Geo-Location: Das Wo im Netz

Autor: David Pachali

Immer mehr Dienste im Netz verwenden ortsbezogene Daten. Welche Technik steckt dahinter, wie werden die Daten verwendet und wie kann man die Verwendung kontrollieren?

Geodaten werden im Netz immer wichtiger. Schon lange werden zum Beispiel Fotos von Nutzern mit den Koordinaten des Aufnahmeortes versehen, aktuelle Kameras machen das ganz automatisch. Aber auch viele weitere Inhalte und Daten werden mit Geo-Koordinaten verknüpft. Bei standortbezogenen Diensten wie Foursquare, bei denen Nutzer aktiv ihren aktuellen Aufenthaltsort veröffentlichen und zum Beispiel „Bürgermeister" eines Ortes werden, hat das noch eher spielerischen Charakter. Andere Dienste wie die Kriseninformations-Plattform Ushahidi zeigen darüber hinaus, welcher enorme Nutzen aus der Kombination von Geodaten mit dem freiwilligen Datensammeln durch Viele entstehen kann. Nach der Tsunami-Katastrophe in Japan etwa trugen Nutzer dort Meldungen über Vermisste und die Versorgungslage vor Ort per SMS, Smartphone oder Karteneintrag über das Web zusammen (vgl. www.sinsai.info).

Umgekehrt hängt auch das, was wir vom Internet zu sehen bekommen, zunehmend vom eigenen Standort ab. Wohl jeder kennt (vgl. www.klicksafe.de/irights – Text 19) die Meldung „Dieses Video ist in deinem Land nicht verfügbar". Die Ergebnisse von Suchanfragen sind ebenfalls je nach Standort des Nutzers unterschiedlich. Wenn Dienste Geodaten berücksichtigen, ist das häufig hilfreich, indem sie passgenauere Informationen liefern – ein Trend, der durch das mobile Internet noch verstärkt wird. Wer etwa mobil nach dem Wort „Café" sucht, bekommt dann vor allem Treffer in seiner Stadt angezeigt, die gleiche Suche am Schreibtisch führt auf allgemeinere Informationen zum Thema. Zugleich entstehen unweigerlich noch mehr Daten über die Nutzer, deren Verwendung sie kaum mehr kontrollieren können. Die Wissenschaftler Jerome Dobson und Peter Fisher prägten den Begriff „Geo-Slavery" (vgl. http://dusk.geo.orst.edu/virtual/2005/geoslavery.pdf), um auf die Gefahrenseite – etwa durch neue Überwachungsmöglichkeiten – hinzuweisen.

Wie Nutzer geortet werden

Es gibt verschiedene Techniken, mit denen ortsbezogene Daten ermittelt werden – streng genommen wird dabei natürlich nie der jeweilige Nutzer selbst, sondern immer das zugehörige Gerät mit mehr oder weniger großer Genauigkeit geographisch bestimmt.

Lokalisierung per IP-Adresse

Viele Dienste ziehen die IP-Adresse eines Nutzers heran, die zumindest eine sehr grobe geographische Orientierung ermöglicht. IP-Adressen – die Nummern, die jeder Computer im Internet zugewiesen bekommt – lassen zumindest das Land, aus dem ein Nutzer eine Website oder einen Dienst aufruft, erkennen, häufig auch die Region oder die Stadt. Die meisten Internet-Provider vergeben täglich neue („dynamische") IP-Adressen an Endnutzer. Weil die Provider diese Adressen aber wiederum in Blöcken zugewiesen bekommen und sie diese meist für bestimmte regionale Einwahlknoten nutzen, lässt sich der Standort eines Nutzers dennoch mit hoher Wahrscheinlichkeit bestimmen.

Geo-Lokalisierung mittels IP-Adresse kommt in vielen Bereichen zum Einsatz. Download- und Streaming-Plattformen setzen entsprechende Techniken ein, um zu steuern, in welchen Ländern die Inhalte verfügbar sind. Ein weiterer großer Einsatzbereich sind Werbe-Einblendungen auf Webseiten oder Suchmaschinen, die zusammen mit weiteren Daten ebenfalls den Standort des Nutzers berücksichtigen können. Auch Banken und Online-Zahlungsdienste nutzen die Geo-Lokalisierung, um verdächtige Muster zu erkennen oder Transaktionen aus bestimmten Ländern ganz zu verhindern.

GPS, Funkzellen und WLAN-Netze

Das Satelliten-Navigationssystem GPS ist aus Navigationsgeräten bei Autos bekannt, auch in Handys findet sich häufig ein Empfänger. GPS ist eine amerikanische Entwicklung; Europa arbeitet mit dem „Galileo"-Programm an einem ähnlichen System, das jedoch noch nicht in Betrieb ist. Ortungsdienste bei Smartphones basieren je nach Dienst und Geräte-Einstellungen neben GPS auch auf den Daten der jeweiligen Mobilfunkzellen und den Signalen von WLAN-Netzwerken.

Weil letztere vor allen in städtischen Gebieten nahezu flächendeckend anzutreffen sind, lassen sie sich zur Positionsbestimmung einsetzen, indem das Telefon oder der Laptop nachsieht, welche WLAN-Netz in der Nähe sind (Beispielkarte vgl. http://wigle.net/gps/gps/Map/onlinemap2/?maplat=52.51562020180085&maplon=13.382635116576475&mapzoom=15&useosm=on). Der eigentliche WLAN-Zugang selbst wird dabei gar nicht genutzt. Der Vorteil: Sind viele Netze vorhanden, ist diese Methode sehr präzise und funktioniert auch innerhalb von Gebäuden.

Den Standort ändern: VPN- und Proxy-Dienste

Viele Nutzer verwenden mittlerweile VPN-Dienste (Virtual Private Network, vgl. www.virenschutz.info/Netzwerke-VPN-vpn-2.html), um die IP-basierten Geosperren von Streaming-Diensten zu umgehen. Mit ihnen lassen sich Streams anschauen, die in

Deutschland eigentlich nicht verfügbar sind. So kommt die neue Staffel der Lieblingsserie im Original zum heimischen Bildschirm, die hierzulande womöglich erst Jahre später offiziell zu haben ist. Hintergrund: Die Rechte für die Sendungen werden jeweils national vergeben, entsprechend komplex und langwierig können sich die Lizenzverhandlungen im europäischen Markt gestalten.

VPN-Dienste leiten den Datenstrom vom eigenen Rechner durch einen digitalen Tunnel weiter. Für einen Streamingdienst sieht es dann zum Beispiel so aus, als stünde der eigene Rechner in einem anderen Land – dort, wo der Ausgang des Tunnels ist, denn der Datenverkehr dazwischen ist verschlüsselt und für Dritte nicht ohne Weiteres einsehbar. Ein ähnliches Ergebnis wird mit Proxy-Diensten erzielt, also zwischengeschalteten Rechnern, die den Datenverkehr hin und her reichen. Webseiten oder Browser-Erweiterungen, die zum Beispiel die Ländersperren bei YouTube umgehen, beruhen darauf.

Ist Geosperren umgehen legal?

Zunächst handelt es sich sowohl bei VPN- als auch bei Proxy-Diensten um legale Werkzeuge, die jedermann einsetzen darf. Weder im deutschen Urheberrecht noch durch andere Gesetze ist es verboten, solche Dienste zu nutzen. Umgekehrt bleiben illegale Nutzungen wie z. B. das Anbieten urheberrechtlich geschützter Filme oder Musik über Torrent-Systeme illegal – unabhängig davon, welche Werkzeuge man dabei einsetzt.

Darf man VPN-Dienste aber nutzen, um Geosperren für die Nutzung legaler Dienste – wie zum Beispiel Hulu, YouTube & Co. – zu umgehen? Eine hundertprozentig eindeutige Antwort darauf gibt es leider nicht. Manche Rechtsexperten vertreten die Ansicht, dass Geosperren als „wirksame technische Schutzmaßnahme" mit einem Kopierschutz vergleichbar sind. Solche Schutzmaßnahmen darf man nach einer Norm im Urheberrechtsgesetz nicht umgehen (vgl. http://dejure.org/gesetze/UrhG/95a.html). Spitzt man diese Argumentation weiter zu, könnte der Nutzer das Urheberrecht verletzen, weil beim Anschauen eines solchen Streams eine „flüchtige" Kopie im Arbeitsspeicher entsteht. Solche „flüchtigen" Kopien entstehen bei digitalen Diensten unausweichlich und sind durch eine weitere Regel für sogenannte „vorübergehende Vervielfältigungshandlungen" auch weitgehend erlaubt (vgl. http://dejure.org/gesetze/UrhG/44a.html). Manche Vertreter der Rechteinhaber könnten aber womöglich argumentieren, dass die Regel in diesem Fall nicht greift.

Die gegenteilige Ansicht anderer Experten besagt, dass Geosperren gar nicht unter die Regelung für „wirksame technische Schutzmaßnahmen" fallen. Im Zweifel wäre es

auch fraglich, wer tatsächlich Verwertungsrechte gegenüber Nutzern geltend machen würde, da die entsprechenden Rechte – etwa bei den Streamingdiensten für Serien – noch gar nicht für Deutschland vergeben wurden. Eine andere Frage ist es, ob ein Nutzer die Geschäftsbedingungen eines Anbieters verletzt, wenn er die Dienste aus anderen Ländern nutzt. Wo es solche Klauseln gibt, könnte ein Dienst aus diesem Grund dann das Konto kündigen. Dafür muss man den Bedingungen jedoch wirksam zugestimmt haben, etwa beim Anlegen eines Benutzerkontos. Die bloße Nutzung eines Dienstes ohne Registrierung gehört noch nicht dazu, obwohl einige Dienste das in ihren AGB behaupten.

Bislang sind solche Fragen jedoch nur theoretische Diskussionen. Gerichtsentscheidungen und Auseinandersetzungen dazu sind nicht bekannt, für Nutzer droht diesbezüglich im Moment kein Risiko. VPN-und Proxy-Dienste machen es Dritten auch naturgemäß schwierig, entsprechende Nutzungen festzustellen. So oder so: Eindeutig illegale Handlungen verbieten sich auch bei VPN-Diensten; das Umgehen von Geosperren gehört aber nicht dazu.

Wie Standortdaten genutzt werden

Bei geosozialen Netzwerken wie etwa Foursquare ist der „Deal" für die Nutzer noch relativ gut erkennbar: Sie geben ihre Standortdaten bekannt, die Dienste verwerten sie und können die Daten zum Beispiel an lokale Unternehmen weitergeben, die wiederum mit Rabatten und ähnlichen Belohnungen für häufige Besucher werben. Die beteiligten Firmen wiederum gewinnen Informationen über ihre Kunden. Der Nutzer kann entscheiden, ob ihm das Modell zusagt oder nicht.

Einen Haken hat die Sache manchmal dennoch: Einige Dienste sammeln Standortdaten über das notwendige Maß hinaus. „Sie speichern die Standortdaten oft unentwegt, ohne dass der Nutzer das weiß und eine solche Datenerhebung ausdrücklich erlaubt hat", stellt das Projekt „Surfer haben Rechte" (vgl. www.surfer-haben-rechte.de/cps/rde/xchg/digitalrechte/hs.xsl/1535.htm) fest. Dort findet sich auch eine Checkliste (vgl. www.surfer-haben-rechte.de/cps/rde/xbcr/digitalrechte/Checkliste_Lokalisierungsdienste.pdf) darüber, was Nutzer von Lokalisierungsdiensten beachten sollten.

Vage Klauseln auch bei Standortdaten

Undurchsichtiger wird es für Nutzer bei jenen Unternehmen, die neben vielen anderen Daten *auch* Standortdaten erheben. So heißt es in der Datenschutzerklärung von Google, dass bei der Verwendung standortbezogener Dienste „möglicherweise Informationen über Ihren tatsächlichen Standort" erhoben und verarbeitet werden. „Unter

Umständen" können dann solche und andere personenbezogenen Daten mit denen von anderen Diensten des Unternehmens verknüpft werden, so die Erklärung weiter (Stand 24.06.2013, vgl. www.google.de/intl/de/policies/privacy).

Solche Formulierungen sind jedoch zu vage, kritisieren Verbraucherschützer. Sie halten die Bestimmungen für rechtswidrig; es sei nicht klar, wozu genau der Nutzer eigentlich seine Zustimmung gibt. Ähnlich sieht es im Fall von Apple aus. Nach dessen Datenschutzerklärung (Stand 21.05.2012, vgl. www.apple.com/de/privacy) kann das Unternehmen ebenso wie weitere „Partner und Lizenznehmer präzise Standortdaten erheben, nutzen und weitergeben, einschließlich des geographischen Standorts deines Apple Computers oder Geräts in Echtzeit".

Das Landgericht Berlin hat im Mai einer Klage des Verbraucherzentrale Bundesverbands gegen diese und weitere Klauseln in Apples Datenschutzbestimmungen stattgegeben. Trotz der zugesicherten Anonymisierung müsse der Nutzer im Zweifel davon ausgehen, dass die erhobenen Daten auf einzelne Personen beziehbar seien, so die Richter in dem noch nicht rechtskräftigen Urteil (vgl. www.vzbv.de/cps/rde/xbcr/vzbv/Urteil_des_LG_Berlin_zur_Datenschutzrichtlinie_von_Apple.pdf).

Anonyme Daten sind weniger anonym als gedacht

Viele Dienste erheben Ortungsdaten in anonymisierter Form – welcher konkrete Nutzer wann und wo gewesen ist, wird also nicht mitgespeichert. Tatsächlich interessieren sich die Unternehmen in der Regel nicht für die individuellen Daten eines Nutzers. Wo sich ein einzelner Nutzer konkret aufhält, wie sein konkretes Bewegungsprofil aussieht, ist für die meisten „Datenkraken" nicht interessant. Für sie ist es eines unter vielen anderen Merkmalen, aus denen komplexe statistische Gruppen gebildet werden. Hier setzen dann weitere Auswertungsschritte – Informatiker sprechen auch von „Klassifikatoren" – an, anhand derer die Dienste personalisiert und etwa spezifische Werbeeinblendungen ausgewählt werden.

Auf den ersten Blick geht eine einzelne Information wie der Standort eines Nutzers also im allgemeinen Datenwust unter. Auf den zweiten Blick sind anonyme Daten gar nicht so anonym: Sie lassen sich zum Beispiel mit weiteren Datenbeständen kombinieren und so wieder einzelnen Nutzern zuordnen. Auch durch besonders charakteristische Muster lassen sich anonyme Nutzungsdaten wieder ent-anonymisieren. Forscher des MIT untersuchten etwa einen Datensatz eines europäischen Telefonanbieters und demonstrierten, dass aus anonymisierten Ortungsdaten mehr als neun von zehn Nutzern – also praktisch alle Teilnehmer – wieder identifiziert werden können, wenn man

den Aufenthaltsort zu vier Zeitpunkten an einem Tag kennt (vgl. www.nature.com/srep/2013/130325/srep01376/full/srep01376.html).

Wenn man sich als Nutzer dafür entscheidet, Ortungsdienste zu nutzen, ist man daher gut beraten, auch vermeintlich anonymisierte Daten so zu behandeln, als ob sie das nicht sind. Der Unterschied zwischen anonymen und nicht-anonymen Daten ist am Ende geringer, als es auf den ersten Blick erscheint.

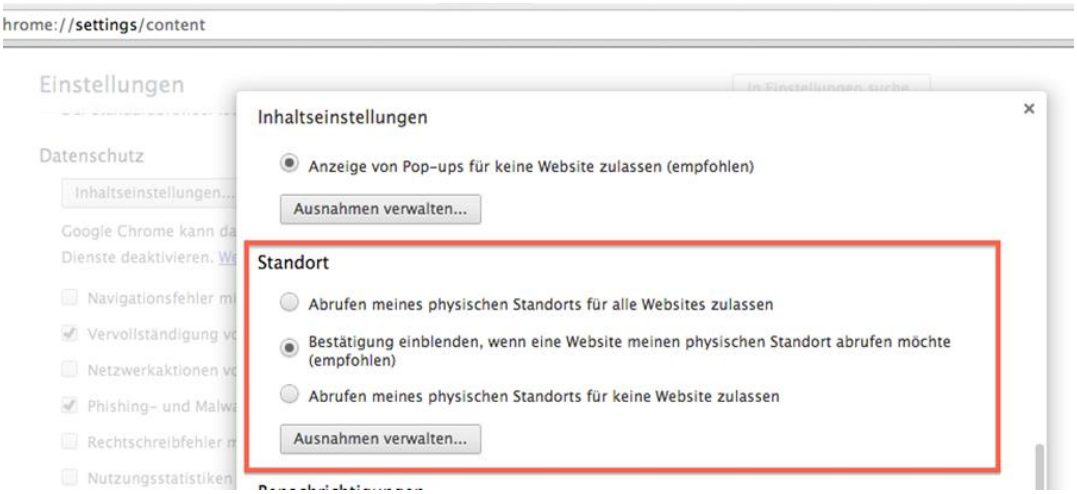
Standortdaten kontrollieren

Nach den deutschen und europäischen Datenschutzgesetzen haben Nutzer das Recht zu erfahren, was Unternehmen über sie speichern. Sie können der weiteren Nutzung ihrer Daten widersprechen und Daten gegebenenfalls etwa auch sperren oder löschen lassen. Allerdings: In der Praxis kommt man als Nutzer häufig nicht besonders weit, diesen Anspruch tatsächlich auch umzusetzen. So oder so: Wer die Geo-Spuren, die er im Netz hinterlässt, bewusst kontrollieren will, muss mittlerweile eine Vielzahl von Einstellungen vornehmen, Häkchen setzen oder abwählen und regelmäßig prüfen, ob auch alles noch so läuft, wie vorgesehen – und die Dienste nicht etwa über Nacht re-noviert haben.

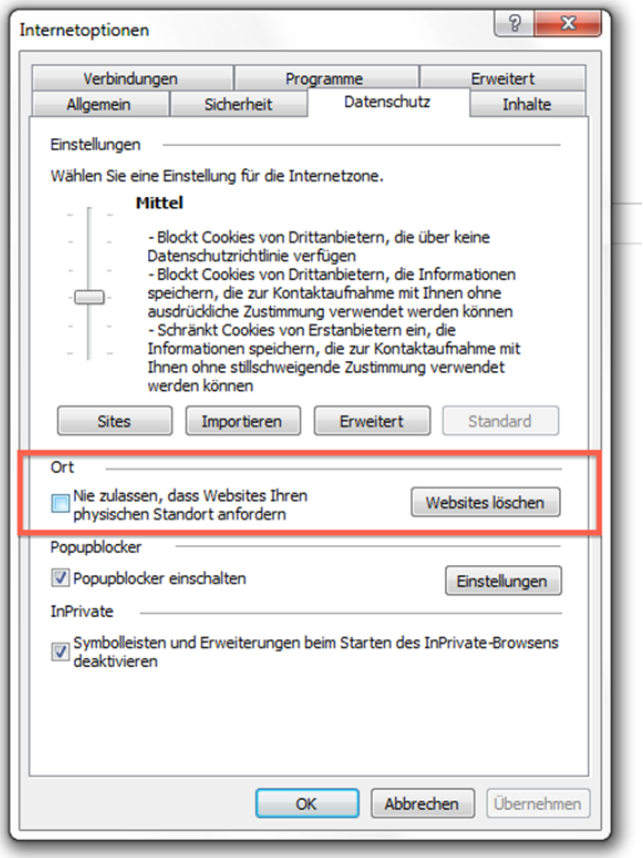
Einstellungen im Webbrowser

Neben den Einstellungen bei Plattformen wie Facebook & Co. ist der Browser die erste Anlaufstelle, um einzustellen, wann welche Standortdaten genutzt werden dürfen. Wichtig: Diese Einstellungen beziehen sich nur auf Ortungsfunktionen, die allgemeine geographische Schätzung etwa über die IP-Adresse ist davon unberührt.

- Im Chrome-Browser befindet sich die Einstellungsmöglichkeit in den erweiterten Einstellungen unter dem Button „Inhaltseinstellungen". Dort kann man einstellen, ob Standortdaten generell, gar nicht oder im Einzelfall abgefragt werden dürfen:

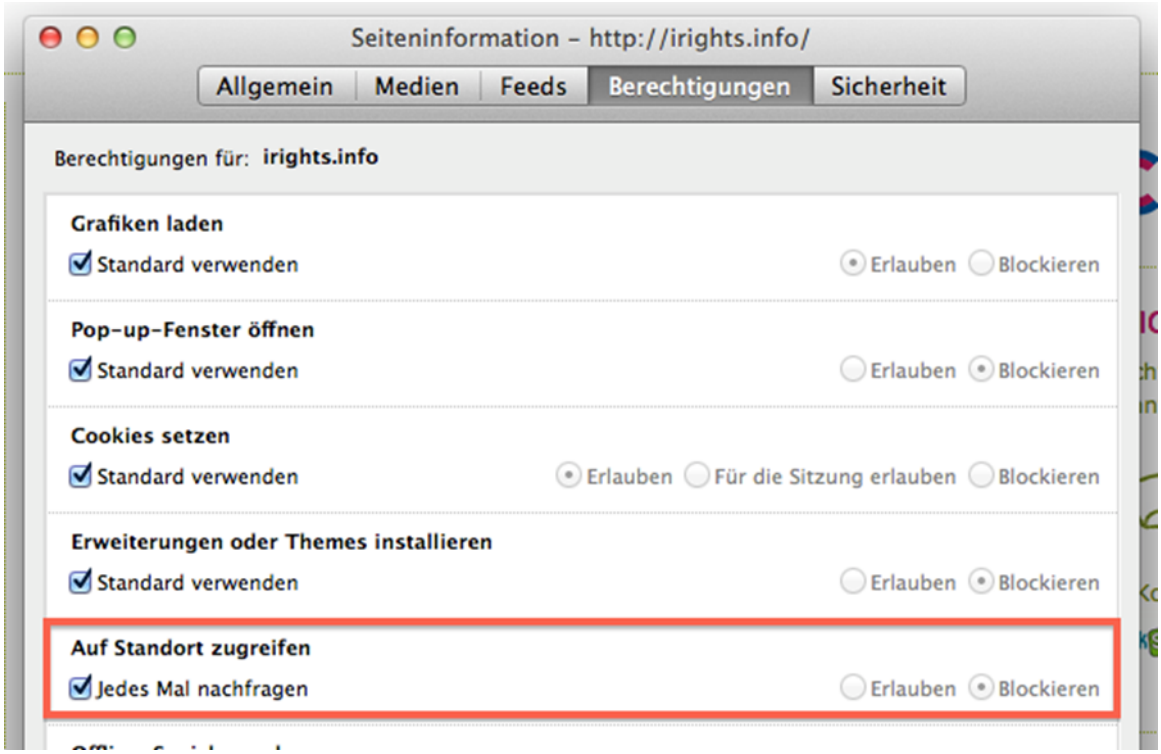


- Nutzer des Internet Explorers finden die Einstellung in der Version 9, indem sie auf das Zahnrad klicken und in den „Internetoptionen" im Menüpunkt „Ort" die Standort-Abfrage aktivieren oder abwählen:



- Eine ähnliche Einstellung findet sich in den Einstellungen des Safari-Browsers unter dem Punkt „Datenschutz":

- Im Firefox-Browser sind die Einstellungen etwas komplizierter vorzunehmen. Sie finden sich nicht unter „Einstellungen", sondern im Menüpunkt „Extras" unter dem Reiter „Berechtigungen". Allerdings gilt das nur für die Seite, die man aktuell geöffnet hat. Die Einstellung erscheint auch dann, wenn die Seite gar keine Standortdaten abfragt – wie etwa hier am Beispiel von iRights.info:



- Will man Standortdaten hingegen dauerhaft ab- oder anschalten, muss man „about:config" in die Firefox-Adresszeile eingeben, gegebenenfalls in der folgenden Warnmeldung „Ich werde vorsichtig sein, versprochen" bestätigen und auf den Einstellungsnamen „geo-enabled" doppelklicken.

Anwendungen bei Smartphones und Tablets

Auf Smartphones oder Tablets lassen sich zumindest die Ortungsdienste bei Anwendungen kontrollieren – häufig aber mehr schlecht als recht, wie die Stiftung Warentest in einer aktuellen Untersuchung festgestellt hat (vgl. www.test.de/Smartphones-Der-Datenschutz-im-Test-4542585-0, Artikelabruf kostenpflichtig). Unter den gängigen mobilen Betriebssystemen bietet demnach nur Apples iOS die Möglichkeit, den Zugriff auf Ortungsdienste pro Anwendung zu justieren. Allerdings monieren die Tester, dass der Nutzer eine Funktion erst wieder abschalten muss, mit der das Gerät Standortdaten durchgängig an Apple sendet. Bei Android- und Windows-Geräten hingegen herrsche „Friss oder stirb": Eine Feinjustierung der Zugriffe auf Ortungsdaten durch Anwendun-

gen ist nicht vorgesehen. Schaltet man die Ortungsdienste wiederum ganz ab, verliert man auch gewünschte Funktionen, etwa bei Kartendiensten.

Bei mobilen Geräten empfiehlt es sich in jedem Fall, vor dem Installieren zu prüfen, welche Rechte man Anwendungen erteilt und abzuwägen, ob eine Installation notwendig ist. Auch nach dem Einspielen von Updates sollte man prüfen, ob die Zugriffsmöglichkeiten erweitert wurden. Das Problem derzeit: Kein Nutzer kann sich durch hunderte von Seiten an Nutzungsbedingungen aller genutzten Anwendungen wühlen, um mögliche Schnüffel-Apps zu erkennen. Tatsächlich nutzen deutlich mehr Anwendungen Standort- und andere Daten von Nutzern, als die meisten – zum Beispiel bei Spielen – wohl vermuten würden. Häufig werden diese auch an Dritte weitergegeben, wie etwa Auswertungen des Wall Street Journal (vgl. http://blogs.wsj.com/wtk-mobile) über eine Vielzahl an Apps zeigen.

Hier ist die Situation also bis auf Weiteres unübersichtlich. Abzuwarten bleibt, ob die derzeit in Brüssel erarbeitete EU-Datenschutzreform die Situation für Nutzer verbessert. Die Ansätze dafür – zum Beispiel eine klare und informierte Einwilligung, welche Daten die Dienste wie nutzen oder datenschutzfreundliche Voreinstellungen – sind zumindest vorhanden.