you?* (Boston: Addison-Wesley).

Cortesi, Aldo (2011), How UDIDs are used: a survey. <http://corte.si/posts/security/apple-udid-survey/index.html>.

Deleuze, Gilles (1993), Postskriptum über die Kontrollgesellschaften, *Unterhandlungen 1972 – 1990.* (Frankfurt am Main), 254-62.

DerStandard.at (2008), Sicherheitspolizeigesetz im Eiltempo und ohne Diskussion beschlossen. <http://derstandard.at/3141872>.

DerStandard.at (2012), iPhone-Bug ermöglicht Zugang zu Adressbuch. <http://derstandard.at/1329870145613/Leck-in-iOS-501-iPhone-Bug-ermoeglicht-Zugang-zu-Adressbuch>.

Dolphin Technologies, GPS Ortungs- und Sicherheitssystem. <http://www.dolphin-technologies.com/produkte/gps-ortung/satalarm-metasat-ortung-tracking/33-74.htm>.

Eck, John E., et al. (2005), Mapping Crime: Understanding Hotspots, in National Institute of Justice (ed.), *MAPS. mapping & analysis for public safety* (Washington DC: U.S. Department of Justice, Office of Justice Programs).

Eikenberg, Ronald (2012), Gut App-geschaut, *c't*, Heft 7/2012, S. 120.

Enck, William, et al. (2010), TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. *9th USENIX Symposium on Operating Systems Design and Implementation (OSDI '10)* (Vancouver, BC, Canada).

Flickr-Blog (2011), Introducing geofences on Flickr!, <http://blog.flickr.net/en/2011/08/30/introducing-geofences-on-flickr/>.

Flickr, Beliebteste Kameras in der Flickr Community. <http://www.flickr.com/cameras/>.

Foucault, Michel (1994), *Überwachen und Strafen. Die Geburt des Gefängnisses.ed.* Suhrkamp (Frankfurt am Main.).

Fox, Dirk (2002), Der IMSI-Catcher, *Datenschutz und Datensicherheit*, 26/4 212-15.

GDACS (2012), Global Disaster Alert and Coordination System. <http://www.gdacs.org/default.aspx>.

Geier, Jim (2002), Deploying Indoor WLAN Positioning Systems. <http://www.wi-fiplanet.com/tutorials/article.php/1487271>.

Heider, Jens and Khayari, Rachid El (2012), Geht Ihr Smartphone fremd?, *Datenschutz und Datensicherheit*, 36/3/2012, S. 155-60.

Heise.de (2007), Neues österreichisches Sicherheitspolizeigesetz in der Kritik. <http://www.heise.de/newsticker/meldung/Neues-oesterreichisches-Sicherheitspolizeigesetz-in-der-Kritik-171122.html>.

Hogben, Giles and Dekker, Marnix (2010), Smartphones: Information security risks, opportunities and recommendations for users, (ENISA (European Network and Information Security Agency)).

Kampitsch, Karin, Leitner, Michael, and Schabauer, Horst (2008), Der Einsatz von Geografischen Informationssystemen im österreichischen Bundeskriminalamt.

Kang, Jerry, et al. (2012), Self-Surveillance Privacy, *Iowa Law Review*, 97, 809-47.

Korteland, E. and Bekkers, V. (2007), Diffusion of E-Government Innovations in the Dutch Public Sector: The Case of Digital Community Policing, *In Proceedings of 6th International Conference on Electronic Government (EGOV)* (Regensburg: M. Wimmer, H. J. Scholl, und A. Gronlund, Eds.,), 252-64.

Kreis, Düsseldorfer (2011), Datenschutzgerechte Smartphone-Nutzung ermöglichen!, *Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich* (Düsseldorfer Kreis).

Lawton, Brian A. and Schulenburg, Jennifer (2007), Assessing the impact of Hurricane Katrina on space-time clusters of crime patterns in Houston, *Ninth Crime Mapping Research Conference* (Pittsburgh, PA).

Levine, Ned (2007), CrimeStat: A spatial statistics program for the analysis of crime incident locations (Version 3.1), (Houston, TX: Ned Levine & Associates and Washington DC, National Institute of Justice.).

Lischka, Konrad and Volkery, Carsten (2012), W-Lan-Mitschnitte bei Street View. Europa gegen Google. <http://www.spiegel.de/netzwelt/netzpolitik/google-street-view-datenschuetzer-zu-w-lan-mitschnitten-a-831174.html>.

Lyon, David (1994), *The Electronic Eye: The Rise of the Surveillance Society*.

Lyon, David (2003), *Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination* (London and New York).

Lyon, David (2005), Wir haben gerade erst begonnen – Überwachen zwischen Klassifikation und Ethik des Antlitzes, in Leon Hempel and Jörg Metelmann (eds.), *Bild-Raum-Kontrolle: Videoüberwachung als Zeichen gesellschaftlichen Wandels.* (Suhrkamp, Frankfurt am Main), S. 22-32.

Manyika, James, et al. (2011), Big data: The next frontier for innovation, competition, and productivity, (McKinsey Global Institute).

Marx, Gary T. (1998), Ethics for the New Surveillance, *The Information Society*, Volume 14, 171-85.

MetroSense (2009), Our projects. <http://www.metrosense.dartmouth.edu/project.html>.

Miluzzo, E., et al. (2008), Sensing meets mobile social networks: The design, implementation and evaluation of the cenceme application, *6th ACM Conference on Embedded Networked Sensor Systems (SenSys' 08)* (Raleigh, NC, U.S.A.).

ORF-help (2011), Schnüffelsoftware konnte SMS abfangen. <http://help.orf.at/stories/1691796/>.

ORF-news (2012), Aufregung um russische „Stalking"-App. <http://orf.at/stories/2113256/>.

Party, ARTICLE 29 Data Protection Working (2011), WP 185, Opinion 13/2011 on Geolocation services on smart mobile devices, (ARTICLE 29 Data Protection Working Party).

Peissl, Walter (2003), Privacy in Österreich: Eine Bestandsaufnahme, in Walter Peissl (ed.), *Privacy – Ein Grundrecht mit Ablaufdatum? Interdisziplinäre Beiträge zur Grundrechtsdebatte* (Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften).

Riederer, Christopher, et al. (2011), For sale : Your Data, By: You, in USA; Telefonica Research Columbia Univ. New York, Barcelona, Spain; AT&T Labs-Research, NJ, USA (ed.), *Hotnets '11* (Cambridge, MA, USA.).

Rössler, Beate (2001), *Der Wert des Privaten*, ed. Suhrkamp Taschenbuch (Frankfurt am Main).

Roßnagel, Heiko and Zibuschka, Jan (2011), Using Mobile Social Media for Emergency Management – A Design Science Approach, *Proceedings of the 8th International ISCRAM Conference.* (Lisbon, Portugal).

Slivka, Eric Live Coverage of Apple's iPad 3 Media Event. <http://www.macrumors.com/2012/03/07/live-coverage-of-apples-ipad-3-media-event/>.

Solove, Daniel J. (2008), I've Got Nothing to Hide and Other Misunderstandings of Privacy, *George Washington University Law School Public Law Research Paper No. 289*.

Teufl, Peter (2010), SICHERHEITSANALYSE – IPHONE, (Zentrum für sichere Informationstechnologie – Austria).

Thurm, Scott and Kane, Yukari Iwatani (2010), Your Apps are Watching You, *Wall Street Journal*.

Tichy, Gunther und Peissl, Walter (2001), Beeinträchtigung der Privatsphäre in der Informationsgesellschaft, ITA-01-01.

UrbanSensing. <http://urban.cens.ucla.edu/projects/>.

Venne, Patrick Kolla-ten, Eikenberg, Ronald, and Schmidt, Jürgen (2012), Seblstbedienungsladen Smartphone, *c't*, Heft 7/2012, S. 114.

Wetherall, David, et al. (2011), Privacy Revelations for Web and Mobile Apps, (University of Washington, Intel Labs and Microsoft Research).

Wikipedia-Artikel (2012a), Problem des Handlungsreisenden. <http://de.wikipedia.org/wiki/Problem_des_Handlungsreisenden>.

Wikipedia-Artikel (2012b), Google Play. <http://de.wikipedia.org/wiki/Google_Play>.

Wikipedia-Artikel (2012c), Geofencing. <https://de.wikipedia.org/wiki/Geofencing>.

Wikipedia-Artikel (2012d), Smartphone. <http://de.wikipedia.org/wiki/Smartphone>, accessed 02.06.2012.

Glossar und Abkürzungsverzeichnis

3G Verbindungen
3G steht für die 3. Generation von Mobilfunkstandards, mit denen deutlich höhere Übertragungsraten möglich sind (max. 21 Mbit/s mit HSPA+, sonst 384 kbit/s für Verbindungen nach dem UMTS-Standard; in Amerika und Asien meist Verbindungen nach dem CDMA2000-Standard), als mit den Standards der 2. Generation (2 G; Edge (220 kbit/s) und GPRS (55 kbit/s) im GSM-Standard). Dadurch wurden Anwendungen, die hohe Datenraten verlangen, wie TV-Übertragungen, Video-Telefonie, schnelle Internetverbindungen u. dgl. erst ermöglicht *(siehe auch UMTS)*.

API (Application Programming Interface)
Unter API wird eine Schnittstelle für Anwendungsprogrammierung verstanden. Es handelt sich dabei um einen Programmteil einer Software, der anderen Programmen eine Schnittstelle zur Anbindung an das System zur Verfügung stellt.

APK-Datei (Application Package)
APK ist ein Dateiformat für die Verteilung und Installation von Application-Software und Middleware auf Google's Betriebssystem Android.

BAN (Body Area Network, WBAN für **Wireless Body Area Network)**
bezeichnet eine Unterkategorie eines PAN, die die Kommunikation zwischen medizinischen Sensoren und Geräten im und am Körper einer einzelnen Person umfasst *(siehe auch LAN)*.

Bluetooth
ist ein in den 1990er-Jahren entwickelter Funktechnik-Industriestandard für die Datenübertragung zwischen Geräten über kurze Distanz.

CAN (City Area Network)
CAN bezeichnet ein Netzwerk mit bis zu 5 km Ausdehnung, in dem üblicherweise die LANs verschiedener Filialen einer Firma innerhalb einer Stadt zusammengeschlossen werden *(siehe auch LAN)*.

CDMA2000
ist ein Mobilfunkstandard der dritten Generation, der hauptsächlich in Amerika und Teilen von Afrika und Asien Anwendung findet. Es handelt sich dabei um ein Codemultiplexverfahren, ähnlich wie dem in Europa gebräuchliche UMTS-Standard, das hier namensgebend war (Code Division Multiple Access).

DNT (Do Not Track)
Initiative für den technischen Einsatz von zusätzlichen Softwaremodulen, die Werbenetzwerken mitteilen, dass der Betroffene nicht getrackt werden möchte.

Eavesdroppers
Von Eavesdropping wird gesprochen wenn private Gespräche heimlich, ohne Zustimmung der Betroffenen, belauscht werden.

Firesheep
ist eine Software-Erweiterung für den Webbrowser Mozilla Firefox. Die Erweiterung macht es möglich, in einem ungesicherten Netzwerk (z. B. öffentliches WLAN) sog. Session Hijacking (siehe dort) durchzuführen.

FireWire (auch **1394**, oder **i.Link**)
ist ein Bus-Standard zur seriellen Datenübertragung, wobei 1394 der IEEE-Standard ist, und FireWire die Markenbezeichnung von Apple, und i.Link die Markenbezeichnung von Sony.

Function Creep
Ein sog. Function Creep liegt dann vor, wenn Daten für einen spezifischen Zweck gesammelt werden und mit der Zeit für einen anderen, ursprünglich (offiziell) nicht intendierten, nicht angestrebten Zweck genutzt bzw. weiterverarbeitet werden.

GAN (Global Area Network)
GAN bezeichnet ein Netzwerk unbeschränkter geografischer Ausdehnung, das mehrere Wide Area Networks miteinander verbindet. Das Internet wäre in der Systematik als GAN zu bezeichnen *(siehe auch LAN)*.

Geocaching
Geocaching ist eine Art elektronisch unterstützter Schatzsuche. Der Geocache, oder Cache, ist ein wasserdichter Behälter, dessen Position im Internet unter Angabe der GPS-Koordinaten veröffentlicht wird. Dadurch ist es möglich, mit einem Gerät mit GPS-Sensor auf die Suche danach zu gehen. Der Behälter enthält ein Logbuch, in das sich alle FinderInnen eintragen, und einen „Schatz“, meist kleine Tauschgegenstände.

Geotagging
Unter Geotagging versteht man das Hinzufügen geographischer Informationen bzw. Metadaten (Längen- und Breitengrade, Ortsnamen etc.) zu diversen Medien wie Fotos, Videos, Websites, Kurznachrichten (SMS) oder QR-Codes.

GSM (Global System for Mobile Communications)
Das Global System for Mobile Communications ist ein Standard für volldigitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungsvermittelte und paketvermittelte Datenübertragung sowie Kurzmitteilungen (Short Messages) genutzt wird. Es ist der erste Standard der so genannten zweiten Generation („2G“) als Nachfolger der analogen Systeme und der weltweit am meisten verbreitete Mobilfunk-Standard.

GIS (Geografische Informationssysteme)
Unter Geoinformationssystemen versteht man Systeme zur Erfassung, Bearbeitung, Organisation, Analyse und Präsentation geografischer Daten.

GPRS (General Packet Radio Service)
Der „Allgemeine paketorientierte Funkdienst“ dient zur Datenübertragung in GSM-Netzen, wobei der Funkraum erst dann besetzt wird, wenn wirklich Datenpakete übertragen werden. Die restliche Zeit ist der Funkraum frei für andere BenutzerInnen.

IP-Telefonie (Internet-Protokoll-Telefonie)
auch Internet-Telefonie oder Voice over IP (kurz VoIP).

IMSI (International Mobile Subscriber Identity)
ist eine interne TeilnehmerInnenkennung und dient der eindeutigen Identifizierung von Mobilfunk-NetzteilnehmerInnen. Die IMSI wird auf der sog. SIM-Karte (Subscriber Identity Module) gespeichert.

IMEI (International Mobile Station Equipment Identity)
ist eine 15-stellige Seriennummer, zur eindeutigen Identifizierung von GSM-, bzw. UMTS-Endgeräten.

IrDA (Infrared Data Association)
bezeichnet nicht nur den Zusammenschluss von Unternehmen im Bereich der Infrarot-Datenübertragung, sondern umgangssprachlich auch die Übertragungsart selbst.

LAN (Local Area Network)
Eine grobe Kategorisierung von Datenübertragungsnetzwerken unterteilt die Netzwerke je nach geographischer Ausdehnung in BAN (Body Area Network), PAN (Personal Area Network), LAN, CAN (City Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network) und GAN (Global Area Network). Als LAN wird typischerweise das Netzwerk in einem Gebäude, manchmal auch das Netzwerk einer Gebäudeansammlung (bspw. Firmencampus) bezeichnet, mit einer Ausdehnung von bis zu 500 Metern. Von Bedeutung sind in der Praxis vor allem die Begriffe LAN und WAN, weil damit auch der Unterschied zwischen einem (firmen)internen und einem externen Netz gemeint sein kann.

LTE (**Long-Term-Evolution**)
ist ein neuer Mobilfunkstandard (UMTS-Nachfolger, 4. Generation – 4G), der deutlich höhere Downloadraten (bis zu 300 Mbit/s) als bisherige Technologien erreichen kann.

MAC-Adresse (Media-Access-Control)
Physikalische Kennziffer bzw. Hardware Adresse, über die eine eindeutige Identifikation aller Netzwerkgeräte möglich gemacht werden soll. An diesem alpha-numerischen Code lassen sich auch mit einer gewissen Unschärfe Hersteller, Art des Geräts und Herstellungsdatum ablesen.

MAN (Metropolitan Area Network)
ist ein Netzwerk mit bis zu 100km Ausdehnung, das mehrere CANs und/ oder LANs städteübergreifend miteinander verbindet (siehe auch LAN).

PII (Personal Identifiable Information): Angloamerikanische Bezeichnung für personenbezogenes Datum.

PAN (Personal Area Network)
ist ein Netzwerk mit geringer Ausdehnung, typischerweise wenige Meter, das hauptsächlich PDAs, Mobiltelefone u. dgl. miteinander verbindet. Die Verbindung erfolgt über Bluetooth (in dem Fall spricht man dann von einem Piconet), IrDA, WLAN, USB oder Firewire. *(siehe auch LAN)*

QR-Code (Quick Response Code)
Der QR-Code ist ein zweidimensionaler Code, der von der japanischen Firma Denso Wave im Jahr 1994 entwickelt wurde.

RSSI (Received Signal Strength Indicator)
Der RSSI-Wert ist ein Indikator für die Empfangsfeldstärke kabelloser Kommunikationsanwendungen.

Session Hijacking
Session Hijacking ist ein Angriff auf eine verbindungsbehaftete Datenkommunikation („Entführung einer Kommunikationssitzung“) zwischen zwei Computern. Authentifiziert sich einer der Kommunikationspartner innerhalb der Sitzung gegenüber dem anderen, besitzt diese eine Vertrauensstellung. Ziel der AngreiferInnen ist es, durch die „Entführung“ dieser Sitzung die Vertrauensstellung auszunutzen, um dieselben Privilegien wie die rechtmäßig authentifizierten BenutzerInnen zu erlangen.

TDOA (Time Difference of Arrival)
ist ein zeitbasiertes Verfahren zur Positionsbestimmung von mobilen Endgeräten, wobei die Entfernung zwischen dem Gerät und der Funkzelle aus der Signallaufzeit berechnet werden kann.

UMTS (Universal Mobile Telecommunications System)
siehe auch 3G

UDID (Unique Device Identifier)
40-stelliger Code zur Identifizierung von iPhone-Endgeräten.

W3C (World Wide Web Consortium)
Standardisierungsgremium für Techniken, die das World Wide Web betreffen.

WAN (Wide Area Network)
bezeichnet ein Netzwerk mit großer geografischer Ausdehnung, das LANs, CANs, MANs und/oder einzelne Rechner über weite Strecken miteinander verbindet *(siehe auch LAN)*.

WAP (Wireless Application Protocol)
WAP bezeichnet eine Sammlung von Techniken und Protokollen, deren Zielsetzung es ist, Internetinhalte für langsamere Übertragungsraten und kleinere Displays im Mobilfunk verfügbar zu machen.

WLAN (Wireless Local Area Network)
WLAN ist ein drahtloses lokales Netzwerk bzw. Funknetz
(siehe auch Wi-Fi).

Wi-Fi
ist ein für Marketingzwecke erfundener Kunstbegriff (in Anlehnung an die Abkürzung Hi-Fi für „High-Fidelity"-Audio-Komponenten), der in einigen Ländern (USA, Großbritannien, Kanada, Spanien, Frankreich, Niederlande, Belgien, Italien, Republik Südafrika, Chile, Malta, Peru, Polen, Portugal, Russland, Schweden, Uruguay sowie auch Deutschland) als Synonym für WLAN fungiert.