International Working Group
on Data Protection
in Telecommunications

675.51.14

Arbeitspapier
zur Verfolgung des Aufenthaltsortes auf der Basis von Meldungen von Mobilfunkgeräten

58. Sitzung, 13.-14. Oktober 2015, Berlin (Deutschland)

– Übersetzung –

Anwendungsbereich

1. Die Arbeitsgruppe hat bereits früher Risiken für die „*Aufzeichnung des Aufenthaltsortes und andere personenbezogenen Daten über Netzwerknutzer*“[1] identifiziert. Sie hat einen gemeinsamen Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten verabschiedet[2] und die Nutzung von „Deep Packet Inspection“ für Werbezwecke erörtert[3].

2. Dieses Arbeitspapier untersucht insbesondere die Risiken für Datenschutz und Privatsphäre, die mit der Erhebung von gerätebezogenen Informationen und der Ableitung von Aufenthaltsinformationen aus Verkehrsdaten zusammenhängen. Ein Beispiel bildet die Nutzung von Wi-Fi „probe requests“, die von Geräten wie Smartphones stammen, für die Analyse von Kundenfrequenz und Verkehrswegen im Einzelhandel.

Hintergrund

3. Kommunikationsnetzwerke erfordern die regelmäßige Aussendung bestimmter Datenpakete, um Netzwerk-Controller oder andere Geräten im Netzwerk aufzufinden oder eine Verbindung mit diesen aufrecht zu erhalten. Darüber hinaus muss den Geräten eine eindeutige Adresse zugewiesen werden, um sie in dem Netzwerk unterscheiden zu können, so dass Datenpakete von und zu dem richtigen Gerät gesendet werden können.

4. Eine einzelne drahtlose Basisstation (d. h. ein Sender und Empfänger), wie eine Mobilfunk-Basisstation oder ein Wi-Fi-Zugangspunkt, hat eine bestimmte Reichweite. Außerhalb dieser Reichweite (oder der Reichweite eines Signalverstärkers) können das Endgerät und die Basisstation nicht miteinander kommunizieren. Eine einzelne Basisstation ist mit kompatiblen Geräten in Reichweite verbunden und empfängt dabei Signale von dem Gerät (unter der An-

[1] Arbeitspapier zu potenziellen Risiken drahtloser Netzwerke – Allgemeine Empfehlungen, 2004. http://www.datenschutz-berlin.de/attachments/196/1_de.pdf
[2] Gemeinsamer Standpunkt zu Datenschutz und Aufenthaltsinformationen in mobilen Kommunikationsdiensten, 2004. http://www.datenschutz-berlin.de/attachments/192/local_neu_de.pdf
[3] Arbeitspapier zur Nutzung von Deep Packet Inspection zu Marketing-Zwecken, 2010. http://www.datenschutz-berlin.de/attachments/737/675.41.20x.pdf

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

nahme, dass die Netzwerkverbindungen aktiv sind). Die Signalstärke kann für die Bestimmung der Entfernung zwischen Basisstation und Gerät genutzt werden. Um die Reichweite dieses Netzwerks zu erweitern, sind mehrere Basisstationen erforderlich (die sich in der Reichweite überlappen oder nicht). Die Bewegung eines Endgeräts kann festgestellt werden, wenn es in die Reichweite einer bestimmten Basisstation kommt oder diese verlässt. Wenn sich die Reichweiten der Basistationen überlappen, kann die Entfernung zwischen dem Gerät und den verschiedenen Basisstationen genutzt werden, um mit Hilfe von Trilateration den Aufenthaltsort präziser zu berechnen[4].

5. Kommunikationsprotokolle enthalten im Allgemeinen eine Reihe verschiedener Signaltypen für bestimmte Zwecke. Z. B. definieren die IEEE 802.11 Standards für Funknetzwerke[5] Management-Frames, Kontroll-Frames und Daten-Frames. Jeder Frame**,** der vom Geräte des Nutzers stammt, enthält die eindeutige MAC-Adresse des Wi-Fi Netzwerkschnittstellen-Controllers (Network Interface Controller – NIC). Ein spezieller Typ eines Management-Frames ist der „Probe Request" der von dem NIC aktiv gesendet wird, um verfügbare Netzwerke in der Umgebung zu suchen. Eine Organisation kann daher eine Reihe von Wi-Fi-Zugangspunkten (z. B. als Teil eines Wi-Fi-Netzwerks in einem Ladengeschäft) oder Frequenz-Scanner installieren und die MAC-Adresse jedes Geräts in Reichweite erfassen (unter der Annahme, dass die Wi-Fi-Einrichtung des Geräts angeschaltet ist). Da die MAC-Adresse eines bestimmten NIC normalerweise statisch ist, indiziert die Beobachtung des Wiederauftretens einer bestimmten MAC-Adresse die Rückkehr dieses bestimmten Geräts.

6. Viele dieser Geräte, besonders Smartphones, können auf das engste mit einer Einzelperson verbunden sein. Daher kann die Erhebung einer MAC-Adresse in Kombination mit Daten wie Datum und Uhrzeit leicht zur indirekten oder direkten Identifikation des Besitzers des Geräts führen.

7. Andere drahtlose Kommunikationsprotokolle wie Bluetooth und Mobiltelefon-Standards enthalten in gleicher Weise das Aussenden aktiver Signale mit eindeutigen Identifikationsnummern. Im Falle von Bluetooth ist dies die MAC-Adresse des Bluetooth-NIC. Im GSM (Groupe Speciale Mobile, einem globalen Standard zur Mobilkommunikation) werden die „International Mobil Station Equipment Identity" (IMEI), die „International Mobil Subscriber Identity" (IMSI) und die „Temporary Mobile Subscriber Identity" (TMSI) in unterschiedlichen Intervallen gesendet.

8. Geräte-Identifikatoren wie die MAC-Adresse und die IMSI enthalten außerdem Informationen über das Gerät selbst. Z. B. bestimmten die ersten drei Oktette der MAC-Adresse die Organisation, die das NIC herausgegeben hat. Dies kann Informationen über den Gerätehersteller oder den Typ des Gerätes, das verfolgt wird, offen legen. Die ersten drei Ziffern der IMSI beziehen sich auf den Länder-Code, gefolgt von der Kennung des Mobilfunkanbieters. Bluetooth und Wi-Fi-Geräte haben darüber hinaus einen konfigurierbaren Gerätenamen, der übertragen werden kann.

9. Es haben sich Diensteanbieter herausgebildet, die nicht als Kommunikationsnetzwerk fungieren und Internetzugriff anbieten, sondern die ausschließlich Dienste zur Verfolgung von Aufenthaltsinformationen auf der Basis von Scannern anbieten, um die in diesem Arbeitspapier beschriebenen Verkehrsdaten zu erheben. Sie sammeln z. B. Wi-Fi-„Probe Requests" ohne Angebot eines Internetzugangs oder erheben Bluetooth-Signale. Die Risiken, die von Tech-

[4] Trilateration meint den Prozess der Feststellung des Aufenthaltsortes unter Nutzung der Entfernung von bekannten Punkten. Davon zu unterscheiden ist die Triangulation, bei der der gemessene Winkel von bekannten Punkten genutzt wird.

[5] http://standards.ieee.org/getieee802/download/802.11-2012.pdf

nologien zum Verfolgen von Aufenthaltsinformationen herrühren, sind auch nicht exklusiv auf den traditionellen Einzelhandel beschränkt (d. h. einzelne Ladengeschäfte oder Einkaufszentren). Viele andere Geschäftsräume einschließlich Bahnhöfen und Flughäfen nutzen diese Technologie zur Beobachtung oder zur Verfolgung von Einzelpersonen[6]. Strafverfolgungsbehörden benutzten diese Technologie ebenfalls.

10. Darüber hinaus hat das Aufkommen und der Einsatz von Bluetooth 4.x NICs (auch bekannt als „Bluetooth Low Energy“ oder BLE) zu sog. „hyper-lokalen“ Geolokalisierungsdiensten geführt. BLE-Baken arbeiten mit einer kurzen Reichweite und können von einem Gerät zur Berechnung seines Aufenthaltsortes (oder zur Veranlassung der Berechnung seines Aufenthaltsortes) mit einem hohen Grad an Genauigkeit genutzt werden.

11. Eine Zunahme der Anzahl von Mobiltelefonen, die mit Wi-Fi ausgerüstet sind, zusammen mit einer Zunahme des Vorkommens von Wi-Fi in Ladengeschäften und dem Bedürfnis von Organisationen nach mehr Erkenntnissen über das Kundenverhalten, hat ein Momentum für die Entwicklung und Anwendung von Technologien zur Aufenthaltsbestimmung geschaffen. Dies ist nicht auf Wi-Fi beschränkt, weil Bluetooth ebenfalls standardmäßig aktiviert sein kann oder für eigene Zwecke genutzt wird (z. B. um die Nutzung von Freisprecheinrichtungen, die Anbindung „smarter“ Uhren, tragbarer Geräte **o**der drahtloser Kopfhörer zu ermöglichen).

12. Weil Kommunikationsfähigkeiten in eine immer weiter wachsende Anzahl von Geräten eingebaut werden, werden die Möglichkeiten zur Verfolgung dieser Geräte anwachsen. In einigen Fällen können verschiedene Geräte-Identifikatoren auf eine Einzelperson bezogen werden, um die Effektivität der Verfolgung weiter zu steigern (z. B. könnte ein Einzelner verschiedene Smartphones, Tablets, eine Uhr und ein Fitness-Armband tragen und ein vernetztes Fahrzeug benutzen).

Risiken für den Datenschutz und die Privatsphäre

13. Viele Risiken für den Datenschutz und die Privatsphäre rühren von der Tatsache her, dass die Verfolgung des Aufenthaltsorts mobiler Geräte (technisch) verdeckt stattfindet. Wie im Falle von Wi-Fi ist es zur Erhebung und Verarbeitung von Daten ausreichend, einfach an einem bestimmten Ort anwesend zu sein und ein Gerät mit sich zu führen, bei dem Wi-Fi angeschaltet ist. Der Besitzer des Geräts muss keine aktive Wahl treffen, um sich mit dem Netzwerk zu verbinden oder dies zu versuchen. Obwohl manche Technologien wie BLE eine Handlung des Nutzers zur Aktivierung der Funktion erfordern, kann die Funktion angeschaltet bleiben, oder ist sogar standardmäßig durch das Betriebssystem angeschaltet. Unter diesen

---

[6] Z. B. der Flughafen Schiphol (https://www.schiphol.nl/SchipholGroup/ NewsMedia/PressreleaseItem/AmsterdamAirportSchipholFirstAirportInEuropeWithFullBeaconCoverage.htm), die Flughäfen von Barcelona und Madrid (http://cdn1.pps-publications.com/airport-business-archive/2015/ab-summer-2015.pdf) *„ermöglichen es Passagieren, Echtzeit-Informationen über Flüge, Umsteigezeiten, kommerzielle Angebote und andere Dienste durch den Einsatz von iBeacons, die auf der drahtlosen Bluetooth-Technologie basieren“)*, der London City-Flughafen (http://annual.aci-na.org/sites/default/files/Collier-ACI-NA%20September%208%202014%20v2.pdf, s. die Folien zu „Passenger Journey Measurement“), der Flughafen New York JFK (http://www.citylab.com/navigator/ 2015/08/your-phone-could-help-make-airport-lines-shorter/401942/), der Flughafen Helsinki (https://www.finavia.fi/en/news-room/news/2014/a-global-first-helsinki-airports-new-technology-to-develop-the-travel-experience/) und Flughäfen im mittleren Osten (http://www.arabianaerospace.aero/middle-east-airports-going-smart-for-seamless-travel-experience.html)

Umständen ist der Nutzer sich wahrscheinlich der Möglichkeit zur Verfolgung der Aufenthaltsinformation nicht bewusst.

14. Diese Risiken sind besonders verbreitet, wenn die Verfolgung von Aufenthaltsinformationen in öffentlichen Räumen aktiviert ist, weil sich die Möglichkeiten als begrenzt erweisen könnten, darüber zeitnah angemessene Informationen zur Verfügung zu stellen.

15. Die unsichtbare Natur der Verfolgung und der Wunsch einer Organisation, eine solche Verfolgung im Geheimen vorzunehmen, um die „Nutzererfahrung“ nicht zu unterbrechen, führt zu Datenschutzproblemen im Hinblick auf die Transparenz, die Verantwortlichkeit, die Kenntnis des Einzelnen und die Wahlmöglichkeiten für den Nutzer.

16. Diese Risiken für den Datenschutz und den Schutz der Privatsphäre beinhalten:

    a. Die verdeckte Erhebung einer Reihe von Informationen wie gerätespezifischen Identifikatoren, die leicht mit bestimmten Einzelpersonen verknüpft werden können;

    b. Die Beobachtung des Aufenthaltsortes einer Einzelperson, ihres Weges und ihrer Aufenthaltszeit;

    c. Die Verfolgung einer Einzelperson über Zeiträume hinweg, einschließlich wiederholter Besuche an einem bestimmten Ort[7] oder innerhalb der Reichweite des Wi-Fi-Netzwerks;

    d. Die potenzielle Sensitivität der erhobenen Daten oder von Informationen, die aus dem Aufenthaltsort des Einzelnen abgeleitet werden können;

    e. Die Erhebung und Kombination von Aufenthaltsinformationen aus verschiedenen Netzwerken und/oder von verschiedenen Aufenthaltsorten, um ein vollständiges Bild der Bewegung eines Einzelnen in einem breiten Ausmaß zu erstellen (z. B. Verknüpfung von Daten verschiedener Einzelhändler oder deren Erhebung durch einen Netzwerkanbieter, der in verschiedenen Einrichtungen tätig ist);

    f. Die Kombination von Aufenthaltsdaten mit anderen Online- und Offline-Informationen, z.B. Kundenbindungskarten, soziale Medien, (abgeleitete) demografische Daten, Bankkarten- und Überweisungs-Historie oder Videoüberwachung (mit oder ohne zusätzlichen Analyse-Technologien), die zu einer überschießenden Erhebung von Daten führen könnte;

    g. Die Probleme, die erhobenen Daten in adäquater Weise zu de-identifizieren oder zu anonymisieren;

    h. Das Fehlen von Transparenz und Information des Nutzers. Dies wird weiter verstärkt bei Beschränkungen des Geräts wegen seiner Größe oder der Größe seines Displays;

    i. Das Fehlen einer einfachen und effektiven Möglichkeit für den Nutzer, die Erhebung von Daten entweder durch Einwilligung oder Widerspruch je nach den ge-

[7] Aufenthaltsort in diesem Zusammenhang könnte das Innere und Äußere des Geländes einer Organisation und die Verfolgung über verschiedene Liegenschaften einschließen.

setzlichen Anforderungen in dem jeweiligen Rechtsraum zu kontrollieren[8]

j. Die Erstellung schwarzer oder weißer Listen auf Basis der erhobenen Informationen;

k. Die Erhebung von Daten von Arbeitnehmern oder anderen Einzelpersonen, die häufig in einem Gebiet präsent sind und die Möglichkeit, diese Daten für unspezifische oder inkompatible Zwecke einschließlich der Überwachung der Arbeitsleistung oder für Disziplinarmaßnahmen zu nutzen;

l. Zugriff auf die Daten durch Strafverfolgungsbehörden;

m. Fehlende Netzwerksicherheit, die zu einem Versagen des Schutzes gegen das Abhören von Kommunikation führt oder Versagen, die erhobenen Daten adäquat zu schützen;

n. Die Nutzung von Informationen zur Profilbildung, für Werbung oder Direktmarketing;

o. Das Fehlen klarer Verantwortlichkeiten der beteiligten Organisationen aufgrund der Vielzahl der Beteiligten;

17. Wenn ein Gerät sich mit dem Netzwerk verbindet (z. B. für den Zugang zum Internet über Wi-Fi, anstatt das der Netzwerkbetreiber nur die „Probe Request“ überwacht), ist auch ein Potenzial zur Überwachung oder zum Abhören der Kommunikation selbst gegeben.

18. Technologien zur Aufenthaltsbestimmung können genutzt werden, um Informationen zu sammeln, die möglicherweise nicht durch das Telekommunikationsgeheimnis im klassischen Sinne geschützt sind.

Empfehlungen

19. Organisationen, die den Einsatz von Technologien zur Bestimmung des Aufenthaltsortes erwägen, sollten abschätzen, ob, und wenn ja unter welchen spezifischen Bedingungen die Anwendung der Verfolgung des Aufenthaltsortes von Mobilgeräten nach der anwendbaren Datenschutzgesetzgebung in ihrem jeweiligen Rechtsraum gestattet ist.

20. Im Lichte der oben beschriebenen Risiken für den Datenschutz und den Schutz der Privatsphäre wird empfohlen, das Organisationen eine Vorabkontrolle (Privacy Impact Assessment –PIA) durchführen, um sicherzustellen, dass sie alle einschlägigen Risiken vor der Anwendung eines solchen Systems berücksichtigen und minimieren.

21. Organisationen, die die Nutzung von Technologien zur Verfolgung des Aufenthaltsortes erwägen, sollten die einschlägigen von Industrieverbänden für die beabsichtigte Nutzung und

[8] Vgl. Federal Trade Commission, Retail Tracking Firm Settles FTC Charges it Misled Consumers About Opt Out Choices, https://www.ftc.gov/news-events/press-releases/2015/04/retail-tracking-firm-settles-ftc-charges-it-misled-consumers (Das Unternehmen bot nicht wie versprochen eine Widerspruchsmöglichkeit in den Geschäften an).

Anwendung entwickelten Verhaltensregeln bekannt sein[9] [10] [11]. Die Organisationen werden daran erinnert, dass die Einhaltung von Verhaltensregeln nicht automatisch die Einhaltung aller Anforderungen des national anwendbaren Rechts einschließlich der notwendigen Informationen und Wahlmöglichkeiten für die Nutzer beinhaltet.

22. Anbieter und andere Nutzer solcher Analysetechnologien einschließlich der Hersteller von Produkten, von Betriebssystemen und Entwickler von Apps müssen die Beeinträchtigung der Privatsphäre berücksichtigen, die sich aus der Verfolgung des Aufenthaltsortes ergibt, und bestrebt sein, die Erhebung von Daten zu minimieren, die Aufbewahrungsfristen für Daten zu begrenzen und datenschutzfreundliche Voreinstellungen zu wählen.

23. Zusätzlich zur Einhaltung des anwendbaren Datenschutzrechts und unter Berücksichtigung der Ergebnisse der Vorabkontrolle einschließlich einer Untersuchung, ob eine weniger in die Privatsphäre eingreifende Technologie existiert, die genutzt werden könnte, sollten die folgenden Schutzmaßnahmen beachtet werden:

    a. **Information der Betroffenen** – Organisationen müssen sicherstellen, dass ausreichende Informationen vorhanden sind, einschließlich einer Auswahl von physikalischer und digitaler Kennzeichnung**,** um Betroffene in klarer Weise darüber zu informieren, dass eine Technologie zur Bestimmung des Aufenthaltsortes verwendet wird. Die Information muss die Zwecke der Erhebung und die verantwortliche Organisation klar benennen. Es wird empfohlen, dass die Industrie einen Standard für ein Symbol entwickelt, dass in dem betreffenden Bereich verwendet werden kann, um die Betroffenen darauf hinzuweisen, dass die Technologie eingesetzt wird, ähnlich den Hinweisen zur Videoüberwachung. Besondere Aufmerksamkeit muss den Beschäftigten, Angestellten oder anderen Einzelpersonen gewidmet werden, die, wenn sie nicht von der Überwachung ausgeschlossen werden, Gegenstand überschießender Datenerhebung werden könnten;

    b. **Begrenzung der Datenerhebung** – Eine Erhebung sollte nur stattfinden, nachdem der Betroffene angemessen informiert worden ist. Organisationen sollten die die Beobachtung und die Erhebung von Daten außerhalb ihres Firmengeländes unterlassen. Dies kann durch die sorgfältige Platzierung von Empfängern, die Begrenzung der Erhebung von Daten auf Stichproben und auf spezifische Zeiträume oder Tageszeiten (z. B. während der Öffnungszeiten eines Ladengeschäfts) erreicht werden. Die Häufigkeit der Erhebung sollte auf das für den angestrebten Zweck notwendige Maß beschränkt werden. Die Nutzung von „air gaps“ zur Schaffung von nicht-zusammenhängenden Gebieten, in denen Daten erhoben werden und die Beschränkung der Erhebung auf Gebiete, die für den angegebenen Zweck relevant sind, sollten das Risiko der Verletzung der Privatsphäre ebenfalls reduzieren. Organisationen sollten ebenfalls die Festlegung von „Privatsphäre-Zonen“ anstreben, in denen als Folge von technischen oder physikalischen Maßnahmen eine Überwachung nicht stattfinden kann. Dies kann in besonders sensiblen Bereichen von Bedeutung sein, wie Toiletten oder Räumen, die der Ersten Hilfe oder dem Gebet gewidmet sind. In Rechtssystemen, in denen eine Überwachung außerhalb des Geländes einer Organisation im Einklang mit den gesetzlichen Bestimmungen durchgeführt werden kann, sollten an-

[9] Future of Privacy Forum, Mobile Location Analytics Code of Conduct. http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf

[10] Network Advertising Initiative, Mobile Application Code. http://www.networkadvertising.org/code-enforcement/mobile

[11] Digital Advertising Alliance, Application of self-Regulatory Principles to the Mobile environment. http://www.aboutads.info/DAA_Mobile_Guidance.pdf

gemessene Sicherungen zum Schutz der Privatsphäre der Betroffenen vorhanden sein;

c. **Anonymisierung von Daten ohne Zeitverzug** – Organisationen sollten die Löschung oder Anonymisierung von Daten anstreben, sobald diese in ihrer ursprünglichen Form nicht mehr benötigt werden;

d. **Angemessene Aufbewahrungsfristen von Individualdaten** – In Fällen, in denen eine eindeutige rechtliche Grundlage für die Verarbeitung personenbezogener Daten existiert, sollten Organisationen Methoden anwenden, um eindeutige Identifikatoren, wie MAC-Adressen in eine Form umzuwandeln, die das Potenzial zur Beeinträchtigung der Privatsphäre reduziert. Wenn z. B. die Erkennung wiederholter Besuche nicht beabsichtigt ist, kann eine Pseudonymisierung des Identifikators dies verhindern und trotzdem eine ausreichende Analyse der täglichen Kundenfrequenz und der genommenen Wege liefern. Am Ende der gesetzlich erlaubten Speicherungsfrist sollten die betreffenden Daten anonymisiert oder wirksam gelöscht werden. Eine vergleichende Analyse von Ereignissen über verschiedene Berichtsperioden (z. B. die Veränderung von Prozentsätzen von Besuchen in einem bestimmten Zeitraum) kann durch den Vergleich von aggregierten Daten über verschiedene Zeiträume durchgeführt werden;

e. **Einwilligung für die Kombination mit anderen Informationen** – Die Betroffenen sollten umfassend informiert werden, wenn Aufenthaltsinformationen mit anderen Informationen wie z. B. Aufzeichnungen über Geschäftsvorgänge zusammengeführt werden sollen. Dies ist insbesondere relevant, wenn Aufenthaltsinformationen als ein Merkmal zu existierenden Kundenbindungssystemen hinzugefügt werden soll, z. B. durch Hinzufügen der Funktionalität von BLE-Baken zu der existierenden Smartphone-App eines Händlers. Das Akzeptieren eines Updates durch den Nutzer über den App-Store ist wahrscheinlich nicht ausreichend, um als vollständige Information angesehen zu werden. Die Gesetzgebung in einigen Rechtssystemen kann auch die ausdrückliche Einwilligung für bestimmte Arten personenbezogener Daten verlangen[12];

f. **Einwilligung zur Weitergabe von Individualdaten an Dritte** – Organisationen sollten Daten, die zur Identifizierung eines Einzelnen verwendet werden könnten, nicht ohne die gültige, informierte Einwilligung des Betroffenen an Dritte weitergeben (dies schließt die Weitergabe von Daten an andere Kunden oder an einen einzelnen Dritten, der die Analyse von Aufenthaltsinformationen anbietet, ein), soweit es dafür nicht eine gesetzliche Ausnahme gibt; und

g. **Implementierung eines einfachen und effektiven Mittels zur Kontrolle der Erhebung** – Organisationen sollten auch ein System etablieren, das es den Einzelnen erlaubt, die Erhebung solcher Daten auch in den Fällen zu kontrollieren, wo dies nicht ausdrücklich durch das anwendbare Datenschutzrecht gefordert wird. Organisationen sollten gut sichtbar auf die Existenz von Wahl- und Kontrollmöglichkeiten in dem Gebiet hinweisen, in dem die Daten erhoben werden. Dies sollte das Angebot einer leicht zugänglichen, klar beschriebenen und effektiven Möglichkeit einschließen, die Kontrolle auszuüben. Es wird empfohlen, dass ein einheitlicher Mechanismus von allen Anbietern von Aufenthaltsinformations-

[12] Z. B. verlangt die Europäische Datenschutzrichtlinie 95/46/EG die ausdrückliche Einwilligung für die Verarbeitung spezieller Kategorien von Daten wie rassische oder ethnische Herkunft, oder in Bezug auf Gesundheit oder Sexualleben. Ähnliche Anforderungen können auch in den gesetzlichen Bestimmungen anderer Rechtsordnungen vorkommen.

analysediensten unterstützt wird und dass der Einzelne seine Präferenz nur einmal ausdrücken muss. Wenn die Verfolgung auf der informierten Einwilligung basiert, muss der Einzelne in die Lage versetzt werden, seine Einwilligung in einfacher und dauerhafter Weise zurückzuziehen. Wo dies technisch möglich ist, werden aussagekräftige Prüfprotokolle empfohlen, die es den Endnutzern ermöglichen, zu wissen, wann und für welche Zwecke Daten über ihre Endgeräte von wem erhoben worden sind. Nutzer sollten auch in die Lage versetzt werden, alle oder Teile der vorher gesammelten Daten zu löschen.

24. Technologien zur Verfolgung des Aufenthaltsortes dürfen nicht zum Abhören des Inhalts von Kommunikation verwendet werden. Im Hinblick auf die strikt persönliche Nutzung der meisten Smartphones besteht eine Notwendigkeit für ein hohes Maß an Schutz der Kommunikationsdaten, die von diesen Geräten erzeugt werden, auch jenseits des traditionellen Anwendungsbereichs des Fernmeldegeheimnisses.

25. Gerätehersteller und Hersteller von Netzwerkprotokollen sollten das Potenzial zum Eindringen in die Privatsphäre im Blick behalten, dass aus der Nutzung persistenter Identifikatoren und anderen öffentlich gesendeten Signalen entsteht. Es wird empfohlen, dass, wo dies technisch möglich ist, ein Mechanismus angeboten wird, um solche Identifikatoren in nutzerdefinierten Intervallen zurückzusetzen und dass andere Maßnahmen zum Schutz der Privatsphäre standardmäßig aktiviert sind.

Über die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation („ Berlin Group“)

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation (englisch: International Working Group on Data Protection in Telecommunications - IWGDPT, auch bekannt als “Berlin Group”) besteht aus Vertretern von Datenschutz-Aufsichtsbehörden und Organisationen aus aller Welt, die sich mit dem Schutz der Privatsphäre beschäftigen. Die Arbeitsgruppe wurde 1983 im Rahmen der Internationalen Datenschutzkonferenz auf Initiative des Berliner Beauftragten für Datenschutz gegründet, der seither ihren Vorsitz führt. Seit ihrer Gründung hat die Arbeitsgruppe eine Vielzahl von Empfehlungen („Gemeinsame Standpunkte“ und „Arbeitspapiere“) mit dem Ziel verabschiedet, den Schutz der Privatsphäre in der Telekommunikation zu verbessern. Seit Anfang der neunziger Jahre beschäftigt sich die Gruppe insbesondere mit dem Schutz der Privatsphäre im Internet.

Weitere Informationen über die Arbeitsgruppe sowie eine Broschüre mit allen von der Gruppe verabschiedeten Dokumenten sind auf der Webseite der Arbeitsgruppe abrufbar: http://www.berlin-privacy-group.org.