



881/11/NL
WP 185

Advies 13/2011 over geolocatiediensten op slimme mobiele apparaten

Goedgekeurd op 16 mei 2011

Deze groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Het is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer, waarvan de taken zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 15 van Richtlijn 2002/58/EG.

Het secretariaat wordt verzorgd door directoraat C (Grondrechten en burgerschap van de Unie) van het directoraat-generaal Justitie van de Europese Commissie, B-1049 Brussel, België, kamer MO-59 02/013.

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

INHOUD

1. Inleiding	3
2. Context: verschillende geolocatie-infrastructuren	4
2.1 Gegevens van basisstations	4
2.2 Gps-technologie	5
2.3 WiFi	5
2.3.1 WiFi-toegangspunten	5
3. Risico's voor de privacy	7
4. Wettelijk kader	8
4.1 Door telecombedrijven verwerkte basisstationgegevens	8
4.2 Door verleners van diensten van de informatiemaatschappij verwerkte basisstation-, WiFi- en gps-gegevens	9
4.2.1 Toepasbaarheid van de gewijzigde e-privacyrichtlijn	9
4.2.2 Toepasbaarheid van de gegevensbeschermingsrichtlijn	10
5. Verplichtingen die voortvloeien uit wetgeving inzake gegevensbescherming	12
5.1 Voor de gegevensverwerking verantwoordelijke	12
5.1.1 Voor de verwerking van met behulp van geolocatie-infrastructuur verzamelde gegevens verantwoordelijken	13
5.1.2 Aanbieders van geolocatieapplicaties en -diensten	13
5.1.3 Ontwikkelaar van het besturingssysteem	14
5.2 Verantwoordelijkheden van andere partijen	14
5.3 Legitieme grond	15
5.3.1 Slimme mobiele apparaten	15
5.3.2 WiFi-toegangspunten	18
5.4 Informatie	19
5.5 Rechten van betrokkenen	20
5.6 Bewaartermijnen	20
6. Conclusies	21

DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS,

ingesteld bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

gezien artikel 29 en artikel 30, lid 1, onder a), en lid 3, van die richtlijn,

gezien het reglement van orde van de Groep,

HEEFT HET VOLGENDE ADVIES GOEDGEKEURD:

1. Inleiding

Geografische informatie speelt een belangrijke rol in onze samenleving. Bijna alle menselijke activiteiten en besluiten hebben een geografische component. Over het algemeen neemt de waarde van informatie toe wanneer deze is gekoppeld aan een locatie. Allerlei soorten informatie kunnen aan een geografische locatie worden gekoppeld, zoals financiële gegevens, gegevens over de gezondheidszorg die iemand ontvangt en andere gegevens over het gedrag van consumenten. Met de snelle technologische ontwikkeling en de brede ingebruikneming van slimme mobiele apparaten ontwikkelt zich een hele nieuwe categorie van op locatie gebaseerde diensten.

Het doel van dit advies is om meer helderheid te verschaffen over het wettelijk kader dat van toepassing is op geolocatediensten die beschikbaar zijn op en/of worden gegenereerd door slimme mobiele apparaten die verbinding kunnen maken met internet en zijn uitgerust met locatiegevoelige sensoren, zoals gps-sensoren. Voorbeelden hiervan zijn het aanbieden van plattegronden en navigatiediensten, gepersonaliseerde geodiensten (zoals het aangeven van interessante punten in de omgeving), augmented reality, geocodering van informatie op internet, het volgen van waar vrienden zich bevinden, het controleren van kinderen en locatiegebonden reclame.

Dit advies heeft ook betrekking op de drie belangrijkste soorten infrastructuur die worden gebruikt om geolocatediensten aan te bieden, namelijk gps, gsm-basisstations en WiFi. Bijzondere aandacht wordt besteed aan de nieuwe infrastructuur die is gebaseerd op de locatie van WiFi-toegangspunten.

De Groep is zich ervan bewust dat er vele andere diensten bestaan die locatiegegevens verwerken en die ook vragen met betrekking tot gegevensverwerking kunnen oproepen, zoals e-ticketsystemen, tolsystemen voor auto's, satellietnavigatiediensten, locatiebepaling met behulp van bijvoorbeeld camera's en geolocatie van IP-adressen. Gezien de snelle technologische ontwikkelingen, met name op het gebied van het in kaart brengen van draadloze toegangspunten, samen met het feit dat nieuwe spelers in de markt klaar staan om nieuwe locatiegebonden diensten te ontwikkelen op basis van een combinatie van basisstation-, gps- en WiFi-gegevens, heeft de Groep besloten om in het bijzonder de wettelijke voorschriften te verduidelijken waaraan deze specifieke diensten krachtens de gegevensbeschermingsrichtlijn moeten voldoen.

In dit advies wordt eerst de technologie beschreven. Vervolgens worden de risico's voor de privacy vastgesteld en beoordeeld, waarna conclusies worden getrokken over de toepassing van de relevante wetsartikelen op verschillende voor de gegevensverwerking verantwoordelijken die van mobiele apparaten afgeleide locatiegegevens verzamelen en verwerken, waaronder aanbieders van geolocatie-infrastructuur, fabrikanten van smartphones en ontwikkelaars van op geolocatie gebaseerde applicaties.

In dit advies zal geen beoordeling worden gegeven van de specifieke geocoderingstechnologie die verband houdt met het zogeheten 'web 2.0', waarbij gebruikers aan de geografische context gerelateerde informatie in sociale netwerken als Facebook en Twitter integreren. Ook zal in dit advies niet gedetailleerd worden ingegaan op enkele andere geolocatietechnologieën die worden gebruikt om apparaten in een relatief beperkt gebied (winkelcentra, luchthavens, kantoorgebouwen, enz.) met elkaar te verbinden, zoals Bluetooth, ZigBee, elektronische gebiedsafbakening ('geofencing') en op WiFi gebaseerde RFID-tags, hoewel veel van de conclusies in dit advies met betrekking tot de legitieme grond, het informeren van personen waarop gegevens betrekking hebben (hierna: de "betrokkenen") en de rechten van deze personen ook op deze technologieën van toepassing zijn wanneer ze worden gebruikt om personen met behulp van apparaten te lokaliseren.

2. Context: verschillende geolocatie-infrastructuren

2.1 Gegevens van basisstations

Het gebied dat door de verschillende aanbieders van telecommunicatiediensten wordt bestreken, is onderverdeeld in kleinere gebieden, die 'cellen' worden genoemd. Om een mobiele telefoon te kunnen gebruiken of om met behulp van 3G-communicatie verbinding met internet te maken, moet het mobiele apparaat verbinding maken met de antenne (hierna: het "basisstation") die de desbetreffende cel bestrijkt. De omvang van de cellen verschilt, afhankelijk van de interferentie met bijvoorbeeld bergen of hoge gebouwen.

De hele tijd dat een mobiel apparaat is ingeschakeld, is het verbonden met een specifiek basisstation. Het telecombedrijf registreert deze verbindingen voortdurend. Elk basisstation heeft een unieke ID en is geregistreerd met een specifieke locatie. Zowel het telecombedrijf als veel mobiele apparaten zelf kunnen signalen van overlappende cellen (aangrenzende basisstations) gebruiken om de positie van het apparaat met een grotere precisie te kunnen bepalen. Deze techniek wordt ook wel triangulatie genoemd.

De precisie kan verder worden vergroot met behulp van informatie als RSSI (Received Signal Strength Indicator), TDOA (Time Difference of Arrival) en AOA (Angle Of Arrival).

Gegevens van basisstations kunnen worden gebruikt in innovatieve toepassingen, bijvoorbeeld om files te detecteren. Voor elke weg kan voor elk deel van de dag een

gemiddelde snelheid worden vastgesteld, dus wanneer de overgang naar het volgende basisstation langer duurt dan verwacht, is er kennelijk een file.

Deze plaatsbepalingsmethode levert derhalve een snelle, ruwe indicatie van de locatie op, die in vergelijking met gps- en WiFi-gegevens echter weinig precies is. De betrouwbaarheidsmarge bedraagt in dichtbevolkte stedelijke gebieden ongeveer vijftig meter, maar kan in rurale gebieden oplopen tot enkele kilometers.

2.2 Gps-technologie

Slimme mobiele apparaten hebben ingebouwde chipsets met gps-ontvangers die hun locatie bepalen.

Gps-technologie maakt gebruik van 31 satellieten die elk in een van zes verschillende banen om de aarde draaien¹. Elke satelliet zendt een zeer precies radiosignaal uit.

Het mobiele apparaat kan zijn locatie bepalen wanneer de gps-sensor ten minste vier van deze signalen opvangt. Anders dan het geval is bij basisstations, gaat het signaal hierbij maar één richting op. De beheerders van de satellieten kunnen de apparaten die het radiosignaal ontvangen dus niet volgen.

Met gps-technologie kunnen posities worden bepaald met een nauwkeurigheid van vier tot vijftien meter. Het belangrijkste nadeel van gps is dat het relatief langzaam opstart². Een ander nadeel is dat gps in gebouwen niet of niet goed werkt. In de praktijk wordt gps-technologie daarom vaak gecombineerd met gegevens van basisstations en/of in kaart gebrachte Wifi-toegangspunten.

2.3 WiFi

2.3.1 WiFi-toegangspunten

Een relatief nieuwe bron van geolocatie-informatie is het gebruik van WiFi-toegangspunten. De technologie is vergelijkbaar met die van basisstations. Beide zijn gebaseerd op een unieke ID (van het basisstation of het WiFi-toegangspunt) die door een mobiel apparaat kan worden gedetecteerd en kan worden verzonden aan een dienst die de unieke ID aan een locatie koppelt.

¹ Het Global Positioning System (gps) bestaat uit satellieten die door de Verenigde Staten van Amerika voor militaire doeleinden in een baan om de aarde zijn gebracht. De Europese Commissie streeft ernaar om Galileo, het uit achttien satellieten bestaande navigatienetwerk van de EU dat gratis, niet-militaire plaatsbepaling zal aanbieden, vanaf 2014 operationeel te maken. De eerste twee satellieten zullen in 2011 worden gelanceerd, en de volgende twee in 2012. Bron: Europese Commissie, 'Commission presents midterm review of Galileo and EGNOS', 25 januari 2011, URL: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&item_id=4835.

² Om de initiële detectie van het gps-signaal te versnellen, kunnen zogeheten regenboogtabellen (tabellen met de verwachte posities van de verschillende satellieten voor de komende weken) worden geladen.

De unieke ID van elk WiFi-toegangspunt is het MAC-adres (Medium Access Control). Een MAC-adres is een uniek identificatienummer dat wordt toegekend aan een netwerkinterface en doorgaans wordt vastgelegd in hardware als geheugenchips en/of netwerkkarten in computers, telefoons, laptops of toegangspunten³.

De reden dat WiFi-toegangspunten als bron van geolocatie-informatie kunnen worden gebruikt, is dat ze hun bestaan voortdurend bekendmaken. De meeste toegangspunten voor breedbandinternet hebben standaard ook een WiFi-antenne. De standaardinstelling van de meest gebruikte toegangspunten in Europa is dat deze verbinding 'aan' staat, ook als de gebruiker zijn of haar computer(s) alleen via een kabel met het toegangspunt heeft verbonden. Op vergelijkbare wijze als een radio zendt het WiFi-toegangspunt voortdurend zijn eigen netwerknaam en MAC-adres uit, ook als niemand de verbinding gebruikt en als de inhoud van de draadloze communicatie is versleuteld met WEP, WPA of WPA2.

Er zijn twee verschillende manieren om de MAC-adressen van WiFi-toegangspunten te verzamelen⁴:

1. Actieve scanning: hierbij worden actieve verzoeken⁵ aan alle nabijgelegen WiFi-toegangspunten gestuurd en de antwoorden vastgelegd. Deze antwoorden bevatten geen informatie over apparaten die met de WiFi-toegangspunten zijn verbonden.
2. Passieve scanning: hierbij worden de 'beacon frames' die door elk toegangspunt periodiek worden uitgezonden (over het algemeen tien keer per seconde) vastgelegd. Als niet-standaard alternatief registreren enkele instrumenten alle WiFi-frames die door toegangspunten worden uitgezonden, ook de frames die geen bakensignalen uitzenden. Als dit type scanning met opzet zonder behoorlijke bescherming van de persoonlijke levenssfeer wordt uitgevoerd, is het mogelijk om gegevens die tussen toegangspunten en daarmee verbonden apparaten worden uitgewisseld te verzamelen. Op deze manier kunnen de MAC-adressen van desktopcomputers, laptops en printers worden vastgelegd. Dit type scanning kan ook leiden tot het illegaal vastleggen van de inhoud van de communicatie. Deze inhoud is gemakkelijk leesbaar als de eigenaar van het WiFi-toegangspunt de WiFi-versleuteling (WEP/WPA/WPA2) niet heeft geactiveerd.

De locatie van een WiFi-toegangspunt kan op twee verschillende manieren worden berekend.

1. Statisch/eenmalig: voor de gegevensverwerking verantwoordelijken verzamelen zelf de MAC-adressen van WiFi-toegangspunten door rond te rijden in met antennes uitgeruste voertuigen en op het moment dat het signaal wordt opgevangen de exacte lengte/breedtecoördinaten van het voertuig te registreren. Vervolgens kunnen ze de

³ Een voorbeeld van een MAC-adres is: 00-1F-3F-D7-3C-58. Het MAC-adres van een WiFi-toegangspunt wordt de BSSID (Basic Service Set Identifier) genoemd.

⁴ Actieve en passieve scanning om toegangspunten te detecteren zijn gestandaardiseerd in IEEE 802.11.

⁵ Om de MAC-adressen te verzamelen zendt de verzamelaar een zogeheten 'probe request' aan alle toegangspunten.

locatie van de toegangspunten berekenen op basis van onder meer de sterkte van het signaal.

2. Dynamisch/doorlopend: gebruikers van geolocatiediensten verzamelen automatisch de MAC-adressen die door hun met WiFi uitgeruste apparaten worden waargenomen wanneer ze bijvoorbeeld een onlineplattegrond gebruiken om hun eigen positie te bepalen (Waar ben ik?). Het mobiele apparaat zendt vervolgens alle beschikbare informatie naar de aanbieder van de geolocatiedienst, waaronder MAC-adressen, SSID's en de signaalsterkte. De voor de gegevensverwerking verantwoordelijke kan deze doorlopende waarnemingen gebruiken om de locaties van de WiFi-toegangspunten te berekenen en/of de in zijn databank van in kaart gebrachte WiFi-toegangspunten opgeslagen locaties te verbeteren.

Het is belangrijk om op te merken dat mobiele apparaten geen 'verbinding' met WiFi-toegangspunten hoeven te maken om WiFi-informatie te kunnen verzamelen. De mobiele apparaten detecteren de aanwezigheid van de toegangspunten automatisch (in de actieve of de passieve scanningmodus) en verzamelen automatisch gegevens over deze toegangspunten.

Bovendien zullen mobiele telefoons die een verzoek om geolocatie versturen niet alleen WiFi-gegevens verzenden, maar ook alle andere informatie over de locatie waarover ze beschikken, waaronder gps- en basisstationgegevens. Hierdoor kan de aanbieder van de dienst de locatie van de 'nieuwe' WiFi-toegangspunten berekenen en/of de locaties van WiFi-toegangspunten die al in de databank zijn opgenomen verbeteren. Op deze manier wordt het verzamelen van informatie over WiFi-toegangspunten op een heel efficiënte wijze gedecentraliseerd, zonder dat de klanten zich daar noodzakelijkerwijs bewust van zijn.

Samenvattend kan worden gezegd dat geolocatie op basis van WiFi-toegangspunten tot een snelle en op basis van doorlopende metingen steeds preciezere plaatsbepaling leidt.

3. Risico's voor de privacy

Een slim mobiel apparaat is zeer nauw verbonden met een specifieke persoon. De meeste mensen zijn geneigd om hun mobiele apparaten dicht bij zich te houden, zoals in een broek- of jaszak, in een tas of op het nachtkastje naast het bed.

Het gebeurt zelden dat iemand een dergelijk apparaat aan een ander uitleent. De meeste mensen zijn zich ervan bewust dat hun mobiele apparaat zeer persoonlijke informatie bevat, variërend van e-mails tot privéfoto's en van hun browsegeschiedenis tot bijvoorbeeld een contactlijst.

Hierdoor kunnen aanbieders van geolocatiediensten een gedetailleerd overzicht van de gewoonten en patronen van de eigenaar van het apparaat verkrijgen en uitgebreide profielen opstellen. Zo kan uit een patroon van inactiviteit in de nacht de slaapplek worden afgeleid en uit een regelmatig reispatroon in de ochtend de locatie van de

werkgever. Het patroon kan ook gegevens omvatten die zijn afgeleid uit bewegingspatronen van vrienden, op basis van zogeheten ‘social graphs’⁶.

Een gedragspatroon kan ook *speciale categorieën gegevens* opleveren, bijvoorbeeld wanneer dat patroon duidt op bezoeken aan ziekenhuizen of religieuze plaatsen, de aanwezigheid bij politieke demonstraties of de aanwezigheid op andere specifieke locaties die gegevens over bijvoorbeeld iemands seksleven kunnen opleveren. Deze profielen kunnen worden gebruikt om besluiten te nemen die voor de eigenaar belangrijke gevolgen kunnen hebben.

De technologie van slimme mobiele apparaten maakt voortdurende monitoring van locatiegegevens mogelijk. Smartphones kunnen permanent signalen van basisstations en WiFi-toegangspunten verzamelen. Technisch gezien kan de monitoring heimelijk worden gedaan, zonder dat de eigenaar erover wordt geïnformeerd. Monitoring kan ook op semigeheime wijze plaatsvinden, wanneer mensen zijn ‘vergeten’ of niet naar horen zijn geïnformeerd dat locatiediensten ‘aan’ staan, of wanneer de instellingen voor de toegankelijkheid van locatiegegevens worden veranderd van ‘privé’ in ‘openbaar’.

Zelfs wanneer mensen hun geolocatiegegevens bewust toegankelijk maken op internet, via plaatsbepalings- en geocoderingsdiensten, leidt de onbeperkte algemene toegang tot nieuwe risico’s, van diefstal van gegevens en inbraak tot zelfs fysieke agressie of stalkgedrag.

Zoals ook geldt voor andere nieuwe technologieën, is een belangrijk risico van het gebruik van locatiegegevens dat het aantal functies waarvoor de gegevens worden gebruikt sluipenderwijs wordt uitgebreid (‘function creep’). Hierbij worden op basis van de beschikbaarheid van nieuwe typen gegevens nieuwe toepassingen ontwikkeld die ten tijde van de oorspronkelijke verzameling van de gegevens niet werden voorzien.

4. Wettelijk kader

Het relevante wettelijk kader is de gegevensbeschermingsrichtlijn (Richtlijn 95/46/EG). Deze richtlijn is van toepassing in alle gevallen waarin persoonsgegevens worden verwerkt als gevolg van de verwerking van locatiegegevens. De e-privacyrichtlijn (Richtlijn 2002/58/EG, als gewijzigd bij Richtlijn 2009/136/EG) is alleen van toepassing op de verwerking van gegevens van basisstations door openbare elektronischecommunicatiediensten en -netwerken (telecombedrijven).

4.1 Door telecombedrijven verwerkte basisstationgegevens

Telecombedrijven verwerken in het kader van de levering van openbare elektronischecommunicatiediensten voortdurend gegevens van basisstations⁷. Ook

⁶ ‘Social graph’ is een term die betrekking heeft op de zichtbaarheid van vrienden in sociale netwerken op internet en het vermogen om uit gegevens over deze vrienden gedragspatronen af te leiden.

⁷ Opgemerkt dient te worden dat het aanbieden van openbare WiFi-hotspots door telecombedrijven ook wordt aangemerkt als een openbare elektronischecommunicatiedienst en derhalve primair moet voldoen aan de bepalingen van de e-privacyrichtlijn.

kunnen ze dit soort gegevens verwerken om diensten met toegevoegde waarde te verstrekken. Hierover heeft de Groep al geschreven in advies 5/2005 (WP115). Hoewel enkele voorbeelden die in dit advies worden gegeven door de verspreiding van internettechnologieën en het gebruik van sensoren in steeds kleinere apparaten onvermijdelijk achterhaald zijn, blijven de conclusies en aanbevelingen geldig voor het gebruik van basisstationgegevens.

1. Aangezien uit basisstationgegevens afgeleide locatiegegevens een geïdentificeerde of identificeerbare natuurlijke persoon betreffen, zijn ze onderworpen aan de in Richtlijn 95/46/EG van 24 oktober 1995 neergelegde bepalingen inzake de bescherming van persoonsgegevens.
2. Ook Richtlijn 2002/58/EG van 12 juli 2002 (als gewijzigd, in november 2009, bij Richtlijn 2009/136/EG) is van toepassing, op grond van de definitie die in artikel 2, onder c), van deze richtlijn wordt gegeven:
“locatiegegevens”: gegevens die worden verwerkt in een elektronischecomunicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker van een algemeen beschikbare elektronischecomunicatiedienst wordt aangegeven;

Als een telecombedrijf een hybride geolocatedienst aanbiedt die mede is gebaseerd op de verwerking van andere typen locatiegegevens, zoals gps- of WiFi-gegevens, wordt deze activiteit als een openbare elektronischecomunicatiedienst aangemerkt. Het telecombedrijf moet voor voorafgaande toestemming van de klant zorgen voordat het deze geolocatiegegevens aan een derde partij verstrekt.

4.2 Door verleners van diensten van de informatiemaatschappij verwerkte basisstation-, WiFi- en gps-gegevens

4.2.1 Toepasbaarheid van de gewijzigde e-privacyrichtlijn

Locatiediensten en -applicaties die op basis van een combinatie van basisstation-, Wifi- en gps-gegevens worden aangeboden zijn *diensten van de informatiemaatschappij*. Als zodanig zijn ze expliciet uitgesloten van het toepassingsgebied van de e-privacyrichtlijn, op grond van de nauwkeurige definitie van elektronischecomunicatiediensten (artikel 2, onder c, van de herziene kaderrichtlijn (ongewijzigd))⁸.

De e-privacyrichtlijn is niet van toepassing op de verwerking van locatiegegevens door diensten van de informatiemaatschappij, ook niet wanneer die verwerking via een openbaar elektronischecomunicatienetwerk plaatsvindt. Een gebruiker kan

⁸ Richtlijn 2002/21/EG van 7 maart 2002, artikel 2, onder c): “elektronischecomunicatiedienst”: een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronischecomunicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronischecomunicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Hij omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van Richtlijn 98/34/EG, die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronischecomunicatienetwerken;

ervoor kiezen om gps-gegevens via internet uit te zenden, bijvoorbeeld bij het gebruik van navigatiediensten op internet. In dat geval wordt het gps-signaal uitgezonden op het applicatieniveau van de internetcommunicatie, onafhankelijk van het gsm-netwerk en is de aanbieder van de telecommunicatiedienst louter het kanaal. Zonder zeer ingrijpende middelen toe te passen, zoals ‘deep packet inspection’, kan hij geen toegang verkrijgen tot gps- en/of WiFi- en/of basisstationgegevens die naar en vanuit een slim mobiel apparaat tussen een gebruiker/abonnee en een dienst van de informatiemaatschappij worden gecommuniceerd.

4.2.2 Toepasbaarheid van de gegevensbeschermingsrichtlijn

Wanneer de gewijzigde e-privacyrichtlijn niet van toepassing is, is volgens artikel 1, lid 2, van de e-privacyrichtlijn Richtlijn 95/46/EG van toepassing: *“Met het oog op de verwezenlijking van de in lid 1 vermelde doelstellingen, vormt het bepaalde in deze richtlijn een specificatie van en een aanvulling op Richtlijn 95/46/EG.”*

Volgens de gegevensbeschermingsrichtlijn zijn persoonsgegevens *“iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna “betrokkene” te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit”* (artikel 2, onder a) van de richtlijn).

In overweging 26 van de richtlijn wordt speciale aandacht besteed aan de term "identificeerbaar", in de zinsnede *“dat, om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs, door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon, in te zetten zijn om genoemde persoon te identificeren.”*

In overweging 27 van de richtlijn wordt het brede toepassingsgebied van de bescherming toegelicht: *“de reikwijdte van deze bescherming [mag] in feite niet afhankelijk (...) zijn van de gebruikte technieken, omdat zulks ernstig gevaar voor ontduiking zou opleveren;”*

In zijn advies 4/2007 over het begrip persoonsgegevens heeft de Groep een uitgebreide toelichting op de definitie van persoonsgegevens gegeven.

Slimme mobiele apparaten

Slimme mobiele apparaten zijn onlosmakelijk verbonden met natuurlijke personen. Over het algemeen is er sprake van directe en indirecte identificeerbaarheid.

In de eerste plaats houdt het telecombedrijf dat de toegang tot het gsm-netwerk en mobiel internet aanbiedt doorgaans een register bij met de naam, het adres en de bankgegevens van elke klant, in combinatie met verschillende unieke nummers van het apparaat, zoals het IMEI- en het IMSI-nummer.

In de tweede plaats wordt bij de aanschaf van extra software voor het apparaat (*applicaties* of *apps*) doorgaans een creditcardnummer verlangd en wordt de combinatie van het unieke nummer of de unieke nummers en de locatiegegevens op

die manier verrijkt met gegevens die direct kunnen worden gebruikt om een persoon te identificeren.

Indirecte identificeerbaarheid kan worden bereikt door het unieke nummer of de unieke nummers van het apparaat te combineren met een of meer berekende locaties.

Elk slim mobiel apparaat heeft ten minste één uniek identificatienummer, het MAC-adres. Het apparaat kan ook andere unieke identificatienummers hebben, die door de ontwikkelaar van het besturingssysteem zijn toegevoegd. Deze identificatienummers kunnen worden verzonden en verder worden verwerkt in het kader van geolocatiediensten. Het is een feit dat de locatie van een specifiek apparaat heel precies kan worden berekend, vooral wanneer verschillende geolocatie-infrastructuren worden gecombineerd. Deze locatie kan een woning of een werkplek zijn. Met name bij herhaalde waarnemingen is het mogelijk om de eigenaar van het apparaat te identificeren.

Bij het vaststellen van de middelen die beschikbaar zijn voor het tot stand brengen van identificeerbaarheid moet rekening worden gehouden met de ontwikkeling dat mensen steeds meer persoonlijke locatiegegevens op internet bekendmaken, bijvoorbeeld door de locatie van hun woning of werkplek samen met andere identificatiegegevens te publiceren. Dit kan ook gebeuren zonder dat ze het weten, als andere personen hen geocoderen. Deze ontwikkeling maakt het gemakkelijker om een locatie of gedragspatronen aan een specifieke persoon te koppelen.

Bovendien moet worden opgemerkt, op basis van advies 4/2007 over het begrip persoonsgegevens, dat een uniek identificatienummer het in de hierboven beschreven context mogelijk maakt om een gebruiker van een specifiek apparaat te traceren, en de gebruiker derhalve kan worden “geselecteerd”, ook al is zijn of haar naam niet bekend.

WiFi-toegangspunten

Deze indirecte identificeerbaarheid is ook van toepassing op WiFi-toegangspunten⁹. Het MAC-adres van een WiFi-toegangspunt, in combinatie met de berekende locatie ervan, is onlosmakelijk verbonden met de eigenaar van het toegangspunt.

Een redelijk uitgeruste voor de gegevensverwerking verantwoordelijke kan de locatie van een WiFi-toegangspunt op basis van de signaalsterkte en de voortdurende updates van de locatie door de gebruikers van zijn geolocatiedienst steeds nauwkeuriger berekenen.

Met behulp van deze middelen kan in veel gevallen een kleine groep appartementen of huizen worden geïdentificeerd, waaronder zich de woning van de eigenaar van het toegangspunt moet bevinden. Het gemak waarmee deze eigenaar op basis van het MAC-adres kan worden geïdentificeerd is afhankelijk van de omgeving:

- in dunbevolkte gebieden, waar het MAC-adres naar één huis leidt, kan de eigenaar van een woning rechtstreeks worden geïdentificeerd met

⁹ WiFi-toegangspunten kunnen ook direct identificeerbaar zijn, als de aanbieder van de toegang tot internet een register bijhoudt van de MAC-adressen van de WiFi-routers die hij aan zijn geïdentificeerde klanten aanbiedt.

instrumenten als bijvoorbeeld registers van huiseigenaren, telefoongidsen, kiesregisters of zelfs een eenvoudige zoekopdracht aan een zoekmachine¹⁰;

- in dichter bevolkte gebieden kan de exacte locatie van het toegangspunt worden bepaald met behulp van bijvoorbeeld de signaalsterkte en/of de SSID (die iedereen met een apparaat dat met WiFi kan worden verbonden kan detecteren). In veel gevallen kan zo de identiteit van de bewoner of de bewoners van de woning waar het toegangspunt zich bevindt worden vastgesteld;
- in zeer dichtbevolkte gebieden zal het MAC-adres, ook als er informatie over de signaalsterkte beschikbaar is, op verschillende appartementen wijzen als mogelijke locatie van het toegangspunt. In deze omstandigheden is het zonder onredelijke inspanningen niet mogelijk om precies vast te stellen wie de bewoner is van het appartement waar het toegangspunt zich bevindt.

Het feit dat de eigenaar van het apparaat op dit moment in bepaalde gevallen niet kan worden geïdentificeerd zonder onredelijke inspanningen te doen, staat niet in de weg van de algemene conclusie dat de combinatie van een MAC-adres van een WiFi-toegangspunt en de berekende locatie van het toegangspunt moet worden behandeld als een persoonsgegeven.

In deze omstandigheden, en in aanmerking nemend dat het onwaarschijnlijk is dat de voor de gegevensverwerking verantwoordelijke onderscheid kan maken tussen gevallen waarin de eigenaar van het WiFi-toegangspunt identificeerbaar is en gevallen waarin dat niet het geval is, moet de voor de gegevensverwerking verantwoordelijke alle gegevens over WiFi-routers als persoonsgegevens behandelen.

Het is belangrijk om eraan te herinneren dat het doel van de verwerking van deze geolocatiegegevens de identificatie van de gebruikers is. Of voor de identificatie van de eigenaars van de WiFi-toegangspunten onredelijke inspanningen nodig zijn, wordt sterk beïnvloed door de technische mogelijkheden waarover de voor de gegevensverwerking verantwoordelijke of iemand anders beschikt om deze eigenaars te identificeren.

5. Verplichtingen die voortvloeien uit wetgeving inzake gegevensbescherming

5.1 Voor de gegevensverwerking verantwoordelijke

In de context van door diensten van de informatiemaatschappij aangeboden onlinegeolocatediensten kunnen drie verschillende functies worden onderscheiden, die behoren bij verschillende verantwoordelijkheden voor de verwerking van persoonsgegevens. Deze zijn: voor de gegevensverwerking verantwoordelijke, aanbieder van een specifieke geolocatieapplicatie of -dienst en ontwikkelaar van het besturingssysteem van een slim mobiel apparaat. In de praktijk vervullen veel ondernemingen meerdere rollen tegelijk, bijvoorbeeld wanneer ze een besturingssysteem combineren met een databank van in kaart gebrachte WiFi-toegangspunten en een advertentieplatform.

¹⁰ De beschikbaarheid van dergelijke registers of gidsen verschilt per lidstaat.

5.1.1 Voor de verwerking van met behulp van geolocatie-infrastructuur verzamelde gegevens verantwoordelijken

Net als telecombedrijven, wanneer deze met behulp van hun basisstations de locatie van een specifiek apparaat verwerken, verwerken eigenaars van databanken van in kaart gebrachte WiFi-toegangspunten persoonsgegevens wanneer ze de locatie van een specifiek slim mobiel apparaat berekenen. Aangezien ze beide zelf het doel van en de middelen voor deze verwerking vaststellen, zijn ze voor de gegevensverwerking verantwoordelijken als gedefinieerd in artikel 2, lid d, van de gegevensbeschermingsrichtlijn.

Onderstreept moet worden dat het specifieke apparaat, door de eigen locatiegegevens (vaak een combinatie van gps-, WiFi- en basisstationgegevens) en de unieke ID's van nabijgelegen WiFi-toegangspunten door te geven aan de eigenaar van de databank, helpt bij de berekening van zijn eigen locatie¹¹. Een dergelijk apparaat vervult ook de criteria van artikel 4, lid 1, onder c), van de gegevensbeschermingsrichtlijn voor *middelen die zich op het grondgebied van een lidstaat bevinden*.

Aangezien het MAC-adres van een WiFi-toegangspunt, in combinatie met de berekende locatie ervan, moet worden behandeld als een persoonsgegeven, resulteert het verzamelen van deze gegevens ook in de verwerking van persoonsgegevens. Ongeacht de wijze waarop deze gegevens worden verzameld (eenmalig of voortdurend), moet de eigenaar van de databank voldoen aan de verplichtingen van de gegevensbeschermingsrichtlijn.

5.1.2 Aanbieders van geolocatieapplicaties en -diensten

Op slimme mobiele apparaten kan software van derden worden geïnstalleerd, zogeheten *applicaties*. Deze applicaties kunnen de locatiegegevens (en andere gegevens) van een slim mobiel apparaat verwerken, onafhankelijk van de ontwikkelaar van het besturingssysteem en/of de verantwoordelijken voor de verwerking van met behulp van geolocatie-infrastructuur verzamelde gegevens.

Voorbeelden van dergelijke diensten zijn een weersvoorspellingsdienst die de kans op regen in de komende uren in een heel specifieke regio voorspelt, een dienst die informatie over nabijgelegen winkels verstrekt, een identificatiedienst voor verloren telefoons of een dienst die laat zien waar vrienden zich bevinden.

De aanbieder van een applicatie die geolocatiegegevens kan verwerken, is de verantwoordelijke voor de verwerking van persoonsgegevens die uit de installatie en het gebruik van de applicatie resulteren.

¹¹ Het mobiele apparaat kan de verschillende geolocatiegegevens die het ontvangt doorsturen, zodat de voor de gegevensverwerking verantwoordelijke de locatie ervan kan berekenen, of het kan zelf de locatie berekenen. In beide gevallen is het apparaat essentiële uitrusting voor de verwerking.

Natuurlijk is het niet altijd nodig om aparte software op een slim mobiel apparaat te installeren. Veel geolocatiediensten zijn ook via een browser toegankelijk. Een voorbeeld van een dergelijke dienst is het gebruik van een onlineplattegrond door iemand die door een stad loopt.

5.1.3 Ontwikkelaar van het besturingssysteem

De ontwikkelaar van het besturingssysteem van het slimme mobiele apparaat kan een verantwoordelijke voor de verwerking van geolocatiegegevens zijn wanneer er een rechtstreekse interactie met de gebruiker plaatsvindt en hij persoonsgegevens verzamelt (bijvoorbeeld door de gebruiker te vragen om zich te registreren en/of door locatiegegevens te verzamelen om de dienstverlening te verbeteren). Als voor de gegevensverwerking verantwoordelijke moet de ontwikkelaar de beginselen van 'privacy by design' toepassen om heimelijke monitoring te voorkomen, door het apparaat zelf of door de verschillende applicaties en diensten.

Een ontwikkelaar is ook de voor de gegevensverwerking verantwoordelijke als het apparaat een 'phone home'-functie voor de plaatsbepaling van het apparaat heeft. Omdat de ontwikkelaar in dat geval besluit over het doel van en de middelen voor deze gegevensstroom, is hij de voor de verwerking van deze gegevens verantwoordelijke. Een gebruikelijk voorbeeld van een dergelijke 'phone home'-functie is de automatische aanpassing van de instellingen voor de tijdzone aan de locatie.

In de derde plaats is de ontwikkelaar de voor de gegevensverwerking verantwoordelijke wanneer hij een advertentieplatform en/of een internetwinkelachtige omgeving voor applicaties aanbiedt en in staat is om, onafhankelijk van de aanbieders van de applicaties, uit (de installatie en het gebruik van) geolocatieapplicaties resulterende persoonsgegevens te verwerken.

5.2 Verantwoordelijkheden van andere partijen

Er zijn veel andere onlinepartijen die de (verdere) verwerking van locatiegegevens mogelijk maken, zoals browsers, sociale netwerken en communicatiemediën die bijvoorbeeld 'geocoding' mogelijk maken. Wanneer deze partijen geolocatiefaciliteiten in hun platform inbouwen, hebben ze de belangrijke verantwoordelijkheid om een besluit te nemen over de standaardinstellingen van de applicatie (standaard 'aan' of standaard 'uit'). Hoewel ze alleen voor de gegevensverwerking verantwoordelijken zijn voor zover ze zelf actief persoonsgegevens verwerken, hebben ze een belangrijke taak met betrekking tot de rechtmatigheid van de verwerking van gegevens door voor de gegevensverwerking verantwoordelijken, zoals de aanbieders van specifieke applicaties, bijvoorbeeld in verband met de zichtbaarheid en de kwaliteit van de informatie over de verwerking van geolocatiegegevens.

5.3 Legitieme grond

5.3.1 Slimme mobiele apparaten

Als telecombedrijven basisstationgegevens willen gebruiken om een dienst met toegevoegde waarde aan een klant te verstrekken, moeten ze volgens de gewijzigde e-privacyrichtlijn de voorafgaande toestemming van deze klant verkrijgen. Ook moeten ze ervoor zorgen dat de klant in kennis wordt gesteld van de voorwaarden van deze verwerking.

Gezien de gevoeligheid van de verwerking van (patronen van) locatiegegevens, is *voorafgaande geïnformeerde toestemming* ook de belangrijkste toepasselijke grond voor de rechtmatigheid van gegevensverwerking als het gaat om de verwerking van de locaties van een slim mobiel apparaat in de context van diensten van de informatiemaatschappij.

Volgens artikel 2, onder h), van de gegevensbeschermingsrichtlijn moet de toestemming een vrije, specifieke en op informatie berustende wilsuiting van de betrokkene zijn.

Afhankelijk van het soort technologie dat wordt gebruikt, speelt het apparaat van de gebruiker een relatief actieve rol in de verwerking van geografischeplaatsbepalingsgegevens. Het apparaat kan locatiegegevens uit verschillende bronnen naar derden doorsturen. Deze technische capaciteit mag niet worden verward met de wettigheid van de gegevensverwerking. Als de standaardinstellingen van een besturingssysteem het versturen van locatiegegevens mogelijk maken, mag het ongewijzigd laten van deze instellingen door de gebruikers niet worden opgevat als uit vrije wil gegeven toestemming.

Voor zover ontwikkelaars van besturingssystemen en andere diensten van de informatiemaatschappij zelf actief geolocatiegegevens verwerken (bijvoorbeeld wanneer ze via of door middel van het apparaat toegang tot locatiegegevens verkrijgen), moeten ze eveneens voorafgaande geïnformeerde toestemming van hun gebruikers verkrijgen. Het moet duidelijk zijn dat deze toestemming niet op basis van een vrije wilsuiting kan worden verkregen door verplichte instemming met de algemene voorwaarden, en evenmin door de mogelijkheid van een 'opt-out' te bieden. De standaardinstelling moet zijn dat de locatiediensten 'uit' staan en dat gebruikers granulair toestemming moeten geven voor het 'aan'-zetten van specifieke applicaties.

Toestemming van werknemers

Toestemming als legitieme grond voor verwerking is problematisch in de beroepssfeer. In zijn advies over de verwerking van persoonsgegevens in het kader van de arbeidsverhouding schreef de Groep: *“Wanneer toestemming van een werknemer is vereist en uit het niet verlenen van toestemming een reëel of potentieel relevant nadeel voortvloeit, is de toestemming niet geldig in de zin dat wordt voldaan aan het bepaalde in artikel 7 of artikel 8 als deze toestemming niet uit vrije wil is verleend. Als de werknemer niet kan weigeren om toestemming te verlenen, is er geen sprake van toestemming. (...) Een problematisch gebied is dat waar het verlenen van toestemming een voorwaarde is om in dienst te worden genomen. De werknemer kan in theorie toestemming weigeren, maar de consequentie daarvan kan zijn dat de kans op een dienstverband verloren gaat. In dergelijke omstandigheden wordt niet uit vrije wil toestemming verleend en is de toestemming derhalve niet geldig.”*¹² In plaats van om toestemming te vragen, moeten werkgevers onderzoeken of het aantoonbaar noodzakelijk is om voor gerechtvaardigde doeleinden toezicht te houden op de exacte locaties van werknemers en die noodzaak afwegen tegen de fundamentele rechten en vrijheden van de werknemers. Wanneer de noodzaak voldoende kan worden gerechtvaardigd, kan de rechtsgrondslag van de verwerking worden gebaseerd op het legitieme belang van de voor de gegevensverwerking verantwoordelijke (artikel 7, onder f), van de gegevensbeschermingsrichtlijn). De werkgever moet altijd naar de minst ingrijpende middelen zoeken, voortdurende controle vermijden en bijvoorbeeld voor een systeem kiezen dat een waarschuwing uitzendt wanneer een werknemer een vooraf bepaalde virtuele grens overschrijdt. Een werknemer moet controleapparaten buiten werktijden kunnen uitschakelen en moet worden gedemonstreerd hoe hij of zij dit kan doen. Voertuigtracering is geen personeelstracering. De functie van apparaten voor het traceren van voertuigen is het traceren of controleren van de locatie van de voertuigen die door personeelsleden worden gebruikt. Werkgevers zouden ze niet moeten beschouwen als apparaten om het gedrag of de locatie van de bestuurders of andere personeelsleden te traceren of te controleren, bijvoorbeeld door waarschuwingen met betrekking tot de snelheid van het voertuig uit te zenden.

Toestemming van kinderen

In bepaalde gevallen moeten de ouders of andere wettelijke vertegenwoordigers toestemming voor een kind verlenen. Dat betekent bijvoorbeeld dat aanbieders van een geolocatieapplicatie de ouders in kennis moeten stellen van het feit dat ze geolocatiegegevens van het kind verzamelen en gebruiken en hun toestemming moeten verkrijgen voor het verzamelen en verder gebruiken van de informatie over het kind. Bepaalde geolocatieapplicaties zijn speciaal voor het uitoefenen van ouderlijk toezicht ontwikkeld, zoals applicaties waarbij de locatie van het apparaat voortdurend wordt weergegeven op een website of een waarschuwing wordt afgegeven wanneer het apparaat een vooraf bepaald gebied verlaat. Het gebruik van dergelijke applicaties is problematisch. In zijn advies 2/2009¹³ over de bescherming van persoonsgegevens van kinderen schreef de Groep: *“Kinderen mogen nooit, om redenen van beveiliging, worden geconfronteerd met overmatig toezicht dat hun*

¹² WP48, Advies 8/2001 over de verwerking van persoonsgegevens in het kader van de arbeidsverhouding.

¹³ WP160, Advies 2/2009 over de bescherming van persoonsgegevens van kinderen (Algemene richtlijnen en het bijzondere geval van scholen).

autonomie zou beperken. In deze context moet een evenwicht worden gevonden tussen de bescherming van de intimiteit en het privéleven van kinderen en hun veiligheid”.

Het wettelijk kader bepaalt dat ouders ervoor verantwoordelijk zijn dat het recht op privacy van kinderen wordt gegarandeerd. Op zijn minst moeten kinderen, wanneer de ouders van oordeel zijn dat het gebruik van een dergelijke applicatie in specifieke omstandigheden gerechtvaardigd is, hiervan zo snel als redelijkerwijs mogelijk is in kennis worden gesteld en moeten ze kunnen deelnemen aan de besluitvorming over het gebruik van een dergelijke applicatie.

De toestemming moet specifiek zijn voor elk van de verschillende doeleinden waarvoor de gegevens worden verwerkt. De voor de gegevensverwerking verantwoordelijke moet heel duidelijk maken of zijn dienst zich beperkt tot het verstrekken van een antwoord op de vrijwillige vraag ‘Waar ben ik op dit moment?’ of dat het zijn doel is om antwoorden te krijgen op de vragen ‘Waar bent u, waar bent u geweest en waar zult u volgende week zijn?’ Met andere woorden, de voor de gegevensverwerking verantwoordelijke moet specifieke aandacht besteden aan de toestemming voor doeleinden die een betrokkene niet verwacht, zoals bijvoorbeeld profilering en/of gedragsgestuurde reclame.

Als de doeleinden van de verwerking wezenlijk veranderen, moet de voor de gegevensverwerking verantwoordelijke hernieuwde specifieke toestemming verkrijgen. Als een bedrijf oorspronkelijk heeft verklaard dat het geen persoonsgegevens met derden zal delen, maar dat nu wel wil doen, moet het actief voorafgaande toestemming van elke klant verkrijgen. Het niet ontvangen van een antwoord (of een ander type scenario) volstaat niet.

Het is belangrijk om onderscheid te maken tussen toestemming voor een eenmalige dienst en toestemming voor een regulier abonnement. Om een specifieke geolocatiedienst te kunnen gebruiken, kan het bijvoorbeeld nodig zijn om geolocatiediensten in het apparaat of de browser in te schakelen. Als die geolocatiecapaciteit ‘aan’ is gezet, kan elke website de locatiedetails van de gebruiker van een slim mobiel apparaat lezen. Om de risico’s van heimelijke monitoring te vermijden, acht de Groep gegevensverwerking artikel 29 het van essentieel belang dat het apparaat voortdurend waarschuwt dat de geolocatiefunctie ‘aan’ staat, bijvoorbeeld door middel van een permanent zichtbaar pictogram.

De Groep beveelt aan dat aanbieders van geolocatieapplicaties of -diensten de individuele toestemming na een passende periode moeten hernieuwen, ook als de aard van de verwerking niet verandert. Het zou bijvoorbeeld niet in orde zijn om locatiegegevens te blijven verwerken wanneer iemand de dienst in de afgelopen twaalf maanden niet heeft gebruikt. Ook wanneer iemand de dienst wel heeft gebruikt, moet die persoon ten minste eenmaal per jaar (of vaker wanneer de aard van de verwerking dit rechtvaardigt) worden herinnerd aan de aard van de verwerking van zijn of haar persoonsgegevens en een middel worden aangeboden om zijn of haar toestemming op gemakkelijke wijze in te trekken.

Niet in de laatste plaats moet het voor de betrokkenen heel gemakkelijk zijn om hun toestemming in te trekken, zonder enig negatief gevolg voor het gebruik van het apparaat. Onafhankelijk van de Europese gegevensbeschermingsrichtlijnen heeft het

World Wide Web Consortium (W3C) een ontwerpnorm voor applicatieprogrammeerinterfaces ("application programming interface" – API) voor geolocatieapplicaties opgesteld, waarin de noodzaak van voorafgaande, uitdrukkelijke en geïnformeerde toestemming wordt benadrukt¹⁴. Het W3C stelt specifiek dat intrekkingen van toestemming dienen te worden gerespecteerd en adviseert gebruikers van de norm om in aanmerking te nemen dat *“de inhoud die door een bepaalde URL wordt aangeboden zodanig kan veranderen dat de eerder verleende locatietoestemmingen wat de gebruikers betreft niet langer van toepassing zijn. Of de gebruikers kunnen gewoonweg van mening veranderen.”*

Voorbeeld van een goede praktijk voor aanbieders van geolocatiediensten

Een applicatie die geolocatiegegevens wil gebruiken, informeert de gebruiker duidelijk over de doeleinden waarvoor de gegevens zullen worden gebruikt en vraagt ondubbelzinnig om toestemming voor elk van de mogelijk verschillende doeleinden. De gebruiker kiest actief het granulariteitsniveau van de geolocatie (bijvoorbeeld het niveau van een land, het niveau van een stad, het niveau van een postcode, of zo precies mogelijk). Zodra de locatiedienst is geactiveerd, is op elk scherm permanent een pictogram te zien dat aangeeft dat de locatiediensten ‘aan’ staan. De gebruiker kan zijn of haar toestemming voortdurend intrekken, zonder dat hij of zij hoeft te stoppen met het gebruik van de applicatie. De gebruiker kan ook gemakkelijk en permanent een deel van of alle in het apparaat opgeslagen locatiegegevens wissen.

5.3.2 WiFi-toegangspunten

Op basis van de gegevensbeschermingsrichtlijn kunnen bedrijven een gerechtvaardigd belang hebben bij de voor het specifieke doel om geolocatiediensten aan te bieden noodzakelijke verzameling en verwerking van MAC-adressen en berekende locaties van WiFi-toegangspunten.

De legitieme grond van artikel 7, onder f), van de gegevensbeschermingsrichtlijn vereist evenwicht tussen de gerechtvaardigde belangen van de voor de gegevensverwerking verantwoordelijke en de fundamentele rechten van de betrokkenen. Gegeven de semistatische aard van WiFi-toegangspunten, vormt het in kaart brengen van WiFi-toegangspunten in beginsel een minder grote bedreiging voor de privacy van de eigenaars van deze toegangspunten dan de reallimetraçering van de locaties van slimme mobiele apparaten.

Het evenwicht tussen de rechten van de voor de gegevensverwerking verantwoordelijke en de rechten van de betrokkene is dynamisch. Om hun gerechtvaardigde belangen met succes te laten prevaleren boven de belangen van de betrokkenen, moeten voor de gegevensverwerking verantwoordelijken garanties ontwikkelen en toepassen, zoals het recht om zich gemakkelijk en permanent uit de databank terug te trekken zonder de voor de gegevensverwerking verantwoordelijke van de databank daarvoor aanvullende persoonsgegevens te hoeven verstrekken. Ze kunnen bijvoorbeeld software gebruiken om automatisch te detecteren dat iemand met een specifiek toegangspunt is verbonden¹⁵.

¹⁴ W3C, Geolocation API Specification: <http://www.w3.org/TR/geolocation-API/>

¹⁵ Een mogelijke use case ziet er als volgt uit:

Om geolocatediensten aan te bieden is het niet nodig om SSID's te verzamelen en te verwerken. De verzameling en verwerking van SSID's is buitensporig voor het doel van het aanbieden van geolocatediensten op basis van het in kaart brengen van de locaties van WiFi-toegangspunten.

5.4 Informatie

De verschillende voor de gegevensverwerking verantwoordelijken moeten ervoor zorgen dat de eigenaars van slimme mobiele apparaten naar behoren worden geïnformeerd over de belangrijkste elementen van de verwerking, in overeenstemming met artikel 10 van de gegevensbeschermingsrichtlijn, zoals de identiteit van de voor de gegevensverwerking verantwoordelijke, de doeleinden van de verwerking, het soort gegevens dat wordt verwerkt, de duur van de verwerking, het recht van betrokkenen om toegang tot hun eigen persoonsgegevens te krijgen en om deze te rectificeren of te annuleren, en het recht om de verleende toestemming in te trekken.

De geldigheid van de toestemming is onlosmakelijk verbonden met de kwaliteit van de informatie over de aangeboden dienst. De informatie moet duidelijk, volledig, voor een breed, niet-technisch geschoold publiek begrijpelijk en permanent en gemakkelijk toegankelijk zijn.

De informatie moet gericht zijn op een breed publiek. Voor de gegevensverwerking verantwoordelijken mogen niet uitgaan van de veronderstelling dat hun klanten technisch onderlegd zijn op basis van alleen het feit dat ze in het bezit van een slim mobiel apparaat zijn. De informatie moet zijn aangepast aan de leeftijd als de voor de gegevensverwerking verantwoordelijke weet dat de informatie een jong publiek aantrekt.

Als aanbieders van geolocatieapplicaties van plan zijn de locaties van een apparaat meer dan eens te berekenen, moeten ze hun klanten daarover geïnformeerd houden zolang ze locatiegegevens verwerken. Ook moeten ze hun klanten in staat stellen hun toestemming te verlengen of in te trekken. Om deze doelen te bereiken moet de aanbieder van applicaties nauw samenwerken met de ontwikkelaar van het besturingssysteem. De ontwikkelaar bevindt zich technisch in de beste positie om een permanent zichtbaar pictogram te creëren dat eraan herinnert dat locatiegegevens worden verwerkt. De ontwikkelaar bevindt zich ook in de beste positie om te

-
1. een betrokkene logt in op bepaalde webpagina, waar het MAC-adres van zijn of haar WiFi-toegangspunt kan worden ingevoerd;
 2. als het MAC-adres in de databank met de in kaart gebrachte WiFi-toegangspunten verschijnt, kan de voor de gegevensverwerking verantwoordelijke de betrokkene doorsturen naar een verificatiepagina die een script bevat waarmee de ARP-tabel wordt opgevraagd. De WLAN MAC-adressen zijn theoretisch gezien op te vragen door middel van het commando 'ARP -a'. Met behulp van een browsercode, bijvoorbeeld java, kan deze ARP-tabel worden opgevraagd op de achtergrond;
 3. als het opgegeven MAC-adres in de ARP-tabel staat, is vastgesteld dat de gebruiker, die verbonden is met het WLAN, degene is die toegang heeft tot het lokale WLAN MAC-adres. De voor de gegevensverwerking verantwoordelijke verifieert aldus het verzoek om verwijdering, op een gemakkelijke en automatische wijze.

controleren dat er geen applicaties worden aangeboden die heimelijk de locatie van slimme mobiele apparaten monitoren.

Als de ontwikkelaar van het besturingssysteem een phone home-functionaliteit heeft gecreëerd, of andere middelen om toegang tot op het apparaat opgeslagen gegevens te krijgen, of zichzelf op andere manieren toegang tot op het apparaat opgeslagen gegevens verschaft, bijvoorbeeld via derde adverteerders, moet hij de betrokkene van tevoren in kennis stellen van de (specifieke en gerechtvaardigde) doeleinden waarvoor hij deze gegevens wil verwerken en de duur van de verwerking.

De verplichting om de betrokkenen te informeren is ook van toepassing op de voor de gegevensverwerking verantwoordelijken van databanken met geogelocaliseerde WiFi-toegangspunten. Ze moeten het algemene publiek op adequate wijze in kennis stellen van hun identiteit en de doeleinden van de verwerking en ook andere relevante informatie verstrekken. Het louter vermelden van de mogelijkheid dat er gegevens over WiFi-toegangspunten zullen worden verzameld in een op de gebruikers van een geolocatiedienst gerichte specifieke privacyverklaring is niet genoeg. Er zijn voldoende manieren, online en offline, om het algemene publiek te informeren.

5.5 Rechten van betrokkenen

Betrokkenen hebben het recht om van de verschillende voor de gegevensverwerking verantwoordelijken toegang te verkrijgen tot de locatiegegevens die deze hebben verzameld van hun slimme mobiele apparaten, evenals informatie over de doeleinden van de verwerking en over de ontvangers of categorieën ontvangers aan wie de gegevens bekend zijn gemaakt. De informatie moet in een voor de mens leesbare tekst worden verstrekt, dat wil zeggen in de vorm van geografische locaties en niet in de vorm van abstracte cijfers voor bijvoorbeeld basisstations.

Betrokkenen hebben ook recht op toegang tot de profielen die mogelijk op basis van deze locatiegegevens zijn opgesteld. Als locatie-informatie wordt opgeslagen, moeten gebruikers deze informatie kunnen actualiseren, rectificeren of verwijderen.

De Groep beveelt aan dat voor de gegevensverwerking verantwoordelijken naar veilige manieren zoeken om directe onlinetoegang tot locatiegegevens en mogelijke profielen te bieden. Het is essentieel dat deze toegang wordt geboden zonder dat er om aanvullende persoonsgegevens wordt gevraagd om de identiteit van de betrokkenen vast te stellen.

5.6 Bewaartermijnen

Aanbieders van geolocatie- en applicatiediensten moeten een termijn voor het bewaren van locatiegegevens vaststellen die niet langer mag zijn dan noodzakelijk is voor de doeleinden waarvoor de gegevens zijn verzameld of verder worden verwerkt. Ze moeten ervoor zorgen dat geolocatiegegevens, of van deze gegevens afgeleide profielen, na een gerechtvaardigde periode worden gewist.

Wanneer het voor de ontwikkelaar van het besturingssysteem en/of de voor de gegevensverwerking verantwoordelijke van een geolocatie-infrastructuur aantoonbaar noodzakelijk is om anonieme gegevens over de locatiegeschiedenis te verzamelen om zijn dienst te updaten of te verbeteren, moet hij de grootst mogelijke zorgvuldigheid betrachten om te voorkomen dat deze gegevens (indirect) identificeerbaar worden. In het bijzonder geldt dat ook als het mobiele apparaat is geïdentificeerd aan de hand van een willekeurig toegekende UDID (Unique Device Identifier), een dergelijk uniek nummer niet langer dan 24 uur mag worden opgeslagen voor operationele doeleinden. Na die periode moet deze UDID verder anoniem worden gemaakt, rekening houdend met het feit dat werkelijke anonimiteit steeds moeilijker te realiseren is en dat de gecombineerde locatiegegevens nog steeds tot identificatie kunnen leiden. De UDID mag noch aan eerdere of toekomstige aan het apparaat toegekende UDID's kunnen worden gekoppeld, noch met enig vast identificatienummer van de gebruiker van de telefoon (zoals het MAC-adres, het IMEI- of IMSI-nummer of andere accountnummers).

Met betrekking tot gegevens over WiFi-toegangspunten geldt het volgende: zodra het MAC-adres van een WiFi-toegangspunt is gekoppeld aan een nieuwe locatie, op basis van continue waarnemingen van eigenaars van slimme mobiele apparaten, moet de eerdere locatie onmiddellijk worden gewist om verder gebruik van de gegevens voor ongepaste doeleinden, zoals marketing gericht op personen die van locatie zijn veranderd, te voorkomen.

6. Conclusies

Met behulp van geolocatietechnologieën als basisstationgegevens, gps en in kaart gebrachte WiFi-toegangspunten kunnen slimme mobiele apparaten door allerlei verschillende voor de gegevensverwerking verantwoordelijken worden getraceerd, voor doeleinden die variëren van gedragsgestuurde reclame tot het elektronisch volgen van kinderen.

Aangezien smartphones en tabletcomputers onlosmakelijk zijn verbonden met hun eigenaars, bieden de bewegingspatronen van deze apparaten een gedetailleerd inzicht in het privéleven van de eigenaars. Een van de grote risico's is dat de eigenaars zich niet van bewust zijn van het feit dat ze hun locatie doorzenden, en aan wie. Een ander, daaraan gerelateerd risico is dat de toestemming aan bepaalde applicaties om locatiegegevens te gebruiken ongeldig is, omdat de informatie over essentiële elementen van de verwerking onbegrijpelijk, achterhaald of anderszins ontoereikend is.

De verschillende belanghebbende partijen, van de ontwikkelaars van het besturingssysteem tot de aanbieders van applicaties en partijen als sociale netwerken op internet die locatiefunctionaliteiten voor mobiele apparaten in hun platforms inbouwen, hebben diverse verplichtingen.

6.1 Wettelijk kader

- Het wettelijk kader van de EU voor het gebruik van geolocatiegegevens van slimme mobiele apparaten wordt primair gevormd door de gegevensbeschermingsrichtlijn. Locatiegegevens van slimme mobiele apparaten zijn persoonsgegevens. De combinatie van het unieke MAC-adres

en de berekende locatie van een WiFi-toegangspunt moet worden behandeld als een persoonsgegeven.

- Daarnaast is de gewijzigde e-privacyrichtlijn 2002/58/EG alleen van toepassing op de verwerking van basisstationgegevens door telecombedrijven.

6.2 Voor de gegevensverwerking verantwoordelijken

- Er kunnen drie typen voor de gegevensverwerking verantwoordelijken worden onderscheiden, te weten: verantwoordelijken voor de verwerking van met behulp van geolocatie-infrastructuur verzamelde gegevens (in het bijzonder in kaart gebrachte WiFi-toegangspunten), aanbieders van geolocatieapplicaties en -diensten, en ontwikkelaars van de besturingssystemen van slimme mobiele apparaten.

6.3 Legitieme grond

- Omdat locatiegegevens van slimme mobiele apparaten details over het privéleven van hun eigenaars prijsgeven, is de belangrijkste van toepassing zijnde legitieme grond voorafgaande geïnformeerde toestemming.
- Toestemming kan niet worden verkregen door middel van de algemene voorwaarden.
- De toestemming moet specifiek zijn voor de verschillende doeleinden waarvoor de gegevens worden verwerkt, zoals bijvoorbeeld profilering en/of gedragsgestuurde reclame door de voor de gegevensverwerking verantwoordelijke. Als de doeleinden van de verwerking wezenlijk veranderen, moet de voor de gegevensverwerking verantwoordelijke nieuwe specifieke toestemming verkrijgen.
- Locatiediensten moeten standaard 'uit' staan. Een mogelijk opt-outmechanisme is geen adequaat mechanisme om geïnformeerde toestemming van de gebruiker te verkrijgen.
- De toestemming is problematisch met betrekking tot werknemers en kinderen. Wat betreft werknemers mogen werkgevers deze technologie alleen toepassen als dit aantoonbaar noodzakelijk is voor een gerechtvaardigd doel en dit doel niet kan worden verwezenlijkt met minder ingrijpende middelen. Wat betreft kinderen, moet het aan ouders zijn om te oordelen of het gebruik van een applicatie in specifieke omstandigheden is gerechtvaardigd. Op zijn minst moeten zij hun kinderen informeren en hen zo snel als redelijkerwijs mogelijk is laten deelnemen aan de besluitvorming over het gebruik van een de applicatie.
- De Groep beveelt aan om de tijd dat de toestemming geldig blijft te beperken en de verplichting in te stellen om gebruikers er ten minste eenmaal per jaar aan te herinneren dat er locatiegegevens worden verzameld. Ook beveelt de Groep aan om voor voldoende granulariteit in de toestemming ten aanzien van de precisie van de locatiegegevens te zorgen.
- Betrokkenen moeten hun toestemming gemakkelijk en zonder negatieve gevolgen voor het gebruik van het apparaat kunnen intrekken.
- Met betrekking tot het in kaart brengen van WiFi-toegangspunten kunnen bedrijven een gerechtvaardigd belang hebben bij de voor het specifieke doel om geolocatiediensten aan te bieden noodzakelijke verzameling en verwerking van MAC-adressen en berekende locaties van WiFi-toegangspunten. Het vinden van een goed evenwicht tussen de rechten van de voor de

gegevensverwerking verantwoordelijke en de rechten van de betrokkenen vereist dat de voor de gegevensverwerking verantwoordelijke de betrokkenen het recht biedt, zonder om aanvullende persoonsgegevens te vragen, om zich gemakkelijk en permanent uit de databank terug te trekken.

6.4 Informatie

- Informatie moet duidelijk, volledig, voor een breed, niet-technisch geschoold publiek begrijpelijk, en permanent en gemakkelijk toegankelijk zijn. De geldigheid van de toestemming is onlosmakelijk verbonden met de kwaliteit van de informatie over de aangeboden dienst.
- Derden als browsers en sociale netwerken op internet hebben een belangrijke taak met betrekking tot de zichtbaarheid en de kwaliteit van de informatie over de verwerking van geolocatiegegevens.

6.5 Rechten van betrokkenen

- De verschillende verantwoordelijken voor de verwerking van van mobiele apparaten verkregen geolocatiegegevens moeten hun klanten toegang bieden tot hun locatiegegevens, in een voor de mens leesbare vorm, en hun klanten in staat stellen, zonder buitensporig veel persoonsgegevens te verzamelen, om deze locatiegegevens te rectificeren of te verwijderen.
- Betrokkenen hebben ook het recht om de profielen die mogelijk op basis van deze locatiegegevens zijn opgesteld in te zien, te rectificeren en te wissen.
- De Groep beveelt aan om (veilige) onlinetoegang te ontwikkelen.
-

6.6 Bewaartermijnen

- Aanbieders van geolocatieapplicaties of -diensten moeten een bewaarbeleid volgen dat ervoor zorgt dat geolocatiegegevens, of daarvan afgeleide profielen, na een gerechtvaardigde termijn worden gewist.
- Wanneer de ontwikkelaar van het besturingssysteem en/of de voor de gegevensverwerking verantwoordelijke van de geolocatie-infrastructuur een uniek nummer als een MAC-adres of een UDID verwerkt in relatie met locatiegegevens, mag een dergelijk uniek nummer niet langer dan 24 uur worden opgeslagen, voor operationele doeleinden.

Gedaan te Brussel
16 mei 2011

*namens de Groep,
Jacob KOHNSTAMM,
Voorzitter*