ARTIKEL-29-DATENSCHUTZGRUPPE

881/11/DE
WP 185

Stellungnahme 13/2011 zu den Geolokalisierungsdiensten von intelligenten mobilen Endgeräten

Angenommen am 16. Mai 2011

Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen durch die Generaldirektion Justiz, Direktion C (Grundrechte und Unionsbürgerschaft) der Europäischen Kommission, B-1049 Brüssel, Belgien, Büro MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_de.htm

INHALT

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN
eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDES DOKUMENT ANGENOMMEN:

1. Einleitung

Geografische Informationen spielen eine wichtige Rolle in unserer Gesellschaft. Fast alle menschlichen Aktivitäten und Entscheidungen weisen eine geografische Komponente auf. Im Allgemeinen steigt der Wert einer Information, wenn sie mit einem Standort verbunden ist. Es können alle Arten von Informationen Bezug zu einem geografischen Standort haben, wie beispielsweise Finanzdaten, Gesundheitsdaten und andere Verhaltensdaten der Verbraucher. Durch die rasche technologische Entwicklung und die weitverbreitete Nutzung von intelligenten mobilen Endgeräten entsteht eine ganz neue Kategorie standortbezogener Dienste.

Mit Hilfe dieser Stellungnahme soll für Klarheit hinsichtlich des für Geolokalisierungsdienste geltenden Rechtsrahmens gesorgt werden, die auf intelligenten mobilen Endgeräten verfügbar sind und/oder durch diese generiert werden. Die betreffenden Endgeräte können eine Verbindung mit dem Internet erstellen oder sind mit Standortsensoren wie GPS ausgestattet. Beispiele für solche Dienste sind: Karten und Navigation, geopersonalisierte Dienste (einschließlich der Sehenswürdigkeiten der Umgebung), Augmented Reality, Georeferenzierung von Inhalten im Internet (Geotagging), Lokalisierung des Aufenthaltsortes von Freunden, Überwachung von Kindern und standortbezogene Werbung.

Die vorliegende Stellungnahme befasst sich auch mit den drei wichtigsten Arten der Infrastruktur, die zur Bereitstellung von Geolokalisierungsdiensten verwendet werden, nämlich GPS, GSM-Basisstationen und Wi-Fi. Hierbei wird besonderes Augenmerk auf die neue Infrastruktur gerichtet, die auf der Lokalisierung von Wi-Fi-Zugangspunkten basiert.

Es ist der Datenschutzgruppe sehr wohl bewusst, dass es noch viele andere Dienste gibt, die Standortdaten verarbeiten und ebenfalls zu datenschutzrechtlichen Bedenken führen können. Das reicht von elektronischen Ticketsystemen zu Mautsystemen für Autos und von Satellitennavigationsdiensten und der Standortbestimmung beispielsweise mit Hilfe von Kameras zur Geolokalisierung von IP-Adressen. Angesichts der raschen technologischen Entwicklung insbesondere im Hinblick auf das Kartografieren drahtloser Zugangspunkte, verbunden mit der Tatsache, dass neue Marktteilnehmer neue standortbezogene Dienste anbieten wollen, die auf einer Kombination aus Basisstation, GPS und Wi-Fi-Daten besteht, hat sich die

Datenschutzgruppe entschieden, die rechtlichen Voraussetzungen gemäß der Datenschutzrichtlinie insbesondere für diese Dienste klarzustellen.

In der Stellungnahme wird zuerst die Technologie beschrieben, dann werden die Risiken für den Datenschutz herausgearbeitet und bewertet und schließlich werden Schlussfolgerungen gezogen zur Anwendbarkeit der einschlägigen Artikel auf die verschiedenen für die Verarbeitung Verantwortlichen, die Standortdaten von mobilen Endgeräten erheben und verarbeiten. Dazu gehören zum Beispiel Anbieter der Infrastruktur für die Geolokalisierung, Hersteller von Smartphones und die Entwickler von standortbezogenen Anwendungen.

Diese Stellungnahme bewertet nicht die spezielle Technologie zur Georeferenzierung, die mit dem sogenannten Web 2.0 verknüpft ist, bei dem Nutzer georeferenzierte Informationen in soziale Netzwerke wie Facebook oder Twitter integrieren. Die Stellungnahme wird auch einige andere Technologien zur Geolokalisierung nicht näher untersuchen, die verwendet werden, um Geräte innerhalb eines relativ kleinen Bereichs miteinander zu verbinden (Einkaufszentren, Flughäfen, Bürogebäude usw.), wie Bluetooth, ZigBee, Geofencing und Wi-Fi-basierte RFID-Etiketten. Dennoch gelten viele der Schlussfolgerungen, die in der vorliegenden Stellungnahme in Bezug auf berechtigte Gründe, Informationsrechte und die Rechte der betroffenen Person gezogen werden, auch für diese Technologien, wenn sie dazu genutzt werden, den geografischen Standort von Menschen über ihrer Endgeräte zu bestimmen.

2. Hintergrund: verschiedene Infrastrukturen für die Geolokalisierung

2.1 Daten der Basisstation

Das von den verschiedenen Telekommunikationsbetreibern abgedeckte Gebiet ist in Bereiche aufgeteilt, die gemeinhin als Zellen bekannt sind. Um ein Mobiltelefon nutzen oder eine Verbindung mit dem Internet über die 3G-Kommunikation aufbauen zu können, muss das mobile Endgerät eine Verbindung mit der Antenne (im Folgenden: Basisstation) aufnehmen, die diese Zelle abdeckt. Die Zellen decken Bereiche unterschiedlicher Größe ab. Das hängt von den Interferenzen beispielsweise mit Bergen oder hohen Gebäuden ab.

Immer, wenn ein mobiles Endgerät angeschaltet ist, ist es mit einer bestimmten Basisstation verbunden. Der Telekombetreiber zeichnet diese Verbindungen ständig auf. Jede Basisstation hat eine eindeutige ID und ist unter einem bestimmten Standort registriert. Sowohl der Telekombetreiber als auch viele mobile Endgeräte können die Signale sich überschneidender Zellen nutzen (benachbarte Basisstationen), um so den Standort des mobilen Endgeräts mit steigender Genauigkeit zu schätzen. Diese Technik wird auch Triangulation genannt.

Die Genauigkeit kann durch Informationen wie RSSI (Received Signal Strength Indicator), TDOA (Time Difference of Arrival) und AOA (Angle Of Arrival) weiter vergrößert werden.

Die Daten von Basisstationen können auf innovative Weise genutzt werden, beispielsweise zum Aufspüren von Verkehrsstaus. Auf jeder Straße gibt es für jeden

Tagesabschnitt eine bestimmte Durchschnittsgeschwindigkeit. Wenn es länger als erwartet dauert, bis das Endgerät das Gebiet der benachbarten Basisstation erreicht, liegt offensichtlich ein Verkehrsstau vor.

Zusammenfassend lässt sich sagen, dass diese Methode der Standortbestimmung eine schnelle, grobe Standortangabe ermöglicht, jedoch verglichen mit GPS und Wi-Fi-Daten nicht sehr genau ist. Die Genauigkeit beträgt in eng besiedelten Stadtgebieten ungefähr 50 Meter, in ländlichen Gebieten aber bis zu einigen Kilometern.

2.2 GPS-Technologie

In intelligente mobile Endgeräte sind Chipsätze mit GPS-Empfängern eingebaut, die ihren Standort bestimmen.

Bei der GPS-Technologie (Satellitennavigationssystem) werden 31 Satelliten verwendet, die alle in einem der sechs verschiedenen Orbits um die Erde kreisen.[1] Jeder Satellit sendet ein sehr genaues Funksignal.

Das mobile Endgerät kann seinen Standort bestimmen, wenn der GPS-Sensor mindestens vier dieser Signale auffängt. Anders als bei den Daten der Basisstationen geht das Signal nur in eine Richtung. Die die Satelliten betreibenden Einrichtungen können nicht nachverfolgen, welche Endgeräte das Funksignal empfangen haben.

Mit Hilfe der GPS-Technologie kann die Position mit einer Genauigkeit von vier bis 15 Metern bestimmt werden. Der größte Nachteil von GPS ist der relativ langsame Start.[2] Ein weiterer Nachteil ist, dass es in Gebäuden nicht oder nur schlecht funktioniert. Deshalb wird die GPS-Technologie in der Praxis häufig mit Daten von Basisstationen und/oder kartografierten Wi-Fi-Zugangspunkten kombiniert.

2.3 Wi-Fi

2.3.1 Wi-Fi-Zugangspunkte

Die Verwendung von Wi-Fi-Zugangspunkten ist eine relative neue Quelle für Informationen zur Geolokalisierung. Die Technologie ähnelt der Verwendung von Basisstationen. Sie stützen sich beide auf eine eindeutige ID (von der Basisstation oder dem Wi-Fi-Zugangspunkt), die von einem mobilen Endgerät aufgespürt werden kann und zu einem Dienst gesendet wird, der für jede eindeutige ID den Standort hat.

---

[1] Das Satellitennavigationssystem besteht aus Satelliten, die von den Vereinigten Staaten von Amerika aus militärischen Zwecken in die Umlaufbahn gebracht wurden. Die Europäische Kommission plant den Start von Galileo bis 2014. Galileo ist ein Netzwerk aus 18 Satelliten, die eine freie, nichtmilitärische Satellitennavigation ermöglichen. Die ersten zwei Satelliten sollen 2011 in die Umlaufbahn gebracht werden und zwei weitere in 2012. Quelle: European Commission, 'Commission presents midterm review of Galileo and EGNOS', 25. Januar 2011, URL: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&item_id=4835

[2] Um die Erkennung des ersten GPS-Signals zu beschleunigen, können sogenannte Rainbow Tables mit den erwarteten Positionen der verschiedenen Satelliten in den nächsten Wochen vorgeladen werden.

Die MAC-Adresse (Medium Access Control) ist die eindeutige ID jedes Wi-Fi-Zugangspunktes. Die Mac-Adresse ist eine eindeutige, einer Netzwerkschnittstelle zugewiesene ID. Sie ist üblicherweise in der Hardware hinterlegt, wie Speicherchips und/oder Netzwerkkarten in Computern, Telefonen, Laptops oder Zugangspunkten.[3]

Wi-Fi-Zugangspunkte können als Quelle für die Geolokalisierung herangezogen werden, da sie ihre Verfügbarkeit ständig anzeigen. Die meisten Breitband Internet-Zugangspunkte verfügen standardmäßig auch über eine Wi-Fi-Antenne. Die Standard-Einstellung der am häufigsten genutzten Zugangspunkte in Europa für diese Verbindung ist „an", auch wenn der Nutzer seine(n) Computer nur mit Kabeln mit dem Zugangspunkt verbunden hat. Gleich einem Radio sendet der Wi-Fi-Zugangspunkt selbst dann ständig seinen Netzwerknamen und seine MAC-Adresse, wenn niemand die Verbindung nutzt und selbst wenn die Inhalte der drahtlosen Kommunikation mit WEP, WPA oder WPA2 verschlüsselt sind.

Es gibt zwei verschiedene Wege, die MAC-Adressen von Wi-Fi-Zugangspunkten zu sammeln:[4]

1. Aktives Scannen: Versenden von aktiven Abfrage-Paketen[5] an alle Wi-Fi-Zugangspunkte in der Umgebung und Aufzeichnen der Antworten. Diese Antworten enthalten keine Informationen über die mit dem Wi-Fi-Zugangspunkt verbundenen Endgeräte.

2. Passives Scannen: Verzeichnen der regelmäßigen Beacon-Frames, die jeder Zugangspunkte sendet (üblicherweise zehnmal je Sekunde). Als eine nicht dem Standard entsprechende Alternative zeichnen einige Geräte alle von den Zugangspunkten übermittelten Wi-Fi-Frames auf, einschließlich derjenigen, die keine Beacon-Signale übertragen. Wenn diese Art Scannen ohne die richtige Anwendung des eingebauten Datenschutzes (Privacy by Design) durchgeführt wird, kann es zur Erhebung von Daten führen, die zwischen Zugangspunkten und den mit ihnen verbundenen Geräten ausgetauscht werden. Auf diese Weise könnten die MAC-Adressen von Desktop-Computern, Laptops und Druckern aufgezeichnet werden. Diese Art von Scannen könnte auch zur rechtswidrigen Aufzeichnung des Inhalts der Mitteilungen führen. Die Inhalte sind leicht lesbar, wenn der Inhaber eines Wi-Fi-Zugangspunktes keine Wi-Fi-Verschlüsselung (WEP/WPA/WPA2) ermöglicht hat.

Der Standort eines Wi-Fi-Zugangspunktes kann auf zwei verschiedene Arten berechnet werden:

1. Statisch/einmal: die für die Verarbeitung Verantwortlichen sammeln die Mac-Adressen von Wi-Fi-Zugangspunkten selbst, indem sie mit Fahrzeugen herumfahren,

---

[3] Ein Beispiel für eine MAC-Adresse: 00-1F-3F-D7-3C-58. Die MAC-Adresse eines Wi-Fi-Zugangspunktes wird BSSID (Basic Service Set Identifier) genannt.

[4] Aktives und passives Scannen wurden in der IEEE 802.11 standardisiert, um Zugangspunkte zu finden.

[5] Zum Sammeln der MAC-Adressen sendet der Sammler einen Probe-Request-Frame an alle Zugangspunkte.

die mit Antennen ausgestattet sind. Sie zeichnen den genauen Breiten- und Längengrad des Fahrzeuges zu dem Zeitpunkt auf, wenn das Signal eingefangen wird. So können sie den Standort der Zugangspunkte unter anderem anhand der Signalstärke errechnen.

2. Dynamisch/ständig: die Nutzer von Geolokalisierungsdiensten sammeln automatisch die MAC-Adressen, die ihre Wi-Fi-fähigen Geräte empfangen, wenn sie beispielsweise eine Online-Karte nutzen, um ihre Position zu bestimmen (Wo bin ich?). Das mobile Endgerät sendet dann dem Anbieter der Geolokalisierungsdienste alle verfügbaren Informationen zu, einschließlich der MAC-Adressen, der SSIDs und der Signalstärke. Der für die Verarbeitung Verantwortliche kann diese ständigen Beobachtungen dazu nutzen, den Standort der Wi-Fi-Zugangspunkte zu berechnen oder deren Berechnung in seiner Datei mit den kartografierten Wi-Fi-Zugangspunkten zu verbessern.

Es muss angemerkt werden, dass mobile Endgeräte keine Verbindung mit den Wi-Fi-Zugangspunkten aufnehmen müssen, um Wi-Fi-Informationen zu sammeln. Sie spüren Zugangspunkte (im aktiven oder passiven Scannermodus) automatisch auf und sammeln automatisch Daten über sie.

Darüber hinaus senden Mobiltelefone, die eine Geolokalisierung erfragen, nicht nur Wi-Fi-Daten sondern oft auch andere Standortinformationen, über die sie verfügen, einschließlich GPS- und Basisstationsdaten. Das ermöglicht es dem Anbieter, den Standort „neuer“ Wi-Fi-Zugangspunkte zu berechnen und/oder die bestehenden Berechnungen der Wi-Fi-Zugangspunkte zu verbessern, die bereits in der Datenbank verzeichnet sind. Auf diese Weise wird die Erhebung von Informationen über Wi-Fi-Zugangspunkte auf eine sehr wirksame Weise dezentralisiert, ohne dass dies den Kunden unbedingt bewusst ist.

Zusammenfassung: die Geolokalisierung auf der Basis von Wi-Fi-Zugangspunkten ermöglicht eine schnelle und basierend auf ständigen Messungen, immer genauere Positionsbestimmung.

3. Gefahren für den Datenschutz

Ein intelligentes mobiles Endgerät ist sehr eng mit einer bestimmten Person verbunden. Die meisten Menschen neigen dazu, ihr Mobiltelefon dicht bei sich zu tragen – von der Hosentasche oder Tasche zum Nachttisch an ihrem Bett.

Es kommt selten vor, dass ein solches Gerät an eine andere Person verliehen wird. Den meisten Menschen ist es bewusst, dass ihr mobiles Endgerät eine Reihe von sehr persönlichen Informationen enthält, von E-Mails zu privaten Bildern und vom Browserverlauf beispielsweise zu einer Kontaktliste.

Dies ermöglicht es den Anbietern von auf der Geolokalisierung basierenden Diensten, einen persönlichen Überblick über die Gewohnheiten und Muster der Inhaber solcher Endgeräte zu bekommen und umfassende Profile zu erstellen. Von dem Muster der Inaktivität bei Nacht können Rückschlüsse auf den Schlafplatz gezogen werden und aus einem regelmäßigen Reisemuster am Morgen kann der Standort des Arbeitgebers geschlossen werden. Das Muster kann auch Daten umfassen, die basierend auf dem

sogenannten *Social Graph*[6] aus den Bewegungsmustern der Freunde erschlossen werden.

Ein Verhaltensmuster kann *besondere Datenkategorien* enthalten, wenn es zum Beispiel Besuche im Krankenhaus oder an religiösen Orten aufzeigt oder die Anwesenheit bei politischen Demonstrationen oder an bestimmten anderen Orten, die Daten zum Beispiel über das Sexualleben offenbaren. Diese Profile können für Entscheidungen herangezogen werden, die den Inhaber massiv beeinträchtigen.

Die Technologie von intelligenten mobilen Endgeräten ermöglicht die ständige Überwachung von Standortdaten. Smartphones können ständig Signale von Basisstationen und Wi-Fi-Zugangspunkten sammeln. Technisch ist es möglich, die Überwachung im Geheimen durchzuführen, ohne den Inhaber zu informieren. Die Überwachung kann auch im Halbgeheimen erfolgen, wenn die Leute „vergessen" oder nicht richtig darüber informiert werden, dass die Dienste zur Standortbestimmung „eingeschaltet" sind oder wenn die Zugangseinstellungen der Standortdaten von „privat" auf „öffentlich" verstellt werden.

Selbst wenn Personen ihre Standortdaten im Internet bewusst über Aufenthaltsort- und Georeferenzierungsdienste verfügbar machen, schafft der uneingeschränkte globale Zugang neue Probleme, die von Datendiebstahl zu Einbrüchen und sogar zu körperlichen Angriffen und Stalking führen.

Wie bei anderen neuen Technologien auch, liegt ein großes Risiko in Bezug auf die Nutzung der Standortdaten in der schleichenden Ausweitung der Zweckbestimmung. Das heißt, dass basierend auf der Verfügbarkeit eines neuen Datentyps neue Zweckbestimmungen entwickelt werden, die zum Zeitpunkt der ursprünglichen Erhebung der Daten nicht vorhergesehen wurden.

4. Rechtsrahmen

Die Datenschutzrichtlinie (95/46/EG) ist der einschlägige Rechtsrahmen. Sie findet in jedem Fall Anwendung, in dem personenbezogene Daten als Folge der Verarbeitung von Standortdaten verarbeitet werden. Die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG in der durch die Richtlinie 2009/136/EG geänderten Fassung) findet nur auf die Verarbeitung von Daten der Basisstation von öffentlichen elektronischen Kommunikationsdiensten und –netzen (Telekombetreiber) Anwendung.

4.1 Von Telekombetreibern verarbeitete Daten von Basisstationen

Telekombetreiber verarbeiten im Rahmen der Bereitstellung von öffentlichen elektronischen Kommunikationsdiensten[7] ständig Daten von Basisstationen. Sie können dies auch tun, um Dienste mit Zusatznutzen bereitzustellen. Dieser Fall wurde

---

[6] Der Begriff „Social Graph" wiest auf die Sichtbarkeit von Freunden in sozialen Netzwerken hin sowie auf die Möglichkeiten, Verhaltensmerkmale anhand der Daten über diese Freunde zu erschließen.

[7] Merke, dass die Bereitstellung von öffentlichen Wi-Fi-Hotspots durch Telekombetreiber auch als öffentlicher elektronischer Kommunikationsdienst gilt und deshalb vorrangig die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation erfüllen sollte.

bereits von der Datenschutzgruppe in der Stellungnahme 5/2005 (WP115) behandelt. Obwohl einige der Beispiele in der Stellungnahme durch die ausgeweitete Nutzung der Internettechnologie und der Sensoren in immer kleineren Endgeräten zwangsläufig überholt sind, bleiben die rechtlichen Schlussfolgerungen und Empfehlungen aus dieser Stellungnahme in Bezug auf die Verwendung der Daten von Basisstationen gültig.

1. Da sich Standortdaten von Basisstationen auf bestimmte oder bestimmbare Personen beziehen, unterliegen sie den Bestimmungen zum Schutz personenbezogener Daten, die in der Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 niedergelegt sind.
2. Die Richtlinie 2002/58/EG vom 12. Juli 2002 (in der durch die Richtlinie 2009/136/EG geänderten Fassung) ist gemäß der Definition in Artikel 2 Buchstabe c dieser Richtlinie ebenfalls anzuwenden:
   „Standortdaten" Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben;

Wenn ein Telekombetreiber einen hybriden Geolokalisierungsdienst anbietet, der auch auf der Verarbeitung anderer Arten von Standortdaten wie GPS oder Wi-Fi-Daten basiert, gilt diese Tätigkeit als öffentlicher elektronischer Kommunikationsdienst. Der Telekombetreiber muss die vorherige Einwilligung seiner Kunden sicherstellen, wenn er diese Geolokalisierungsdaten Dritten anbietet.

4.2 Verarbeitung von Basisstations-, Wi-Fi- und GPS-Daten durch Anbieter von Diensten der Informationsgesellschaft

4.2.1 Anwendbarkeit der geänderten Datenschutzrichtlinie für elektronische Kommunikation

Typischerweise sind Unternehmen, die Lokalisierungsdienste und -anwendungen anbieten, die auf einer Kombination von Basisstations-, GPS- und Wi-Fi-Daten basieren, Anbieter von *Diensten der Informationsgesellschaft*. Als solche sind sie aufgrund der strengen Definition von elektronischen Kommunikationsdiensten ausdrücklich von der Datenschutzrichtlinie für elektronische Kommunikation ausgeschlossen (Artikel 2 Absatz c der geänderten Rahmenrichtlinie (unverändert).[8]

Die Datenschutzrichtlinie für elektronische Kommunikation findet keine Anwendung auf die Verarbeitung von Standortdaten durch Dienste der Informationsgesellschaft,

[8] Richtlinie 2002/21/EG vom 7. März 2002, Artikel 2 Buchstabe c: *„elektronische Kommunikationsdienste": gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen;*

selbst wenn eine solche Verarbeitung über ein öffentliches elektronisches Kommunikationsnetz erfolgt. Ein Nutzer kann sich entscheiden, GPS-Daten über das Internet zu übermitteln, zum Beispiel, wenn er Navigationsdienste des Internets nutzt. In diesem Fall wird das GPS-Signal unabhängig von dem GSM-Netzwerk in die Anwendungsebene der Internetkommunikation übertragen. Der Anbieter des Telekommunikationsdienstes fungiert als reiner Kanal. Er kann ohne sehr einschneidende Methoden wie *Deep Packet Inspection* keinen Zugang zu GPS- und/oder Wi-Fi- und/oder Basisstationsdaten erhalten, die von und zu einem intelligenten mobilen Endgerät zwischen einem Nutzer/Teilnehmer und einem Dienst der Informationsgesellschaft gesendet werden.

4.2.2 Anwendbarkeit der Datenschutzrichtlinie

Ist die geänderte Datenschutzrichtlinie für elektronische Kommunikation nicht anwendbar, findet gemäß Artikel 1 Absatz 2 die Richtlinie 95/46/EG Anwendung: „*Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz 1 genannten Zwecke dar.*“

Basierend auf der Datenschutzrichtlinie sind personenbezogene Daten *alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind* – Artikel 2 Buchstabe a der Richtlinie.

Erwägungsgrund 26 der Richtlinie legt besondere Betonung auf den Begriff „bestimmbar“. Es steht zu lesen: „*Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.*“

Erwägungsgrund 27 der Richtlinie legt den breiten Geltungsbereich des Schutzes dar: „*In der Tat darf der Schutz nicht von den verwendeten Techniken abhängen, da andernfalls ernsthafte Risiken der Umgehung entstehen würden.*“

In ihrer Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ hat die Datenschutzgruppe umfangreiche Leitlinien zur Definition personenbezogener Daten bereitgestellt.

Intelligente mobile Endgeräte
Intelligente mobile Endgeräte sind untrennbar mit natürlichen Personen verbunden. Normalerweise liegt eine direkte und indirekte Identifizierbarkeit vor.

Erstens hat der, den GSM- und mobilen Internetzugang bereitstellende Telekombetreiber üblicherweise ein Verzeichnis mit dem Namen, der Adresse und Bankverbindung jedes Kunden zusammen mit verschiedenen Kennnummern des Geräts wie IMEI und IMSI.

Zweitens wird für den Kauf zusätzlicher Software für das Endgerät (*Anwendungen oder Apps*) gewöhnlicherweise eine Kreditkartennummer benötigt. Dadurch wird die Kombination aus Kennnummer(n) und Standortdaten um Daten zur direkten Identifizierung bereichert.

Indirekte Identifizierbarkeit kann durch eine Kombination aus Kennnummer(n) des Endgeräts in Verbindung mit einem oder mehreren errechneten Standort/en erzielt werden.

Jedes intelligente mobile Endgerät hat zumindest ein Kennzeichen, die MAC-Adresse. Das Endgerät kann noch andere eindeutige Identifikationsnummer haben, die von dem Entwickler des Betriebssystems hinzugefügt wurden. Diese Kennzeichen können im Zusammenhang mit Geolokalisierungsdiensten übermittelt und weiter verarbeitet werden. Es ist eine Tatsache, dass der Standort eines bestimmten Gerätes sehr präzise bestimmt werden kann, insbesondere wenn die verschiedenen Infrastrukturen zur Geolokalisierung kombiniert werden. Ein solcher Standort kann auf ein Haus oder einen Arbeitgeber hinweisen. Insbesondere durch wiederholte Beobachtungen ist es möglich, den Inhaber des Endgeräts zu identifizieren.

Bei der Berücksichtigung der verfügbaren Mittel zur Identifizier muss die Entwicklung berücksichtigt werden, dass die Menschen dazu tendieren, immer mehr persönliche Standortdaten im Internet bekannt zu geben, indem sie beispielsweise den Standort ihres Wohn- oder Arbeitsplatzes zusammen mit anderen Identifizierungsdaten angeben. Eine solche Offenlegung kann auch ohne ihr Wissen erfolgen, wenn sie von anderen Leuten mit geografischen Tags versehen werden. Diese Entwicklung macht es einfacher, einen Standort oder ein Verhaltensmuster mit einer spezifischen Person in Verbindung zu bringen.

Gemäß Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ sollte auch angemerkt werden, dass es in dem oben beschriebenen Kontext ein Kennzeichen möglich macht, den Nutzer eines spezifischen Endgeräts ausfindig zu machen und Rückschlüsse über ihn zu ziehen, selbst wenn sein wirklicher Name nicht bekannt ist.

Wi-Fi-Zugangspunkte
Diese indirekte Identifizierbarkeit trifft auch auf Wi-Fi-Zugangspunkte zu.[9] Die MAC-Adresse eines Wi-Fi-Zugangspunktes in Verbindung mit seinem berechneten Standort ist untrennbar verbunden mit dem Standort des Inhabers dieses Zugangspunktes.

Basierend auf der Signalstärke und den ständigen Aktualisierungen des Standortes durch die Nutzer seines Geolokalisierungsdienstes kann ein vernünftig ausgestatteter, für die Verarbeitung Verantwortlicher einen in zunehmendem Maße genauen Standort eines Wi-Fi-Zugangspunktes berechnen.

Mit Hilfe dieser Mittel kann häufig eine kleine Gruppe von Wohnungen oder Häusern identifiziert werden, in denen der Inhaber eines Zugangspunktes lebt. Wie leicht es ist,

[9] Wi-Fi-Zugangspunkte können sogar direkt identifizierbar sein, wenn der Anbieter des Internetzugangs ein Verzeichnis aller MAC-Adressen der Wi-Fi-Router führt, die er für seine identifizierten Kunden bereithält.

diesen Inhaber mit Hilfe der MAC-Adresse zu identifizieren, hängt von der Umgebung ab:

- In dünn besiedelten Gebieten, in denen die MAC-Adresse auf ein einziges Haus hinweist, kann der Inhaber des Hauses direkt mit Hilfe von Grundbüchern, Telefonbüchern, Wählerverzeichnissen oder sogar anhand einer einfachen Suchmaschinenabfrage bestimmt werden.[10]
- In dichter besiedelten Gebieten ist es möglich, mit Hilfe der Signalstärke und/oder SSID (die jeder mit einem Wi-Fi-fähigen Gerät aufspüren kann) den genauen Standort des Zugangspunktes zu ermitteln. So kann häufig die Identität der Person/en festgestellt werden, die an dem genauen Ort (Haus oder Wohnung) lebt/leben, an dem sich der Zugangspunkt befindet.
- In sehr dicht besiedelten Gebieten weist die MAC-Adresse selbst mit Hilfe der Informationen über die Signalstärke auf mehrere Wohnungen hin, in denen sich der Zugangspunkt möglicherweise befindet. In diesen Fällen ist es ohne unvertretbaren Aufwand nicht möglich, genau festzustellen, wer in der Wohnung lebt, in der der Zugangspunkt ermittelt wurde.

Die Tatsache, dass es in einigen Fällen derzeit nicht möglich ist, den Inhaber eines Endgeräts ohne unvertretbaren Aufwand zu ermitteln, ändert nichts an der generellen Schlussfolgerung, dass die Kombination einer MAC-Adresse und einem WI-Fi-Zugangspunkt mit seinem berechneten Standort als personenbezogene Daten zu behandeln ist.

Unter diesen Umständen und angesichts der Tatsache, dass es unwahrscheinlich ist, dass der für die Verarbeitung Verantwortliche dazu in der Lage ist, zwischen Fällen zu unterschieden, in denen der Inhaber eines Wi-Fi-Zugangspunktes identifizierbar ist und solchen, in denen er es nicht ist, sollte der für die Verarbeitung Verantwortliche alle Daten über Wi-Fi-Router als personenbezogene Daten behandeln.

Es muss daran erinnert werden, dass der Zweck der Verarbeitung dieser Geolokalisierungsdaten nicht die Identifizierung der Nutzer sein muss. Ob es ohne unverhältnismäßigen Aufwand möglich ist, die Inhaber von Wi-Fi-Zugangspunkten zu ermitteln, hängt stark von den technischen Möglichkeiten des für die Verarbeitung Verantwortlichen oder jeder sonstigen Person ab, die die Inhaber ermitteln möchte.

5. Verpflichtungen aus Datenschutzgesetzen

5.1 Für die Verarbeitung der Daten Verantwortliche

Im Zusammenhang mit Geolokalisierungsdiensten, die von Diensten der Informationsgesellschaft bereitgestellt werden, können drei Funktionsbereiche mit unterschiedlichen Verantwortlichkeiten in Bezug auf die Verarbeitung personenbezogener Daten unterschieden werden. Diese sind: der für die Verarbeitung einer Infrastruktur für die Geolokalisierung Verantwortliche; der Anbieter einer bestimmten Anwendung oder eines bestimmten Dienstes zur Geolokalisierung und

[10] Die Verfügbarkeit solcher Register oder Verzeichnisse unterscheidet sich von Mitgliedstaat zu Mitgliedstaat.

der Entwickler des Betriebssystems eines intelligenten mobilen Endgeräts. In der Praxis übernehmen Unternehmen häufig viele Rollen zur selben Zeit, beispielsweise, wenn sie ein Betriebssystem mit einer Datenbank mit kartografierten Wi-Fi-Zugangspunkten und einer Werbeplattform verbinden.

5.1.1 Für die Verarbeitung Verantwortliche einer Infrastruktur für die Geolokalisierung

Ähnlich den Telekombetreibern bei der Verarbeitung des Standortes eines spezifischen Endgeräts mit Hilfe der Basisstationen, verarbeiten die Inhaber von Datenbanken mit kartografierten Wi-Fi-Zugangspunkten personenbezogene Daten, wenn sie den Standort eines bestimmten intelligenten mobilen Endgeräts errechnen. Da sie beide die Zwecke und die Mittel dieser Verarbeitung bestimmen, sind sie beide für die Verarbeitung Verantwortliche im Sinne der Definition von Artikel 2 Buchstabe d der Datenschutzrichtlinie.

Es muss betont werden, dass das spezielle Endgerät entscheidend für die Berechnung seines Standortes ist, indem es seine eigenen Standortdaten (oft eine Kombination aus GPS, Wi-Fi und Basisstation) und die eindeutigen IDs von nahegelegenen Wi-Fi-Zugangspunkten an den Inhaber der Datenbank übermittelt.[11] Ein solches Gerät erfüllt auch das Kriterium von Artikel 4 Absatz 1 Buchstabe c der Datenschutzrichtlinie, *Mittel, die im Hoheitsgebiet eines Mitgliedstaates belegen sind.*

Da die MAC-Adresse eines Wi-Fi-Zugangspunktes in Kombination mit seinem errechneten Standort als personenbezogene Daten behandelt werden sollte, führt die Erhebung dieser Daten auch zur Verarbeitung personenbezogener Daten. Ungeachtet der Art, auf die diese Daten erhoben werden (einmalig oder ständig) sollte der Eigentümer einer solchen Datenbank die Verpflichtungen aus der Datenschutzrichtlinie erfüllen.

5.1.2 Anbieter von Geolokalisierungsanwendungen und -diensten

Intelligente mobile Endgeräte ermöglichen die Installation von Software Dritter, sogenannter *Anwendungen*. Solche Anwendungen können die Standortdaten (und andere Daten) von einem intelligenten mobilen Endgerät unabhängig von dem Entwickler des Betriebssystems und/oder dem für die Verarbeitung der Infrastruktur für die Geolokalisierung Verantwortlichen verarbeiten.

Beispiele solcher Dienste sind: Wettervorhersagen für die Regenwahrscheinlichkeit in den nächsten paar Stunden in einer ganz bestimmten Region; Dienste, die Informationen über nahegelegene Geschäfte anbieten; Dienste, die die Identifizierung eines verlorenen Mobiltelefons anbieten oder die den Standort von Freunden anzeigen.

---

[11] Das mobile Endgerät kann die verschiedenen Standortdaten, die es empfängt, übermitteln, damit der für die Verarbeitung Verantwortliche den Standort des Endgeräts berechnen kann oder damit es seinen Standort selbst berechnen kann. In beiden Fällen ist das Gerät ein wesentliches Mittel für die Verarbeitung.

Der Anbieter einer Anwendung, die zur Verarbeitung von Standortdaten fähig ist, ist der für die Verarbeitung der personenbezogenen Daten Verantwortliche, die aus der Installation und der Verwendung der Anwendung resultieren.

Natürlich ist es nicht immer erforderlich, gesonderte Software auf einem intelligenten mobilen Endgerät zu installieren. Viele Dienste zur Geolokalisierung sind auch über einen Browser zugänglich. Ein Beispiel hierfür ist die Nutzung einer Online-Karte, die eine Person durch eine Stadt führt.

5.1.3 Entwickler des Betriebssystems

Der Entwickler des Betriebssystems eines intelligenten mobilen Endgeräts kann ein für die Verarbeitung der Standortdaten Verantwortlicher sein, wenn das Endgerät direkt mit dem Nutzer interagiert und personenbezogene Daten erhebt (beispielsweise durch das Anfordern einer Erstregistrierung als Nutzer und/oder durch die Erhebung von Standortinformationen zur Verbesserung der Dienste). Als ein für die Verarbeitung Verantwortlicher muss der Entwickler die Grundsätze des eingebauten Datenschutzes anwenden, um eine heimliche Überwachung entweder durch das Endgerät selbst oder durch verschiedene Anwendungen und Dienste zu verhindern.

Ein Entwickler ist auch der für die Verarbeitung der Daten Verantwortliche, die er verarbeitet, wenn das Endgerät eine Phone-Home-Funktion für seinen Aufenthaltsort hat. Da in diesem Fall der Entwickler über die Mittel und Zwecke des Datenstroms entscheidet, ist er der für die Verarbeitung dieser Daten Verantwortliche. Ein verbreitetes Beispiel einer solchen „Phone-Home-Funktion“ ist die automatische Bereitstellung von Zeitzonen-Aktualisierungen basierend auf dem Standort.

Außerdem ist der Entwickler ein für die Verarbeitung Verantwortlicher, wenn er eine Werbeplattform anbietet und/oder eine Web-Shop-ähnliche Umgebung für Anwendungen und wenn das Gerät dazu in der Lage ist, personenbezogene Daten aus der Installation und Verwendung von Anwendungen zur Geolokalisierung unabhängig von dem Anbieter der Verwendung zu verarbeiten.

5.2 Verantwortlichkeiten Dritter

Es gibt zahlreiche Dritte, die Online tätig sind und die (weitere) Verarbeitung der Standortdaten ermöglichen. Dazu gehören Browser, soziale Netzwerke oder Kommunikationsmedien, die beispielsweise die „Georeferenzierung“ ermöglichen. Wenn sie auf ihrer Plattform Einrichtungen zur Geolokalisierung einbetten, haben sie eine wichtige Verantwortung für die Entscheidung bezüglich der Standardeinstellung der Anwendung (standardmäßig „an“ oder „aus“). Auch wenn sie nur in dem Ausmaß für die Verarbeitung Verantwortliche sind, in dem sie selbst aktiv personenbezogene Daten verarbeiten, haben sie beispielsweise in Bezug auf die Sichtbarkeit und Qualität der Informationen zur Verarbeitung von Geolokalisierungsdaten eine Schlüsselrolle in Bezug auf die Rechtmäßigkeit der Verarbeitung von Daten durch für die Verarbeitung Verantwortliche wie die Anbieter spezieller Anwendungen.

5.3 Berechtigter Grund

5.3.1 Intelligente mobile Endgeräte

Wenn Telekombetreiber die Daten der Basisstation nutzen wollen, um einem Kunden Dienste mit Zusatznutzen anzubieten, müssen sie nach der geänderten Datenschutzrichtlinie für elektronische Kommunikation die vorherige Einwilligung des Kunden einholen. Sie müssen auch sicherstellen, dass der Kunde über die Bedingungen der Verarbeitung informiert ist.

Angesichts der Sensibilität der Verarbeitung von (Mustern von) Standortdaten ist die *vorherige Einwilligung in Kenntnis der Sachlage* auch die wichtigste Grundlage, um die Verarbeitung von Daten in Bezug auf die Verarbeitung der Standorte eines intelligenten mobilen Endgeräts im Zusammenhang mit Diensten der Informationsgesellschaft zu legitimieren.

Gemäß Artikel 2 Buchstabe h der Datenschutzrichtlinie muss die Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage als freie Willensbekundung der betroffenen Person gegeben werden.

Abhängig von der Art der verwendeten Technologie spielt das Endgerät des Nutzers eine relativ aktive Rolle bei der Verarbeitung der Daten zur Bestimmung der Geoposition. Das Gerät kann Standortdaten von verschiedenen Quellen an jeden Dritten übertragen. Diese technische Fähigkeit sollte nicht mit der Rechtmäßigkeit einer solchen Datenverarbeitung verwechselt werden. Wenn die Standardeinstellungen eines Betriebssystems die Übertragung von Standortdaten ermöglicht, sollte das fehlende Einschreiten durch den Nutzer nicht fälschlicherweise als freiwillige Einwilligung missverstanden werden.

In dem Ausmaß, in dem Entwickler von Betriebssystem und andere Dienste der Informationsgesellschaft Standortdaten selbst aktiv verarbeiten (beispielsweise wenn sie Zugang zu Standortinformationen von oder durch das Gerät erhalten) müssen sie ebenfalls von ihren Nutzern die vorherige Einwilligung in Kenntnis der Sachlage einholen. Es muss klar sein, dass eine solche Einwilligung freiwillig weder durch die zwingende Annahme der allgemeinen Geschäftsbedingungen eingeholt werden kann noch durch die Möglichkeit zum Opt-out. Lokalisierungsdienste sollten standardmäßig ausgeschaltet sei. Die Standardeinstellung sollte „aus“ sein und der Nutzer sollte dann die Möglichkeit haben, stufenweise bei bestimmten Anwendungen auf „an“ zu stellen.

Einwilligung von Arbeitnehmern

Die Einwilligung als rechtmäßige Grundlage für die Verarbeitung ist im Beschäftigungsumfeld problematisch. In ihrer Stellungnahme zur Verarbeitung personenbezogener Daten von Beschäftigten schrieb die Datenschutzgruppe: *„Wird eine Einwilligung vom Beschäftigten erbeten und ist die Nichteinwilligung mit tatsächlichen oder potenziellen Nachteilen für ihn verbunden, so ist eine solche Einwilligung nicht gültig im Sinne von Artikel 7 oder Artikel 8, da sie nicht freiwillig erfolgt. Wenn der Arbeitnehmer keine Möglichkeit zur Ablehnung hat, kann nicht von Einwilligung gesprochen werden. (…) Probleme entstehen dort, wo die Einwilligung Einstellungsvoraussetzung ist. Der Arbeitnehmer hat theoretisch das Recht, die Einwilligung zu verweigern, aber er muss in diesem Fall damit rechnen, dass er die Chance auf eine bestimmte Stelle verliert. Unter solchen Umständen wird die Einwilligung nicht freiwillig erteilt und ist daher nicht gültig.“*[12] Statt die Einwilligung zu suchen, müssen Arbeitgeber prüfen, ob es nachweisbar erforderlich ist, den genauen Aufenthaltsort des Arbeitnehmers aus einem rechtmäßigen Grund zu überwachen. Dieses Erfordernis muss dann gegen die Grundrechte und Grundfreiheiten der Arbeitnehmer abgewogen werden. In den Fällen, in denen die Notwendigkeit angemessen gerechtfertigt werden kann, könnte die Rechtsgrundlage für die Verarbeitung auf dem berechtigten Interesse des für die Verarbeitung Verantwortlichen basieren (Artikel 7 Buchstabe f der Datenschutzrichtlinie). Der Arbeitgeber muss stets nach der am wenigsten einschneidenden Maßnahme suchen, eine ständige Überwachung vermeiden und beispielsweise ein System auswählen, das eine Warnung sendet, wenn ein Arbeitnehmer eine vorab gesetzte virtuelle Grenze überschreitet. Ein Arbeitnehmer muss die Möglichkeit haben, jedes Überwachungsgerät außerhalb der Arbeitszeiten auszuschalten. Es muss ihm gezeigt werden, wie das geht. Fahrzeugortungsgeräte sind keine Geräte zur Überwachung der Mitarbeiter. Ihre Funktion ist es, Fahrzeuge zu orten oder den Standort der Fahrzeuge zu überwachen, in denen sie eingebaut sind. Arbeitgeber sollten sie nicht als Gerät ansehen, mit dem sie das Verhalten oder den Aufenthaltsort von Fahrern oder anderen Mitarbeiten überprüfen können, indem sie beispielsweise Warnungen in Bezug auf die Geschwindigkeit des Fahrzeuges senden.

Einwilligung von Kindern

In einigen Fällen muss die Einwilligung von Kindern von ihren Eltern oder anderen gesetzlichen Vertretern gegeben werden. Das bedeutet beispielsweise, dass der Anbieter einer Anwendung zur Geolokalisierung die Eltern über die Erhebung und die Nutzung der Standortdaten ihrer Kinder informieren muss und ihre Einwilligung einholen muss, bevor er weiter Informationen über die Kinder erhebt und nutzt. Einige Anwendungen zur Geolokalisierung wurden speziell für die elterliche Überwachung entworfen. Sie zeigen beispielsweise ständig den Standort des Geräts auf einer Website an oder senden einen Alarm, wenn das Gerät ein vorher festgelegtes Gebiet verlässt. Die Nutzung solcher Anwendungen ist problematisch. In ihrer Stellungnahme 2/2009[13] zum Schutz der personenbezogenen Daten von Kindern schrieb die Artikel-29-Datenschutzgruppe: *Es sollte niemals vorkommen, dass Kinder aus Sicherheitsgründen mit einem Übermaß an Überwachung konfrontiert werden, die ihre Selbstbestimmung einschränken würde. Vor diesem Hintergrund gilt es, das*

[12] WP48, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten.

[13] WP160, Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen**).**

richtige Gleichgewicht zwischen dem Schutz der Intimität und Privatsphäre von Kindern und ihrer Sicherheit zu finden.

Der Rechtsrahmen sieht vor, dass Eltern dafür verantwortlich sind, dass das Recht der Kinder auf Privatsphäre gewährleistet ist. Wenn Eltern entscheiden, dass die Nutzung einer solchen Anwendung unter bestimmten Umständen berechtigt ist, müssen die Kinder wenigstens informiert werden. Sobald dies vernünftigerweise möglich ist, müssen sie an der Entscheidung über die Nutzung einer solchen Anwendung beteiligt werden.

Die Einwilligung muss für den konkreten Fall und für jeden der unterschiedlichen Zwecke gegeben werden, aus denen die Daten verarbeitet werden. Der für die Verarbeitung Verantwortliche muss es sehr deutlich klarstellen, ob sein Dienst darauf beschränkt ist, auf die freiwillige Frage „Wo bin ich jetzt gerade?“ eine Antwort zu geben oder ob sein Zweck darin besteht, Antworten auf die Fragen zu finden „Wo bist du, wo warst du und wo wirst du nächste Woche sein?“. Anders ausgedrückt: Der für die Verarbeitung Verantwortliche muss besondere Aufmerksamkeit auf die Einwilligung für die Zwecke richten, die die betroffene Person nicht erwartet, wie beispielsweise das Erstellen von Profilen und/oder Behavioural Targeting.

Wenn sich der Zweck der Verarbeitung grundlegend ändert, muss der für die Verarbeitung Verantwortliche erneut die Einwilligung für den konkreten Fall einholen. Wenn ein Unternehmen beispielsweise ursprünglich angegeben hat, es würde personenbezogene Daten Dritten nicht mitteilen, dies aber jetzt tun möchte, muss es die aktive vorherige Einwilligung jedes Kunden einholen. Eine ausbleibende Antwort (oder eine andere Art von Opt-out-Szenario) reicht nicht aus.

Es muss unterschieden werden zwischen der Einwilligung in einen einmaligen Dienst und in ein regelmäßiges Abonnement. Um beispielsweise einen bestimmten Dienst zur Geolokalisierung zu nutzen, kann es möglicherweise erforderlich sein, diesen Dienst an dem Gerät oder in dem Browser einzustellen. Wenn die Geolokalisierungsfunktion auf „an“ steht, kann jede Website die Standortdetails des Nutzers des betreffenden intelligenten mobilen Endgerätes lesen. Um die Risiken einer geheimen Überwachung zu verhindern, ist die Artikel-29-Datenschutzgruppe der Ansicht, dass das Gerät ständig warnen sollte, wenn der Geolokalisierungsdienst eingeschaltet ist. Das könnte beispielsweise mittels eines dauerhaft zu sehenden Icons gemacht werden.

Die Datenschutzgruppe empfiehlt den Anbietern von Geolokalisierungsanwendungen oder -diensten die individuelle Einwilligung nach einer angemessenen Zeitspanne zu erneuern (selbst, wenn keine Änderung in der Art der Verarbeitung erfolgt ist). Es wäre beispielsweise nicht richtig, Standortdaten weiterhin zu verarbeiten, wenn die betreffende Person den Dienst während der letzten zwölf Monate nicht aktiv genutzt hat. Selbst wenn eine Person den Dienst genutzt hat, sollte sie zumindest einmal im Jahr (oder häufiger, wenn die Art der Verarbeitung dies erforderlich macht) an die Art der Verarbeitung ihrer personenbezogenen Daten erinnert werden und es sollte ihr eine einfache Möglichkeit zum Ausschalten aufgezeigt werden.

Schließlich muss die betroffene Person die Möglichkeit haben, ihre Einwilligung auf eine sehr einfache Weise und ohne negative Auswirkungen auf die Verwendung des

Endgeräts zurückzuziehen. Unabhängig von den europäischen Datenschutzrichtlinien, hat das World Wide Web Consortium (W3C) einen Normentwurf für Geolocation API herausgegeben, der die Notwendigkeit der vorherigen, ausdrücklichen Einwilligung in Kenntnis der Sachlage betont.[14] W3C erklärt insbesondere , dass der Widerruf einer Einwilligung respektiert werden muss und rät denjenigen, die die Normen umsetzen, zu berücksichtigen, dass *„der unter einer bestimmte URL gespeicherte Inhalt sich so ändert, dass die vorher gewährten Standortgenehmigungen in Bezug auf den Nutzer nicht mehr zutreffen. Oder die Nutzer könnten einfach ihrer Meinung geändert haben.“*

Beispiel einer bewährten Praxis für Anbieter von Geolokalisierungsanwendungen

Eine Anwendung, die Standortdaten verwenden möchte, informiert den Nutzer deutlich über die Zwecke, für die die Daten genutzt werden sollen und erfragt die ausdrückliche Einwilligung für jeden möglichen Zweck. Der Nutzer wählt aktiv das Maß der Granularität der Geolokalisierung (beispielsweise auf Länderebene, Städteebene, Postleitzahlenebene oder so genau wie möglich). Sobald der Dienst zur Standortbestimmung aktiviert ist, ist ständig ein Icon auf jedem Bildschirm sichtbar, der anzeigt, dass die Dienste zur Standortbestimmung aktiviert sind. Der Nutzer kann seine Einwilligung jederzeit zurückziehen, ohne hierfür die Anwendung verlassen zu müssen. Der Nutzer hat auch die Möglichkeit, alle auf dem Endgerät gespeicherten Standortdaten einfach und dauerhaft zu löschen.

5.3.2 Wi-Fi-Zugangspunkte

Auf der Grundlage der Datenschutzrichtlinie können Unternehmen für den speziellen Zweck des Anbietens von Geolokalisierungsdiensten ein berechtigtes Interesse an der erforderlichen Erhebung und Verarbeitung von MAC-Adressen und errechneten Standorten von Wi-Fi-Zugangspunkten haben.

Der berechtigte Grund gemäß Artikel 7 Buchstabe f der Datenschutzrichtlinie erfordert ein Gleichgewicht zwischen dem berechtigten Interessen des für die Verarbeitung Verantwortlichen und den Grundrechten der betroffenen Personen. Angesichts der halbstatischen Natur der Wi-Fi-Zugangspunkte stellt das Kartografieren von Wi-Fi-Zugangspunkten im Prinzip eine geringere Gefahr für die Privatsphäre der Inhaber dieser Zugangspunkte dar, als die Standortortung in Echtzeit durch die intelligenten, mobilen Endgeräte.

Das Gleichgewicht zwischen den Rechten des für die Verarbeitung Verantwortlichen und den Rechten der betroffenen Personen ist dynamisch. Damit die für die Verarbeitung Verantwortlichen ihre berechtigten Interessen langfristig über die Interessen der betroffenen Personen stellen können, müssen sie Garantien einführen und umsetzen. Dazu gehört zum Beispiel das Recht, sich einfach und dauerhaft von der Datenbank abzumelden, ohne dem für die Verarbeitung dieser Datenbank Verantwortlichen zusätzliche personenbezogene Daten geben zu müssen. Sie können beispielsweise eine Software nutzen, die es automatisch feststellt, wenn eine Person mit einem bestimmten Zugangspunkt verbunden ist.[15]

---

14 W3C Geolocation API: http://www.w3.org/TR/geolocation-API/

15 Folgendes ist ein möglicher Anwendungsfall:

Darüber hinaus ist die Erhebung und Verarbeitung von SSIDs für das Anbieten von Geolokalisierungsdiensten nicht erforderlich. Deshalb geht die Erhebung und Verarbeitung von SSIDs über den Zweck des Anbietens von Geolokalisierungsdiensten hinaus, die auf dem Kartografieren des Standortes von Wi-Fi-Zugangspunkten basieren.

5.4 Information

Die verschiedenen für die Verarbeitung Verantwortlichen müssen sicherstellen, dass die Inhaber der intelligenten mobilen Endgeräte gemäß Artikel 10 der Datenschutzrichtlinie angemessen über die Schlüsselelemente der Verarbeitung informiert werden. Dazu zählen beispielsweise die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmung der Verarbeitung, die Art Daten, die Dauer der Verarbeitung, das Vorliegen von Auskunfts-, Berichtigungs- und Löschungsrechten der betroffenen Personen sowie ihr Recht, die Einwilligung zurückzuziehen.

Die Gültigkeit der Einwilligung ist untrennbar verbunden mit der Qualität der Informationen über den Dienst. Die Informationen müssen klar, umfassend und für ein breites, nicht technisch versiertes Publikum verständlich sowie ständig und einfach zugänglich sein.

Die Informationen müssen auf ein breites Publikum abgestimmt sein. Die für die Verarbeitung Verantwortlichen können nicht davon ausgehen, dass ihre Kunden allein weil sie ein intelligentes mobiles Endgerät haben, technisch versierte Personen sind. Die Informationen müssen altersgemäß sein, wenn der für die Verarbeitung Verantwortliche weiß, dass das Gerät jüngere Menschen anspricht.

Wenn Anbieter von Geolokalisierungsanwendungen den Standort eines Endgerätes häufiger als einmal berechnen wollen, müssen sie ihre Kunden so lange informieren, wie die die Standortdaten verarbeiten. Sie müssen es ihren Kunden auch ermöglichen, die Einwilligung zu verlängern oder zu widerrufen. Damit diese Ziele erreicht werden, sollten die Anbieter der Anwendungen eng mit dem Entwickler des Betriebssystems zusammenarbeiten. Der Entwickler ist technisch in der besten Position, eine dauerhaft sichtbare Erinnerung daran zu schaffen, dass die Standortdaten verarbeitet werden. Der Entwickler kann auch gut kontrollieren, dass keine Anwendungen angeboten werden, die den Standort der intelligenten mobilen Geräte heimlich überwachen.

---

1. Eine betroffene Person geht auf eine spezielle Website, über die sie die MAC-Adresse ihres Wi-Fi-Zugangspunktes eingeben kann.
2. Wenn die MAC-Adresse in der Datenbank mit den kartografierten Wi-Fi-Zugangspunkten erscheint, kann der für die Verarbeitung Verantwortliche eine Überprüfungsseite zeigen, die ein Skript enthält, das nach der ARP-Tabelle des Internetgeräts fragt. Theoretisch können die WLAN MAC-Adressen über den Befehl „ARP-a“ gezeigt werden. Mit Hilfe des Codes in dem Browser, wie Java, kann die ARP-Tabelle im Hintergrund produziert werden.
3. Wenn die MAC-Adresse in der ARP-Tabelle auftaucht, steht fest, dass der mit dem WLAN verbundene Nutzer auch der Nutzer mit dem Zugang zu der lokalen WLAN MAC-Adresse ist. Der für die Verarbeitung Verantwortliche überprüft auf diese Weise die Anfrage nach Löschung auf eine automatische und einfache Weise.

Wenn der Entwickler des Betriebssystems eine Phone-Home-Funktion oder andere Mittel des Zugangs zu auf dem Endgerät gespeicherten Daten geschaffen hat oder wenn er auf einem anderen Weg, beispielsweise durch dritte Werbetreibende, Zugang zu den Daten erhält, muss er die betroffene Person im Voraus über die (spezifischen und berechtigten) Zweckbestimmungen informieren, für die er diese Daten verarbeiten will. Er muss die betroffene Person auch über die Dauer der Verarbeitung informieren.

Die Verpflichtung zur Informierung der betroffenen Personen besteht auch für die für die Verarbeitung der Datenbanken mit geografisch bestimmten Wi-Fi-Zugangspunkten Verantwortlichen. Sie müssen die Allgemeinheit auf eine angemessene Weise über ihre Identität und die Zweckbestimmungen der Verarbeitung informieren und ihnen sonstige einschlägige Informationen geben. Die reine Erwähnung einer möglichen Erhebung von Daten über Wi-Fi-Zugangspunkte in einer speziellen Datenschutzerklärung, die auf die Nutzer einer Geolokalisierungsanwendung abzielt, reicht nicht aus. Es gibt genügend Mittel, sowohl Online als auch Offline, mit Hilfe derer die Allgemeinheit informiert werden kann.

5.5 Die Rechte der betroffenen Personen

Die betroffenen Personen haben das Recht, von den verschiedenen für die Verarbeitung Verantwortlichen Zugang zu den Standortdaten zu erhalten, die diese von den intelligenten mobilen Endgeräten erhoben haben. Sie haben auch ein Recht auf Informationen bezüglich der Zweckbestimmungen der Verarbeitung und der Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden. Die Information muss in einem Format erteilt werden, das von Menschen gelesen werden kann. Das heißt, es muss ein geografischer Standort genannt werden und nicht abstrakte Zahlen beispielsweise der Basisstationen.

Die betroffenen Personen haben auch ein Zugangsrecht zu den möglichen Profilen, die aufgrund dieser Standortdaten erstellt wurden. Wenn Standortdaten gespeichert werden, sollte es den Nutzern ermöglicht werden, diese zu aktualisieren, zu berichtigen oder zu löschen.

Die Datenschutzgruppe empfiehlt, dass die für die Verarbeitung Verantwortlichen sichere Wege suchen, mit denen Online ein direkter Zugang zu Standortdaten und möglichen Profilen bereitgestellt werden kann. Es ist unabdingbar, dass ein solcher Zugang ermöglicht wird, ohne weitere personenbezogene Daten zur Überprüfung der Identität der betroffenen Personen abzufragen.

5.6 Aufbewahrungsfristen

Anbieter von Geolokalisierungs- und Anwendungsdiensten sollten Aufbewahrungsfristen für die Standortdaten festlegen, die den Zeitraum nicht überstiegen, der für die Zwecke benötigt wird, für die die Daten erhoben wurden oder weiter verarbeitet werden. Sie müssen sicherstellen, dass Standortdaten oder die anhand dieser Daten erstellten Profile nach einem angemessenen Zeitraum gelöscht werden.

Sollte es für den Entwickler des Betriebssystems und/oder den für die Verarbeitung einer Infrastruktur zur Geolokalisierung Verantwortlichen nachweislich erforderlich sein, anonyme Standortdaten für den Zweck der Aktualisierung oder Verbesserung des Dienstes zu erheben, muss mit äußerster Sorgfalt vorgegangen werden, um zu vermeiden, dass die Daten (indirekt) erkennbar gemacht werden. Selbst wenn ein mobiles Endgerät mit einem wahllos zugewiesenen Unique Device Identifier (UDID) identifiziert wird, sollte eine solche Kennnummer maximal für die Dauer von 24 Stunden für Betriebszwecke gespeichert werden. Nach diesem Zeitraum sollte die UDID weiter anonymisiert werden. Dabei muss berücksichtigt werden, dass eine wahre Anonymisierung in zunehmendem Maße schwieriger wird und dass die kombinierten Standortdaten dennoch zu einer Identifizierung führen könnten. Eine solche UDID sollte weder mit früheren noch zukünftigen UDIDs des Endgeräts verknüpft werden können noch sollte sie mit einem festen Kennzeichen des Nutzers oder des Telefons (wie die MAC-Adresse, IMEI oder IMSI-Nummer oder einer sonstigen Kontonummer) verknüpfbar sein.

In Bezug auf die Daten über Wi-Fi-Zugangspunkte ist Folgendes zu beachten. Sobald die MAC-Adresse eines Wi-Fi-Zugangspunktes basierend auf der ständigen Beobachtung von Inhabern intelligenter, mobiler Endgeräte einem neuen Standort zugeordnet ist, muss der vorherige Standort umgehend gelöscht werden. So soll die weitere Nutzung der Daten für unangemessene Zwecke verhindert werden. Dazu zählt Marketing, das auf Personen abzielt, die ihren Standort gewechselt haben.

6. Schlussfolgerungen

Mit Hilfe von Technologien zur Geolokalisierung wie Daten von Basisstationen, GPS und kartografierten Wi-Fi-Zugangspunkten können intelligente, mobile Endgeräte durch alle möglichen für die Verarbeitung Verantwortlichen aufgespürt werden. Die Zwecke reichen hierbei von Behavioural Targeting zur Überwachung von Kindern.

Da Smartphones und Tablet-PCs untrennbar mit ihrem Inhaber verbunden sind, bieten die Bewegungsmuster dieser Endgeräte eine sehr persönliche Einsicht in das Privatleben ihrer Eigentümer. Eine der großen Gefahren ist, dass die Inhaber nicht wissen, dass sie ihren Standort übermitteln und an wen. Eine weitere, damit in Verbindung stehende Gefahr ist die Ungültigkeit der Einwilligung, dass bestimmte Anwendungen ihre Standortdaten nutzen dürfen, da die Schlüsselelemente der Verarbeitung unverständlich, veraltet oder ansonsten unzureichend sind.

Es bestehen verschiedene Verpflichtungen für die unterschiedlichen Betroffenen, von den Entwicklern der Betriebssysteme zu den Anbietern von Anwendungen und Dritten wie sozialen Netzwerken, die auf ihren Plattformen Funktionen der Standortbestimmung für mobile Endgeräte einbetten.

6.1 Rechtsrahmen

- Der EU-Rechtsrahmen für die Verwendung von Geolokalisierungsdaten von intelligenten mobilen Endgeräten ist in erster Linie die Datenschutzrichtlinie. Standortdaten von intelligenten mobilen Endgeräten sind personenbezogene Daten. Die Kombination aus der eindeutigen MAC-Adresse und dem berechneten Standort eines Wi-Fi-Zugangspunktes sollte als personenbezogene Daten behandelt werden.

- Darüber hinaus findet die überarbeitete Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG nur bei der Verarbeitung der Basisstationsdaten durch Telekombetreiber Anwendung.

6.2 Für die Verarbeitung Verantwortliche

- Es können die folgenden drei Arten von für die Verarbeitung Verantwortlichen unterschieden werden: für die Verarbeitung einer Infrastruktur für die Geolokalisierung Verantwortlicher (insbesondere für die Verarbeitung von kartografierten Wi-Fi-Zugangspunkten Verantwortlicher), Anbieter von Geolokalisierungsanwendungen und –diensten und Entwickler der Betriebssysteme intelligenter mobiler Endgeräte.

6.3 Berechtigte Gründe

- Da die Standortdaten intelligenter mobiler Endgeräte sehr persönliche Details über das Privatleben ihrer Nutzer offenlegen, ist der wichtigste berechtigte Grund die vorherige Einwilligung in Kenntnis der Sachlage.
- Die Einwilligung kann nicht durch allgemeine Geschäftsbedingungen eingeholt werden.
- Die Einwilligung muss für den konkreten Fall und für die verschiedenen Zwecke, aus denen die Daten verarbeitet werden, erteilt werden. Dazu gehören auch das Erstellen von Profilen oder Behavioural Targeting durch den für die Verarbeitung Verantwortlichen. Wenn sich der Zweck der Verarbeitung grundlegend ändert, muss der für die Verarbeitung Verantwortliche erneut die Einwilligung für den konkreten Fall einholen.
- Standortdienste müssen standardmäßig ausgeschaltet sein. Eine Möglichkeit zum Opt-out stellt keinen angemessenen Mechanismus zur Einholung der Einwilligung des Nutzers in Kenntnis der Sachlage dar.
- Die Einwilligung ist problematisch in Bezug auf Arbeitnehmer und Kinder. In Bezug auf Arbeitnehmer können Arbeitgeber diese Technologie nur dann anwenden, wenn sie nachweislich für einen rechtmäßigen Zweck erforderlich ist und dieselben Ziele nicht mit weniger einschneidenden Maßnahmen erreicht werden können. In Bezug auf Kinder müssen die Eltern beurteilen, ob die Nutzung einer solchen Anwendung unter bestimmten Umständen berechtigt ist. Sie müssen ihre Kinder zumindest informieren. Sobald es vernünftigerweise möglich ist, müssen die Kinder an der Entscheidung über die Nutzung einer solchen Anwendung beteiligt werden.
- Die Datenschutzgruppe empfiehlt, den Anwendungsbereich der Einwilligung zeitlich zu begrenzen und die Nutzer mindestens einmal im Jahr zu erinnern. Die Datenschutzgruppe empfiehlt auch eine ausreichende Granularität bei der Einwilligung in Bezug auf die Genauigkeit der Standortdaten.
- Die betroffenen Personen müssen die Möglichkeit haben, ihre Einwilligung auf eine sehr einfache Weise und ohne negative Auswirkungen auf die Verwendung des Endgeräts zurückzuziehen.
- In Bezug auf das Kartografieren von Wi-Fi-Zugangspunkten können Unternehmen ein berechtigtes Interesse an der erforderlichen Erhebung und Verarbeitung der MAC-Adressen und berechneten Standorte von Wi-Fi-Zugangspunkten für den speziellen Zweck haben, dass sie Geolokalisierungsdienste anbieten. Das Gleichgewicht der Interessen zwischen den Rechten des für die Verarbeitung Verantwortlichen und den Rechten der

betroffenen Personen macht es erforderlich, dass der für die Verarbeitung Verantwortliche die Möglichkeit des einfachen und dauerhaften Opt-out aus der Datenbank gibt, ohne zusätzliche personenbezogene Daten einzufordern.

6.4 Information

- Die Informationen müssen klar, umfassend und für ein breites, nicht technisch versiertes Publikum verständlich sowie ständig und einfach zugänglich sein. Die Gültigkeit der Einwilligung ist untrennbar verbunden mit der Qualität der Informationen über den Dienst.
- Dritte wie Browser und soziale Netzwerke spielen eine Schlüsselrolle in Bezug auf die Sichtbarkeit und Qualität der Informationen zur Verarbeitung von Geolokalisierungsdaten.

6.5 Die Rechte der betroffenen Personen

- Die verschiedenen für die Verarbeitung von Informationen zur Geolokalisierung von intelligenten mobilen Endgeräten Verantwortlichen sollten ihren Kunden den Zugang zu ihren Standortdaten in einem Format ermöglichen, das von Menschen gelesen werden kann. Die Nutzer sollten auch die Möglichkeit haben, die Daten zu ändern und zu löschen, ohne dass überflüssige personenbezogene Daten erhoben werden.
- Die betroffenen Personen haben auch das Recht, Zugang zu möglicherweise auf diesen Standortdaten erstellten Profilen zu nehmen, diese zu berichtigen oder zu löschen.
- Die Datenschutzgruppe empfiehlt das Einrichten eines (sicheren) Online-Zugangs.

6.6 Aufbewahrungsfristen

- Die Anbieter von Geolokalisierunganwendungen oder –diensten sollten Aufbewahrungspolitiken einführen, die sicherstellen, dass Daten zur Geolokalisierung oder anhand solcher Daten erstellte Profile nach einem angemessenen Zeitraum gelöscht werden.
- Wenn der Entwickler des Betriebssystems und/oder der für die Verarbeitung der Infrastruktur zur Geolokalisierung Verantwortliche eine Kennnummer wie die MAC-Adresse oder die UDID in Bezug auf die Standortdaten verarbeitet, darf die Kennnummer höchstens für die Dauer von 24 Stunden für Betriebszwecke gespeichert werden.

Brüssel, den 16. Mai 2011

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM