

Zentrum für Technologiefolgen-Abschätzung
Centre d'évaluation des choix technologiques
Centro per la valutazione delle scelte tecnologiche
Centre for Technology Assessment



Geographische Wegmarken in der Cyberwelt

Ortungstechnologien als Herausforderung für eine offene Gesellschaft

Angaben zur Studie «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern»

Die Studie wurde unterstützt vom Bundesamt für Statistik BFS, vom Bundesamt für Strassen ASTRA und vom Bundesamt für Landestopografie swisstopo.

Lorenz Hilty, Britta Oertel, Michaela Wölk, Kurt Pärli.

**Lokalisiert und identifiziert
Wie Ortungstechnologien unser Leben verändern**

TA-SWISS, Zentrum für Technologiefolgen-Abschätzung (Hrsg.). vdf Hochschulverlag AG der ETH Zürich, 2012.

ISBN 978-3-7281-3460-8

Auch als Open-access-eBook erhältlich:
www.vdf.ethz.ch/info/showDetails.asp?isbnNr=3460

Zusammenfassung online verfügbar: www.ta-swiss.ch



Inhalt

Ortung in aller Kürze.....	4
1 Geodaten im Übergang zwischen Cyberwelt und Realität	5
Zuordnung und Spionage gleichermassen leicht gemacht	5
Der Schnüffelpfad des Cyberstalkers	5
Ortungstechniken in unterschiedlicher Gestalt.....	6
2 Ortungstechniken für jeden Zweck.....	7
Einfacher mobil.....	7
Freundschaftspflege im sozialen Netzwerk.....	7
Sicherheit gegen Freiheit abwägen	8
Bevormundung oder Selbständigkeit?.....	8
Wo bin ich – und wo sind meine Daten?	9
3 Persönliche Daten schützen.....	10
Garantierter Kontrollverlust.....	10
Abstinenz ist auch keine Lösung	11
Rechtlich fragwürdige Zweckentfremdung	11
Überall Durchsetzungsdefizite.....	11
Globale Kommunikation erfordert globalen Schutz	11
Studie «Ortungstechnologien»	13
Impressum.....	14

Ortung in aller Kürze

Um mit der ganzen Welt vernetzt zu sein, muss man nicht mehr am Computer oder neben einem Telefon sitzen: Dank Laptop und Handy können wir uns praktisch von jedem Standort aus ins Internet einwählen und überall Telefongespräche führen. Allerdings hinterlassen wir dabei Spuren, die dazu dienen können, unsere Wege zu rekonstruieren: Die Mobilfunkanbieter wissen, wann wir uns bei welcher Handyantenne eingebucht haben, und Internetprovider kennen unsere IP-Adresse, die Rückschlüsse auf den ungefähren Standort zulässt. Wenn wir über Kurzstreckenfunktechnik (WLAN) im Internet surfen, ist die Ortung sogar relativ präzise. Kommt dazu, dass immer mehr Gebrauchsgegenstände mit Lokalisierungsfunktionen ausgestattet sind.

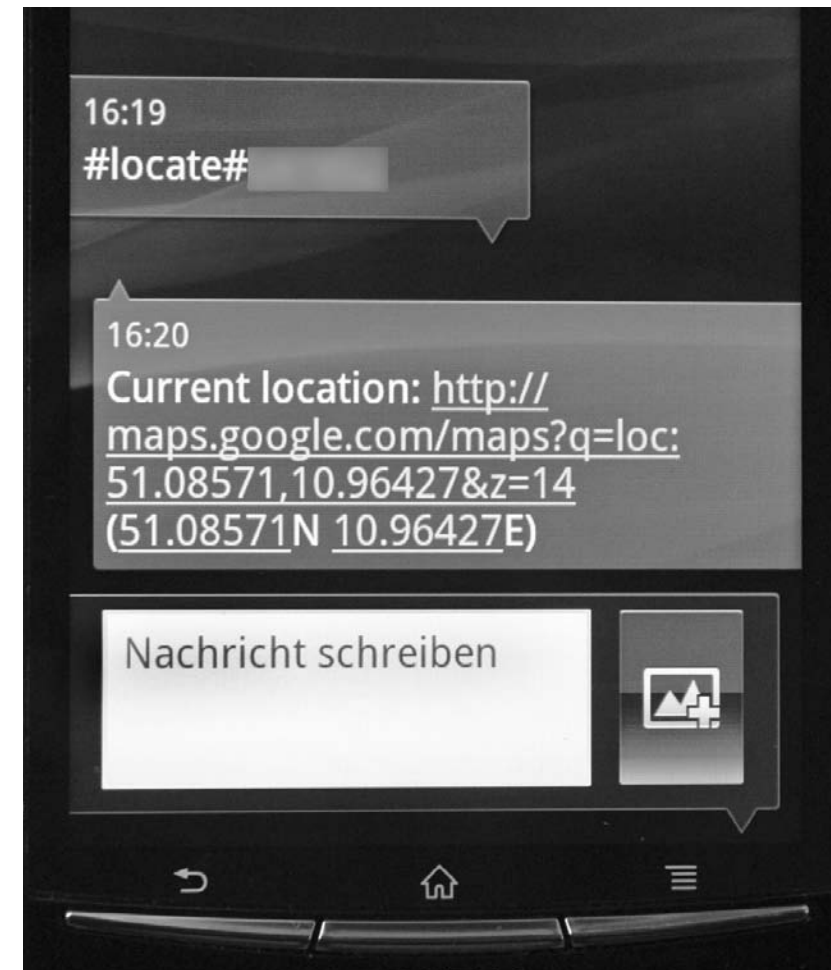
Ortungsdaten werden daher zunehmend zu einer Grundlage für innovative Geschäftsmodelle und Dienstleistungen. Positionsangaben in Echtzeit können beispielsweise bei Verkehrsunfällen helfen, dass Rettungsdienste die Verunglückten rasch finden. Gespeicherte Bewegungsprofile wiederum sind für die Verkehrsplanung hilfreich, um Engpässe auf Strassen zu erkennen und zu beseitigen. Der Umgang mit Ortungsdaten birgt allerdings auch Risiken. Wer standortbezogene Informationen zu offenherzig preisgibt, gewährt Einblick in seinen Alltag und seine Gewohnheiten. Soziale Netzwerke wie Facebook pflegen zudem viele persönliche Informationen an Dritte weiterzugeben, die für ihr Marketing an den Ortungsdaten interessiert sind, sodass diese auf undurchsichtigen Pfaden Verbreitung finden, ohne dass die Betroffenen davon Kenntnis haben.

Mit der Studie «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändert» will TA-SWISS für die Problematik sensibilisieren und Empfehlungen für den Umgang mit standortbezogenen Daten nahelegen.

Empfehlungen aus der Studie von TA-SWISS

Die Entscheidungstragenden in Politik und Verwaltung sind in mehrfacher Hinsicht gefordert:

- Sie müssen sich für Massnahmen starkmachen, damit der Datenschutz im internationalen Rahmen durchgesetzt werden kann.
- In dem Mass, als die Organisation von Rettungsdiensten, Verkehrssystemen und anderen Handlungsfelder der öffentlichen Hand auf Ortungssysteme aufbauen, müssen diese in das Schweizer Programm zum Schutz kritischer Infrastrukturen aufgenommen werden.
- Zudem gilt es, verlässliche und transparente Softwareprodukte zu zertifizieren, sodass der Datenschutz zu einem Qualitätsmerkmal der entsprechenden Angebote erhoben wird.
- Ferner gilt es, eine eingeschränkte Aufbewahrungsdauer von Ortungsdaten gesetzlich festzuschreiben; den Betroffenen sollte eine Art «digitaler Radiergummi» in die Hand gegeben werden, damit sie im Hinblick auf ihre personenbezogenen Ortungsdaten das Recht auf Vergessen durchsetzen können.
- Weiter ist zusätzliche empirische sozialwissenschaftliche Forschungsarbeit vonnöten, um Wissenslücken im Umgang mit Ortungsdaten zu schliessen.
- Schliesslich ist die Kompetenz über elektronische Medien generell und besonders bei Jugendlichen zu verbessern, um diese für die Chancen und Risiken ihrer online gestellten Bewegungsprofile und Aufenthaltsorte zu sensibilisieren.



Die vorliegende Kurzfassung beruht auf der Studie «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern». Verfasst wurde sie von einem interdisziplinären Team unter der Leitung von Lorenz Hilty, EMPA (www.ta-swiss.ch).

1 Geodaten im Übergang zwischen Cyberwelt und Realität

Das Alibi entscheidet oft über Verurteilung oder Freispruch. Nicht von ungefähr. Übersetzt bedeutet das Wort «anderswo» und meint «nicht am Tatort». Tatsächlich lassen Informationen darüber, wo sich jemand aufhält, Rückschlüsse darauf zu, was er oder sie tut, wahrnimmt und weiss. Der Zugang zu Daten, die Aufschluss darüber geben, wer sich zu einer bestimmten Zeit an einem genau definierten Ort aufhält, eröffnet daher zahllose Möglichkeiten – im Guten wie im Schlechten.

«Wow, c'est où ça?», postet am 15. März 2010 ein Betrachter der digitalen Fotosammlung von Jean-Frédéric Beaudet. Die stimmungsvolle Aufnahme zeigt eine verlassene Lagerhalle, auf der die Zeit schwer zu lasten scheint. Allein dem warmen Licht ist es zu verdanken, dass der Blick auf die staubbedeckten Regale und verrosteten Stahlträger eher Nostalgie als Beklemmung hervorruft. Die Frage nach dem Standort freilich hätte sich der Besucher des Google-Fotoportals Picasa sparen können. Denn am rechten Bildschirmrand stehen die Koordinaten des Sujets: 46,755165 Breitengrad Nord und 71,290497 Längengrad West. Google Maps ordnet dieser Positionsangabe ein aufgegebenes Gewerbegebiet am Rand von Saint Louis zu, einem Bezirk der kanadischen Stadt Quebec. Dank Google Street View lässt sich die aufgegebene Halle sogar von aussen besichtigen; der mit Graffiti besprühte weisse Bau nimmt sich wesentlich weniger malerisch aus, als man auf Grund der Innenansicht vermutet hätte.

Die Fotoinformationen verraten auch, dass eine Canon EOS Digital Rebel XT zum Einsatz kam – ein Modell, das mit einem Empfänger für das Global Positioning System GPS ausgestattet und imstande ist, automatisch Informationen über den Aufnahmeort zu speichern. Mit GPS-Empfängern sind immer mehr digitale Fotoapparate und Camcorders ausgerüstet. Doch

selbst mit einem älteren Apparat braucht dank separater GPS-Tracker, die über einen externen Anschluss mit der Kamera verbunden werden, niemand auf die so genannten Geotags zu verzichten. Und wer mit einem Smartphone der neueren Generation fotografiert oder filmt, bekommt mit seinen Bildern standardmässig auch die Daten über den Aufnahmeort mitgeliefert; wird diese Anwendung am Handy ausgeschaltet, funktionieren oft auch andere Apps nicht mehr.

Zuordnung und Spionage gleichermassen leicht gemacht

Viele User von Fotoportalen wie Picasa, Flickr, Fotocommunity oder Locr schätzen die ergänzenden Positionsangaben, denn damit lassen sich online publizierte Fotos auch nach Aufnahmeort durchsuchen. Das Fotoportal Panoramio nutzt geographische Angaben gar als Ordnungsprinzip seiner Sammlung. Was aber bei Bildern von Landschaften und Stadtimpressionen unproblematisch ist, kann im Fall von Schnappschüssen der privaten Geburtstags- oder Hochzeitsparty eine heisse Spur legen, die es Neugierigen ermöglicht, das Leben der Abgebildeten auszuspähen.

Das lässt sich anhand der Online-Aktivitäten einer jungen Familie gut zeigen. Salomé und Klemens Christen-Kaiser haben im Frühherbst 2006 geheiratet; das auf einer Fotoplattform aufgeschaltete Bild zeigt sie am Tag ihrer zivilen Trauung mit ihrer Tochter Gianna vor dem Einwohneramt in der Hauptstadt ihres Wohnkantons. Die Kleine schlägt mit ihren dunklen Augen und dem braunen Haarschopf ganz nach der Mama; von der blonden Lockenmähne des Vaters ist jedenfalls nichts zu sehen. Der Fotosammlung ist auch zu entnehmen, dass Gianna acht Monate vor der Hochzeit zur Welt kam: Bilder zeigen sie als Säugling im blassgelben Strickjäckchen.

Der Schnüffelpfad des Cyberstalkers

Die im Internet publizierte Fotosammlung verrät viel über die Familie Christen. Zusammengestellt hat sie Patrick Siegenthaler, der Patenonkel von Gianna und ein langjähriger Freund von Klemens. Eine Klassenaufnahme aus den frühen 1990er-Jahren belegt, dass die zwei gemeinsam die Sekundarschulbank gedrückt haben. Wenn nun rund 15 Jahre später der Confiseur bei der Hochzeitstorte des jungen Paares auf den üblichen weissen Zuckerguss verzichtet, geht das als Anekdote durch; für die Privatsphäre schon mehr ins Gewicht fällt, dass Klemens ein ausgezeichneter Sportler ist. Auf dem Snowboard in Saas Fee macht er beste Figur, bei verschiedenen Wanderungen, zum Beispiel im Schweizerischen Nationalpark, ist er mit von der Partie («in Tarasp, Kanton Graubünden, Schweiz, aufgenommen», erläutern die Informationen zur Foto), ebenso auf einer Fahrradtour nach Westfrankreich («aufgenommen in Grayan-et-l'Hôpital, Aquitanien, Frankreich»). Aufschlussreich ist auch, dass Salomé und Klemens in einer grossen Parkanlage ihrer Stadt einen so genannten Wunschbaum für Gianna gewählt haben und ihre Tochter dort regelmässig ablichten; wer in Patricks Sammlung die Fotos nach dem entsprechenden Standort absucht, findet eine Bildserie, die die Entwicklung vom pausbäckigen Baby zum kleinen Mädchen mit lustiger Haartracht dokumentiert.

Patrick verhält sich bei der Veröffentlichung seiner Fotos nicht einmal besonders indiskret: Die Familiennamen von Klemens und Salomé erscheinen in keiner Legende. Es sind Bilder verschiedener Sportanlässe in Patricks Sammlung – Marathonläufe, Rad- und Skirennen – die letztlich verräterisch sind. Mehrere Fotos zeigen das Paar als Mitglied eines Teams, und die Website des Anlasses versieht die Mannschaftsbilder mit Vor- und Nachnamen der Teilnehmenden.

Jetzt ist es ein Leichtes, im nächsten Schritt anhand von sozialen Netzwerken wie Facebook, LinkedIn oder Xing noch mehr Details über Klemens und seine Angetraute aufzustöbern: Sie ist Evolutionsbiologin und pflegt in ihrer Freizeit unter anderem gerne Holz zu hacken, er ist als Angestellter in einer Informatikfirma tätig. Die Porträts auf der Homepage des Arbeitgebers bestätigen, dass es sich tatsächlich um die Ausgespähnten handelt und nicht um Personen, die zufällig gleich heissen. Im Übrigen wurden für diesen Bericht die Namen der Beschriebenen geändert und die in den Fotos enthaltenen Ortsangaben teilweise vergrößert. Der Fall aber ist real und zeigt: Wer im Internet persönliche Daten veröffentlicht, muss damit rechnen, dass neugierige Zeitgenossen Details zu Lebensweg, persönlichen Beziehungen und Gewohnheiten aufdecken. Wer wie Salomé zudem noch regelmässig auf Twitter zwitschert, gewährt unwillkürlich weitere Einblicke ins Privatleben: Da werden ihre politischen Sympathien offenbar, persönliche Vorlieben – oder auch die regelmässige Benützung einer bestimmten Bahnverbindung.

Informationen über häufig zurückgelegte Wegstrecken sind besonders aufschlussreich, denn der Mensch ist ein Gewohnheitstier. Gelingt es Schnüfflern, das Bewegungsprofil einer Person während drei Monaten auszuwerten, reicht das laut Studien aus, um ihren Aufenthaltsort zu einem beliebigen Zeitpunkt mit einer Treffwahrscheinlichkeit von 93 Prozent vorauszusagen. Auch Angaben darüber, wo sich jemand gerne aufhält oder wohnt, sind vielsagend. Denn ob die Urlaubsfotos in Dubai oder Engelberg aufgenommen wurden und ob man die Jugendherberge oder das Fünf-Sterne-Hotel frequentiert, lässt Rückschlüsse auf die finanzielle Situation zu. Und obschon Familie Christen bewusst auf den Eintrag im Telefonbuch verzichtet, lässt sich mit etwas Kombinationsgabe die Wohngemeinde ausfindig machen. Dank Diensten wie Google Earth oder Street

View wiederum stellt man auch ohne Besichtigung vor Ort rasch fest, ob das Zuhause im Villenquartier, im Bauerndorf oder in der Hochhaussiedlung liegt.



Ortungstechniken in unterschiedlicher Gestalt

- Satellitenortung, Global Positioning System GPS: Ursprünglich zur Navigation im militärischen Bereich entwickelt, wird das System heute in verschiedensten Bereichen eingesetzt. Im Freien orten sich GPS-Empfänger mit einer Genauigkeit von rund zehn Metern (abgesehen von lokalen Verschattungen durch Tunnels oder Gebäude).
- Handyortung: Die Lokalisierung erfolgt hier über die Mobilfunkantennen. Die Präzision der Ortsangaben hängt denn auch von der Dichte der Sendemasten ab; unter günstigsten Bedingungen, in Ballungsräumen, liegt sie in der Grössenordnung von 100 Metern. Die Identifikation der einzelnen Handys erfolgt über die SIM-Karte. Technisch ausgereifte Handys mit Internetzugang, die sogenannten Smartphones, sind ausserdem mit einem GPS-Modul ausgestattet, das eine genauere Ortung zulässt.
- Wireless Local Area Networks WLANs dienen der drahtlosen Verbindung von nahe beieinander stehenden Computern untereinander und mit dem Internet. Eine WLAN-Basisstation ermöglicht dabei den drahtlosen Zugang zu einem lokalen Netzwerk. Geortet werden die mobilen Geräte in Bezug auf die Basisstationen, sofern diese in entsprechenden Datenbanken verzeichnet sind.
- Ortung über die IP-Adresse: Für den Zugriff aufs Internet benötigt jedes Gerät eine IP-Adresse. Dynamische IP-Adressen werden von den Providern den gerade aktiven Endgeräten zugeteilt. Da jeder Provider über einen festen Bestand an Adressen verfügt, lässt sich bei bekannter IP-Adresse der geographische Standort des Endgerätes auf ein bestimmtes Gebiet einschränken. Die genaue Ortung setzt voraus, dass der Provider die Verbindungsdaten preisgibt.

2 Ortungstechniken für jeden Zweck

Die Satelliten des Global Positioning System GPS wurden in den 1970er-Jahren vom US-amerikanischen Militär eigens für die Positionsbestimmung und Zeitmessung in den Orbit geschossen. Das System ist das bekannteste, bei weitem aber nicht das einzige Mittel, um den Standort von Menschen und Geräten zu bestimmen. Auch die weitherum gebräuchlichen WLAN sowie Internetadressen von Computern und natürlich auch von Smartphones verraten, wo man sich befindet.

Klemens und Salomé fahren – auch das ist fotografisch und durch Blog-Einträge belegt – oft mit dem Rad und mit Eisen- und Strassenbahn. Sie dürften dabei auch die Fahrpläne und Reiseinformationen nutzen, welche die Transportgesellschaften über das Handy bereitstellen – teilweise punktgenau bezogen auf den Standort des Smartphones.

Einfacher mobil

Auch ausgedehntere Ausflüge mit verschiedenen Transportmitteln und über Tarifgrenzen hinaus sind für die Familie Christen-Kaiser dank Ortungstechniken recht einfach geworden: Der Gang zum Billettautomaten entfällt, es reicht aus, das in Form eines Strichcodes auf das Handy geladene elektronische Ticket in der Jackentasche mitzuführen. Ein vor wenigen Jahren in der Schweiz unter dem Namen «ETIK» lanciertes Projekt, das sich im Entwicklungsstadium befindet, treibt die Annehmlichkeiten noch weiter. Man braucht mit ETIK den Zielort eines Ausflugs nicht einmal mehr im Voraus zu kennen. Ein in ein Kunststoffkärtchen eingebrachter Sensor registriert die Fahrgäste berührungsfrei, sobald sie ein Fahrzeug betreten und wieder verlassen. Die für die Bezahlung relevanten Angaben wie Einsteige- und Aussteigeort, Zeitpunkt, Wagenklasse und dergleichen werden erhoben, im

Fahrzeug selber gespeichert und bei Betriebsschluss an einen Server übermittelt. Voraussetzung ist, dass die Fahrzeuge mit GPS ausgerüstet sind, damit immer feststeht, wo sie sich gerade befinden. Sowohl Vorauszahlungen im Prepaid-Verfahren als auch die nachträgliche Abrechnung wären denkbar, und für die weiter entfernte Zukunft ist sogar eine Verfeinerung der Tarifstruktur nicht ausgeschlossen: So könnten flexibel Rabatte gewährt werden, wenn die Fahrgäste in Nebenverkehrszeiten unterwegs sind, und auch ein Klassenwechsel könnte spontan und ohne Aufwand erfolgen. Ausserdem könnten auch erweiterte Angebote wie etwa ein Museumseintritt oder die Benutzung von Skiliften in das elektronische Ticket integriert werden. Eigentliche Bewegungsprofile fallen bei ETIK übrigens keine an: Die Daten werden anonymisiert und nach einer festgeschriebenen Frist gelöscht.

Als begeisterter Wintersportler kann Klemens auch die Entwicklung im Bereich der Lawinenortungsgeräte nutzen. Jene der neueren Generation sind zusätzlich zum üblichen Radar mit GPS-Empfängern ausgerüstet; das bringt für die rasche Lokalisierung der Verschütteten insbesondere abseits der Pisten weitere Informationen. Im Sommer lässt sich die Lawinensuchfunktion abschalten und das Gerät zur Orientierung im Gelände einsetzen. Es zeichnet die eingeschlagenen Pfade auf, die sich anschliessend am Computer herunterladen und mit anderen Bikern oder Wanderern teilen lassen.

Ihre iPhones erlauben es Klemens und Salomé zudem, von der Applikation zu profitieren, die von der Rettungsflugwacht Rega entwickelt wurde. Die App übermittelt bei einem Notruf zugleich die Standortangaben des Anrufers und beschleunigt damit den Ortungsvorgang – ein Zeitgewinn, der Leben retten kann. Auch das von der EU für den Strassenverkehr geplante Notrufsystem eCall baut auf GPS- und Mobilfunkmodulen auf.

Die Idee: Ein Steuergerät löst bei einem Unfall einen Notruf aus, zugleich schalten sich die Ortungssysteme ein. Damit fallen keine Bewegungsprofile an, aber der Rettungsdienst erhält trotzdem die Koordinaten für den raschen Einsatz. Ab 2015 sollen Neuwagen mit dem neuen System ausgerüstet sein; grosse Vorteile verspricht man sich in Fällen, wo die Verunglückten nicht mehr in der Lage sind, mit der Notrufzentrale zu kommunizieren, oder bei Touristen, die die Landessprache nicht beherrschen.

Nicht nur geographische Daten über Einzelpersonen sind aufschlussreich. Insbesondere für die Verkehrssteuerung bringt die «Schwarmüberwachung» Vorteile: Wenn sich viele Handys auf einer Autobahn nur im Schrittempo fortbewegen, lässt das auf einen Stau schliessen. Solche Bewegungsdaten dienen nicht nur der Stauwarnung, sondern lassen sich auch für die Verkehrsplanung auswerten, um den Strassenraum den Bedürfnissen entsprechend zu gestalten.

Schliesslich können Ortungstechniken dazu beitragen, die Wege auch innerhalb eines Gebäudes zu optimieren. So findet eine neue App aus der Hochschule Bingen (D) in Spitälern Verwendung. Bei einem Notruf alarmiert sie dank WLAN über das Handy nur gerade jene Ärztinnen und Ärzte, die sich im nächsten Umkreis befinden. Das spart Zeit und vermeidet Hektik.

Freundschaftspflege im sozialen Netzwerk

In jüngerer Zeit haben Ortungsdaten im Zusammenhang mit den sozialen Netzwerken für Diskussionen gesorgt. Viele klassische soziale Netze wie Facebook, Google+ oder Twitter bieten auch über ihre Handy-Apps eine Lokalisierungsfunktion an. Neuere Kommunikationsplattformen wie Foursquare oder Yelp wurden gar eigens für eine ortsbezogene Nutzung konzipiert. Dabei geht es

darum, den eigenen Standort auf einer interaktiven Karte zu vermerken und zu schauen, welche der «Freunde» sich in der Nähe aufhalten. Es handelt sich dabei in der Regel um eine Selbstortung; das bedeutet, dass der User seinen Standort selbst bekannt gibt, beispielsweise, indem er in einer bestimmten «Location» eincheckt.

Beim Mitteilungsdienst Twitter etwa, der die Länge der Nachrichten beschränkt, ist die zusätzliche Ortungsfunktion ein echtes Plus – vergibt man sich doch keines der 140 Zeichen für eine geographische Angabe. Die Funktion ist nicht standardmässig eingeschaltet, sondern muss von den Nutzerinnen und Nutzern aktiviert werden. Diese können zudem bei jedem Eintrag entscheiden, ob sie ihren Aufenthaltsort veröffentlichen wollen oder nicht. Trotz dieses vergleichsweise vorbildlichen Umgangs mit Positionsangaben warnen Fachleute eifrige «Zwitscherer» vor den Gefahren. Wer häufig Statusmeldungen versendet und dabei auch noch von unterwegs die Positionsdaten publiziert, verrät potenziellen Einbrechern, wann die Wohnung leer steht.

Ihre Schöpfer preisen soziale Netze als Plattformen für den privaten Austausch unter Gleichgesinnten; doch für die Wirtschaft sind sie kaum weniger interessant. Der deutsche Dienst friendticker, der für private Anwender kostenlos ist, erhebt bei Firmen eine Aufnahmegebühr und für jeden erfolgreichen Check-in eines Mitglieds eine weitere Abgabe. Zusätzlich geben die Mitglieder in den allgemeinen Geschäftsbedingungen ihr Einverständnis, dass Werbung auf ihr Endgerät gesendet wird. Dank der Positionsangaben wird nun auch standortbezogenes Mikromarketing möglich, mit Reklame, die passgenau auf die Interessen der Handybesitzer zugeschnitten ist. So könnte Salomé dereinst auf ihrem Display einen Hinweis auf das vegetarische Restaurant gleich um die Ecke bekommen, oder auf das am nächsten gelegene Geschäft für Outdoor-Sportartikel.

Sicherheit gegen Freiheit abwägen

Ein IT-Fachmann wie Klemens kennt verschiedene Wege, um mit Ortungstechniken für den Fall vorzukehren, dass jemand seinen Laptop stiehlt. Es gibt etliche Programme, die zu diesem Zweck auf dem Gerät installiert werden können. Kommt es abhanden, loggt sich ihr Besitzer auf einer Homepage ein, gibt eine Vermisstenanzeige auf und fordert die Positionsdaten des Laptops an. Sobald dieses eingeschaltet wird, übermittelt es seinen Standort, den es dank WLAN oder – weniger präzise – über die IP-Adresse ermittelt. Die Medien berichten von Fällen, wonach ein Bestohler mit der Kamera des Laptops eine Foto des Langfingers schoss und anschliessend auf Facebook veröffentlichte; die private Diebesjagd war angeblich von Erfolg gekrönt. Für das Handy existieren ebenfalls Apps, die ein gestohlenes oder verlorengegangenes Gerät zu orten vermögen.

Um die Sicherheit in Unterführungen, Bahnhofshallen oder in öffentlichen Transportmitteln zu erhöhen, setzen Behörden und Unternehmen immer häufiger Videokameras ein. Tatsächlich kann ihr Einsatz dazu beitragen, das Sicherheitsgefühl von Passantinnen und Passanten zu stärken. Auch viele Kondukteure in Strassenbahn und Bus schätzen die Kamera, um bei Vorfällen wie Schlägereien abgesichert zu sein. Dass insbesondere bei öffentlichen Verkehrsmitteln die Videoüberwachung dazu beiträgt, Gewalt- und Vandalenakten vorzubeugen, ist mittlerweile durch Studien belegt. Aber auch hier fallen geographische Positionsangaben an, weil Personen an bestimmten Orten gefilmt werden – oft ohne dass es ihnen bewusst ist.

Die Sicherheit steht auch bei Systemen zur Überwachung von Personen im Vordergrund. Bekannt sind die elektronischen Fussfesseln im Strafvollzug. Das

Polizeigesetz einzelner Kantone, etwa von Basel-Landschaft, gestattet den Einsatz von mit GPS ausgestatteten elektronischen Fesseln, wenn es gilt, Betroffene vor gewalttätigen Partnern oder ihnen nachstellenden Personen zu schützen. Dank der Daten, die das System übermittelt, sehen die Behörden, ob der Überwachte das verordnete Rayonverbot einhält. Um die gefährdete Person wird damit ein virtueller Schutzzaun gezogen, den der Stalker nicht übertreten darf.

Bevormundung oder Selbständigkeit?

Elektronische Schutzzäune können auch so konzipiert sein, dass sie die Schützlinge davon abhalten, ein bestimmtes Areal zu verlassen. An US-amerikanischen und britischen Schulen sorgten Tracking-Systeme für Empörung. Eine Schulleitung nutzte die Positionsdaten nämlich nicht nur, um die Anwesenheit der Schulkinder im Unterricht zu kontrollieren, sondern gestattete es dem Anbieter, mit den Daten für sein System zu werben. An ihrer unkontrollierten und intransparenten Weiterverwendung stiessen sich viele Eltern.

Schliesslich kann ein virtueller Schutzzaun auch errichtet werden, um einen Alarm auszulösen, wenn gefährdete Menschen – etwa Alzheimerkranke – ein definiertes Gebiet verlassen. In diesem Fall kann ein Armband mit Ortungsfunktion sogar dazu beitragen, dass der Bewegungsspielraum der Betroffenen grösser wird, weil sie sonst von realen Zäunen auf dem Klinikgelände zurückgehalten werden müssten. Dennoch ist bei der Entscheidung, ob dem Bedürfnis nach Sicherheit oder eher dem Streben nach Freiheit nachgelebt werden soll, das Dilemma vorprogrammiert. Gerade bei Personen, die ihre Interessen nicht selber zu artikulieren und die Tragweite der Entscheidungen nicht zu überblicken vermögen, gilt es, besonders sorgfältig zwischen Fürsorge und Autonomie abzuwägen.

Wenn staatliche Behörden über die Mittel verfügen, um – etwa im Kampf gegen die Kriminalität – Individuen auszuspähen, liegt das im Interesse der Gesellschaft. Polizei und Staatsanwaltschaft sind dabei an klare gesetzliche Vorgaben gebunden. Allerdings gibt die Technik auch Privaten die Mittel in die Hand, um Dritten auf illegale Weise nachzuspionieren. Die thailändische Software-Schmiede Vervata etwa hat dazu ein kleines Programm entwickelt, das wie ein trojanisches Pferd funktioniert. Es macht das Handy zur Wanze und leitet sogar die Telefongespräche oder Umgebungsgeräusche – zum Beispiel Diskussionen während eines Treffens – an die Spitzel weiter. Es genügt, dass diese das Smartphone während ein paar unbeaufsichtigten Minuten in die Hand bekommen, um das Programm «Flexispy» zu installieren. Die Software übermittelt anschliessend die Daten an einen Server in Thailand, auf den sich der Schnüffler einloggen und die Angaben zu den ein- und ausgehenden Anrufen ablesen kann: gewählte und empfangene Telefonnummern inklusive der Namen im Adressbuch, Dauer des Gesprächs und dergleichen. Auch der Standort des Handybesitzers bleibt dem Trojaner nicht verborgen, der auf Wunsch die Nummer der Funkbasisstation protokolliert, bei der das Handy gerade eingebucht ist. Ursprünglich wurde Flexispy entwickelt, um untreue Partner beim Fremdgehen zu ertappen; heute empfiehlt der Vertreiber in Deutschland das Programm «für Eltern, die Kontrolle möchten über das Handy ihrer Kinder» oder die ihre Sprösslinge «über das GPS Signal finden» wollen. Bleibt zu hoffen, dass die Ehe von Salomé und Klems lange hält und glücklich bleibt – oder dass sie bei einer Trennung zumindest nicht auf Schnüffelsoftware aus der illegalen Dunkelzone zurückgreifen.

Wo bin ich – und wo sind meine Daten?

In sozialen Netzwerken geben die User eine Menge an Daten preis, die unter Umständen auf wenig durchschaubaren Wegen an Dritte gelangen. So heisst es in der Datenschutzrichtlinie von Facebook Orte: «Wir können zudem Informationen über den Standort deines Computers oder Zugangsgeräts und dein Alter Anwendungen und Webseiten zur Verfügung stellen, damit sie angemessene Sicherheitsmassnahmen einführen und die Verbreitung von altersgemässen Inhalten kontrollieren können.» Genaue Informationen darüber, an wen genau und zu welchem Zweck Facebook die Angaben weitergibt, erhält der Nutzer nicht. Es wäre allerdings blauäugig anzunehmen, dass Facebookgründer Mark Zuckerberg dabei einzig den Schutz der User im Sinn hätte. Vielmehr sind die gesammelten Daten für das Marketing der unterschiedlichsten Firmen von grossem Wert. Diese greifen denn auch für einen Einblick in die Angaben und Mitteilungen von Internet-Surfen tief in die Tasche: Das Unternehmen Gnip hat sich auf das Sammeln öffentlich zugänglicher Daten auf Facebook, Twitter und anderen Plattformen spezialisiert und verkauft sie zu Marketingzwecken weiter. Wer die Hälfte aller getwitterten Botschaften lesen möchte, muss dafür 360 000 US-Dollar entrichten.

Im Unterschied zu zahlungskräftigen Firmen fällt es Privaten ungleich schwerer, selbst über ihr eigenes Datenportfolio Auskunft zu erhalten. Der österreichische Jusstudent Max Schrems beispielsweise musste dazu erst über die von ihm gegründete Initiative «Europe vs Facebook» Anzeige gegen das soziale Netzwerk erstatten. Dieses hatte sich nämlich geweigert, ihm Einsicht in die über ihn gesammelten Daten zu gewähren.



Der Inhalt der CD-ROM, die er daraufhin erhielt, füllte ausgedruckt 1222 Seiten und enthielt sogar sämtliche Einträge, die Schrems gelöscht zu haben glaubte.

Auch das Kulthandy iPhone war von einem handfesten Skandal betroffen. Im April 2011 flog auf, dass mit dem Betriebssystem iOS4 arbeitende iPhones und iPads die Bewegungsdaten der Geräte in einem lokalen File im Speicher des Handys aufzeichneten, so dass die Wege ihrer Nutzer anhand dieser Daten rekonstruiert werden konnten. In Südkorea, einem Land, dessen Einwohner neuen Kommunikationstechniken gegenüber durchaus aufgeschlossen sind, reichten immerhin 26 000 Betroffene Klage gegen Apple ein.

3 Persönliche Daten schützen

Die technischen Mittel für die Datenerhebung und -bearbeitung führen dazu, dass immer mehr persönliche Angaben gespeichert werden. Dass wir dabei noch die Kontrolle über unsere Daten behalten, ist nahezu ausgeschlossen – auch wenn uns Datenschutzgesetze Mittel dazu in die Hand geben. Im weltumspannend Internet allerdings sind nationale Gesetze vollends schwer um- und durchzusetzen.

Wie der Online-Alltag der Familie Christen zeigt, ermöglichen es die zahlreichen Datenbanken und Kommunikationsplattformen im Internet sogar Privaten ohne jegliche Befähigung zum Hacker, Lebensweg und Gewohnheiten Dritter auszuspionieren. Oberflächlich betrachtet, scheint solches Tun sogar rechtens: Immerhin hält die Bundesverfassung der Schweizerischen Eidgenossenschaft in Artikel 16 zur Meinungs- und Informationsfreiheit fest, alle hätten das Recht, «Informationen frei zu empfangen, aus allgemein zugänglichen Quellen zu beschaffen und zu verbreiten». Und das Schweizerische Datenschutzgesetz bekräftigt im dritten Abschnitt, bei der Bearbeitung von Personendaten durch Private liege keine Persönlichkeitsverletzung vor, «wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt» habe. Allerdings ist unter Juristen unumstritten, dass soziale Netzwerke nicht als allgemein zugängliche Plattformen zu gelten haben. Viele Einträge können nämlich nur von den anderen Netzwerksmitgliedern gelesen werden. Zudem bieten die Netzwerke selber ihren Nutzerinnen und Nutzern die Möglichkeit an, ihre Bilder und Postings vor Fremden zu verbergen.

Doch handelt es sich bei geographischen Positionsangaben überhaupt um Personendaten? Artikel 3 des Datenschutzgesetzes legt es nahe, diese Frage zu bejahen. Er definiert Personendaten als «Angaben, die sich auf eine bestimmte oder bestimmbare Person

beziehen». Angaben über regelmässig zurückgelegte Wegstrecken können so gesehen die Tätigkeit oder den Wohnort einer Person und damit letztlich ihre Identität offenbaren. Unter Umständen können geographische Positionsangaben sogar als «schützenswerte Personendaten» gelten – etwa, wenn Bilder, die in der Nähe einer politischen Veranstaltung aufgenommen wurden, zu Spekulationen über die Gesinnung der betreffenden Person anregen.

Garantierter Kontrollverlust

Ein grosses Problem steckt in der unbeschränkten Aufbewahrungsdauer der im Web veröffentlichten Informationen: Faktisch verlieren Personen, die über Jahre hinweg bloggen und Fotos veröffentlichen, den Überblick über ihre Daten. Ob diese aus dem ursprünglichen Zusammenhang gerissen und zu einem späteren Zeitpunkt an anderer Stelle im Internet wieder auftauchen, entzieht sich weitgehend ihrer Kontrolle.

Heikel ist zudem, dass auch Dritte Informationen und Fotos von ihren Bekannten veröffentlichen können – wie es bei Salomé und Klemens in der Fotosammlung von Patrick geschehen ist. Das Paar selber übt nämlich in seinen eigenen Blogs und Foto-Uploads durchaus Zurückhaltung. Die Portraits etwa, die beide in den sozialen Netzwerken veröffentlichen, zeigen nur einen Ausschnitt ihrer Gesichter: eine zurückgebundene Haarsträhne, ein lächelndes Auge, ein keckes Piercing.

Das Problem verschärft sich mit der technischen Entwicklung laufend: Mittlerweile existieren Programme zur Gesichtserkennung, die rasch grosse Mengen an Fotos scannen und einzelnen Individuen zuordnen. Die sozialen Netzwerke Google+ und Facebook haben bereits entsprechende Funktionen in ihr Angebot eingebunden. Die automatische Gesichtserkennung hat in



letzter Zeit beträchtliche Fortschritte erzielt, funktioniert aber noch nicht immer zuverlässig. Für die Betroffenen kann eine fehlerhafte Zuordnung von Bildern ebenso grosse Probleme aufwerfen wie ein lückenloses und korrektes Profil, das Rückschlüsse auf ihre Lebensführung zulässt.

Abstinenz ist auch keine Lösung

Vordergründig kann sich der oder die Einzelne durch die Weigerung schützen, persönliche Daten auf Informations- und Kommunikationsplattformen zu publizieren: Wer sozialen Netzwerken fern bleibt, gibt dort auch keine Informationen preis. Allerdings verrät auch die kommunikative Enthaltsamkeit viel über einen Menschen und kann zu seinem Nachteil ausgelegt werden. Personalmanager, die vor dem Einstellungsgespräch bei den gängigen sozialen Netzwerken erfolglos nach Informationen über den Kandidaten fahnden, könnten vermuten, der Betreffende habe etwas zu verbergen oder sei zumindest ein misstrauischer Zeitgenosse von eingeschränkter Teamfähigkeit. Somit können sogar fehlende Spuren im Internet zur Diskriminierung einer Person führen.

Kommt dazu, dass immer mehr Ortungsdaten im öffentlichen Raum anfallen – etwa, wenn Videokameras installiert werden, um kriminellen Handlungen oder Vandalismus vorzubeugen. Einer solchen Lokalisierung des Aufenthaltsortes kann sich nur entziehen, wer die entsprechenden Stätten meidet; damit wird letztlich aber das in der Bundesverfassung festgeschriebene Grundrecht auf Bewegungsfreiheit beschnitten.

Rechtlich fragwürdige Zweckentfremdung

Der in Artikel 4 des schweizerischen Datenschutzgesetzes aufgeführte Grundsatz der Zweckbindung

besagt, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, «der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist». Nimmt man diesen Grundsatz wörtlich, agieren die meisten sozialen Netze fragwürdig. Denn der User teilt seine Daten mit, um mit seinen «Freunden» in Verbindung zu treten und Nachrichten auszutauschen; dass das Geschäftsprinzip der Plattform darauf beruht, die Daten zu Marketingzwecken zu verkaufen, ist für den Laien «aus den Umständen» nicht ohne weiteres ersichtlich.

Allerdings rechtfertigen Facebook und Co mit ausführlichen und nicht immer gut verständlichen allgemeinen Geschäftsbedingungen die Weitergabe der Daten etwa damit, dass Minderjährige geschützt werden sollen und das Informationsangebot Dritter auf die Interessen der Nutzerinnen und Nutzer zugeschnitten werden soll. Faktisch bedingen sich die sozialen Netzwerke aus, dass die User auf den Schutz ihrer Persönlichkeitsdaten verzichten. Ob diese Einwilligungserklärung rechtsgültig ist, wird von Datenschützern zumindest angezweifelt. Und selbst wenn die Nutzer im Zusammenhang mit anderen Applikationen, zum Beispiel auf dem iPhone, ihren Standort bekannt geben, erteilen sie damit dem Empfänger keinen Freipass für eine beliebige Weiterverwendung der Daten.

Überall Durchsetzungsdefizite

Im Prinzip gibt das schweizerische Datenschutzgesetz Personen, die ihr Recht nach Persönlichkeitsschutz verletzt sehen, verschiedene Mittel in die Hand, um sich zu wehren. So kann die klagende Partei verlangen, dass die Datenbearbeitung gesperrt wird, keine Daten mehr weitergereicht werden oder dass Personendaten richtig gestellt oder vernichtet werden. Die Berufung auf ein nationales Datenschutzgesetz vermag international

operierende Anbieter wie Facebook oder Google allerdings kaum zu beeindrucken; Max Schrems konnte das soziale Netzwerk erst zur Herausgabe seiner Daten bewegen, als er eine öffentlichkeitswirksame Initiative lancierte und von der irischen Behörde Sukkurs erhielt, die in Europa in diesem Fall für den Datenschutz zuständig ist – der europäische Sitz von Facebook befindet sich in Dublin. Der drohende Imageschaden dürfte Facebook nicht weniger zum Einlenken bewogen haben als die rechtlichen Argumente.

Oft ist es allerdings gerade der Wunsch nach Diskretion, der Betroffene davon abhält, sich gegen Verletzungen ihrer Persönlichkeitsrechte zu wehren und auf dem Schutz ihrer Daten zu beharren. Denn eine juristische Auseinandersetzung führt mitunter dazu, dass der Kläger die Informationen, die er lieber verschweigen möchte, noch breiteren Kreisen zugänglich machen muss, als es ohne Rechtsstreit der Fall wäre.

Globale Kommunikation erfordert globalen Schutz

Viele datenschutzrechtliche Unklarheiten ergeben sich aus der Frage, inwiefern das schweizerische Datenschutzgesetz überhaupt anwendbar ist, wenn ein Anbieter Daten erhebt, der aus dem Ausland aus agiert. Juristen gehen davon aus, dass der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) intervenieren kann, wenn in der Schweiz selber Daten bearbeitet werden. Ob diese Voraussetzung aber bei sozialen Netzwerken, die vom Ausland aus operieren, erfüllt ist, gilt unter Juristen zumindest als strittig. Bei internationalen Streitfällen muss zudem die Frage der Zuständigkeit geklärt werden.

Auf europäischer Ebene sind derzeit Bestrebungen für einen stärkeren Datenschutz im Gang. So bemängelt die EU-Kommission insbesondere die in Online-

umgebungen oft unklaren, schwierig zu findenden und intransparenten Datenschutzhinweise. Ferner fordert sie bessere Kontrollrechte für Personen, die von der Datenbearbeitung betroffen sind. Im Hinblick auf geographische Positionsangaben empfiehlt ein beratendes Gremium der EU-Kommission, dass Ortungsdienste standardmässig – d.h. in der Voreinstellung – abgeschaltet sein müssen. Zudem sollten Personen, die der Verwendung «ihrer» Ortungsdaten zugestimmt haben, ihre Einwilligung jährlich wiederholen müssen und diese sehr einfach widerrufen können. Für Ortungsfunktionalitäten, die dem Nutzer nicht bewusst sind, müssten die Anbieter verpflichtet werden, ein ständiges Warnzeichen aufzuschalten.

Die Schweiz ist durch die so genannten Dublin- und Schengenassoziiierungen verpflichtet, verschiedene datenschutzrechtlich relevante EU-Rechtsakte anzuwenden. Modifikationen, die das EU-Recht mit Blick auf die neuen technischen Möglichkeiten vorsieht, hätten demnach auch für die Schweiz Gültigkeit. Dies würde bedeuten, dass auch in der Schweiz die Datenschutzrechte betroffener Personen gegenüber den Datenbearbeitern gestärkt würden – eine Entwicklung, die bestimmt auch die Zustimmung von Salomé und Klemens fände. Die Zurückhaltung, die sie bei den Einstellungen ihrer Netzwerk-Konten üben, indem sie die Angaben zu Wohnort und Telefonnummer nur für Freunde sichtbar veröffentlichen, lässt jedenfalls darauf schliessen, dass ihnen der Schutz ihrer persönlichen Daten am Herzen liegt.

Das Internet lebt von der fortlaufenden und raschen Aktualisierung seiner Inhalte. Auch die sozialen Netzwerke passen ihre Angebote ständig an und verändern dabei auch oft die Formularmasken, die man ausfüllen muss, um zu bestimmen, wer welche Informationen sieht. Tipps für die Privacy-Einstellungen und für sichere Kommunikation im Web sind bspw. zu finden unter: www.datenschutz.ch
www.bsi-fuer-buerger.de
www.cnpd.public.lu
 (Commission Nationale pour la Protection des Données du Grand-Duché de Luxembourg)
www.europe-v-facebook.org/DE/de.html

Report information

Device name: -VAIO
 Sent at: 2012-02-02 07:30:59 UTC
 User agent: Prey/0.5.3 (windows)

Network information

Remote IP: 83.77.107.153

Reports from -VAIO (8)

-VAIO has space for 2 additional reports. Once it runs out, older reports will be deleted when new ones arrive.

#41110630 from -VAIO - 2 months ago
 #41108881 from -VAIO - 2 months ago
 #39105525 from -VAIO - 2 months ago
 #39102695 from VAIO - 2 months ago
 #39100028 from -VAIO - 2 months ago
 #39064539 from VAIO - 2 months ago
 #39062177 from -VAIO - 2 months ago
 #39059878 from -VAIO - 2 months ago

Delete this report

« View all reports (8)

Location



Screenshot



Logged User

Studie «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern»

Begleitgruppe

- Dr. Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich TA-SWISS-Leitungsausschuss (Präsident der Begleitgruppe)
- Florence Bettschart, Fédération romande des consommateurs (FRC), Lausanne
- Alain Buogo, Bundesamt für Landestopografie swisstopo, Wabern
- Dr. Christine Giger, Giger GeoIT, Embrach
- Prof. Dr. Gudela Grote, ETHZ, Arbeits- und Organisationspsychologie, Zürich
- Dr. Jessica Heesen, Eberhard Karls Universität, Tübingen
- Rainer Humbel, Bundesamt für Statistik, Neuenburg
- Thomas Kallweit, FELA Management AG, Diessenhofen
- Dr. Francisco Klauser, Institut Vermessung und Geoinformation, geographisches Institut, Universität Neuenburg
- Michael Kocheisen, Swisscom Innovation Competence Center, Swisscom (Schweiz) AG, Bern
- Ulrich Lattmann, Schweizerische Akademie der Technischen Wissenschaften SATW, Zürich
- Urs Luther, Bundesamt für Strassen ASTRA, Bern
- Franziska Meister, Die Wochenzeitung, Zürich
- Cyrill Osterwalder, Google Schweiz, Zürich
- Hans Kaspar Schiesser, Verband öffentlicher Verkehr, Bern
- Philipp Stüssi, Eidgenössischer Datenschutzbeauftragter, Bern
- Prof. Dr. Rolf H. Weber, Zentrum für Informations- und Kommunikationsrecht, Universität Zürich, Zürich
- Dr. Franz Zeller, Bundesamt für Kommunikation BAKOM, Biel

TA-SWISS-Projekt-Betreuer

- Dr. Sergio Bellucci, TA-SWISS, Bern
- Nadia Ben Zbir, TA-SWISS, Bern

Impressum

TA-SWISS (Hrsg.) Geographische Wegmarken in der Cyberwelt. Ortungstechnologien als Herausforderung für eine offene Gesellschaft.

Kurzfassung der Studie von TA-SWISS «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern», Bern 2012.

TA 57A/2012.

Autorin: Lucienne Rey, Bern

Redaktion: Christine D'Anna-Huber, TA-SWISS

Gestaltung: Hannes Saxer, Bern

Fotos: Lucienne Rey

Druck: Jordi AG – Das Medienhaus, CH-3123 Belp

TA-SWISS – Zentrum für Technologiefolgen-Abschätzung

Neue Technologien bieten oftmals entscheidende Verbesserungen für die Lebensqualität. Zugleich bergen sie mitunter aber auch neuartige Risiken, deren Folgen sich nicht immer von vornherein absehen lassen. Das Zentrum für Technologiefolgen-Abschätzung TA-SWISS untersucht die Chancen und Risiken neuer technologischer Entwicklungen in den Bereichen «Biotechnologie und Medizin», «Informationsgesellschaft», «Nanotechnologien» und «Mobilität/Energie/Klima». Seine Studien richten sich sowohl an die Entscheidungstragenden in Politik und Wirtschaft als auch an die breite Öffentlichkeit. Ausserdem fördert TA-SWISS den Informations- und Meinungsaustausch zwischen Fachleuten aus Wissenschaft, Wirtschaft, Politik und der breiten Bevölkerung durch Mitwirkungsverfahren (zum Beispiel PubliForen und publifocus). Die Studien von TA-SWISS sollen möglichst sachliche, unabhängige und breit abgestützte Informationen zu den Chancen und Risiken neuer Technologien vermitteln. Deshalb werden sie in Absprache mit themenspezifisch zusammengesetzten Expertengruppen erarbeitet. Durch die Fachkompetenz ihrer Mitglieder decken diese so genannten Begleitgruppen eine breite Palette von Aspekten der untersuchten Thematik ab.

TA-SWISS ist ein Kompetenzzentrum der Akademien der Wissenschaften Schweiz.



Zentrum für Technologiefolgen-Abschätzung
Brunngasse 36
CH-3011 Bern
info@ta-swiss.ch
www.ta-swiss.ch

a⁺ Ein Kompetenzzentrum der
Akademien der Wissenschaften Schweiz



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Strassen ASTRA

Bundesamt für Statistik BFS

Bundesamt für Landestopografie swisstopo