ARTICLE 29 Data Protection Working Party

881/11/EN
WP 185

Opinion 13/2011 on Geolocation services on smart mobile devices

Adopted on 16 May 2011

CONTENTS

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA
set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT DOCUMENT:

1. Introduction

Geographical information plays an important role in our society. Almost all human activities and decisions have a geographical component. In general, the value of information increases when it is connected to a location. All kinds of information can be connected to a geographic location, such as financial data, health data and other consumer behavioural data. With the rapid technological development and wide uptake of smart mobile devices, a whole new category of location based services is developing.

The objective of this opinion is to clarify the legal framework applicable to geolocation services that are available on and/or generated by smart mobile devices that can connect with the Internet and are equipped with location sensitive sensors such as GPS. Examples of such services are: maps and navigation, geo-personalised services (including nearby points of interests), augmented reality, geotagging of content on the Internet, tracking the whereabouts of friends, child control and location based advertising.

This opinion also deals with the main three types of infrastructure used to provide geolocation services, namely GPS, GSM base stations and WiFi. Special attention is paid to the new infrastructure based on the location of WiFi access points.

The Working Party is well aware there are many other services that process location data that may also raise data protection concerns. This varies from e-ticketing systems to toll systems for cars and from satellite navigation services, from location tracking with the help of for example cameras and the geolocation of IP addresses. However, given the rapid technological developments with regard to especially the mapping of wireless access points, in combination with the fact that new market entrants are preparing to develop new location based services based on a combination of base station, GPS and WiFi data, the Working Party has decided to specifically clarify the legal requirements for these services under the data protection directive.

The opinion first describes the technology, subsequently identifies and assesses the privacy risks, and then provides conclusions about the

application of the relevant legal articles to various controllers that collect and process location data derived from mobile devices. This includes for example providers of geolocation infrastructure, smartphone manufacturers and the developers of geolocation based applications.

This opinion will not assess specific geotagging technology linked to the so-called web 2.0 in which users integrate geo-referenced information on social networks such as Facebook or Twitter. This opinion will also not go into detail about some other geolocation technologies that are used to interconnect devices within a relatively small area (shopping centres, airports, office buildings, etc) such as Bluetooth, ZigBee, geofencing and WiFi based RFID tags, though many of the conclusions of this opinion with regard to legitimate ground, information and data subjects rights also apply to these technologies when they are used to geolocate people through their devices.

2. Context: different geolocation infrastructures

2.1 Base station data

The area covered by the different telecommunication operators is divided in areas that are generally known as cells. In order to be able to use a mobile phone or to connect to Internet using 3G communication, the mobile device has to connect to the antenna (hereafter: base station) that covers that cell. The cells cover areas of different sizes, depending on interference with for example mountains and high buildings.

All the time a mobile device is switched on, the device is linked to a specific base station. The telecom operator continuously registers these links. Every base station has a unique ID, and is registered with a specific location. Both the telecom operator and many mobile devices themselves are able to use signals from overlapping cells (neighbouring base stations) to estimate the position of the mobile device with increased accuracy. This technique is also called triangulation.

The accuracy can be further increased with the help of information such as RSSI (Received Signal Strength Indicator), TDOA (Time Difference of Arrival) and AOA (Angle Of Arrival).

Base station data can be used in innovative ways, for example to detect traffic jams. Each road has an average speed for each segment of the day, but when hand-overs to the next base station take longer than expected, there apparently is a traffic jam.

In sum, this positioning method provides a quick, rough indication of location, but not very accurate compared to GPS and WiFi data. The accuracy is approximately 50 meters in densely populated city areas, but up to several kilometers in rural areas.

2.2 GPS technology

Smart mobile devices have on board chipsets with GPS-receivers that determine their location.

GPS technology (Global Positioning System) uses 31 satellites that each rotate in one of the 6 different orbits around the earth.[1] Each satellite transmits a very precise radio signal.

The mobile device can determine its location when the GPS-sensor captures at least 4 of those signals. Different from base station data, the signal only goes one way. The entities managing the satellites can not keep track of devices that have received the radio signal.

GPS technology provides accurate positioning, between 4 and 15 meters. The major disadvantage of GPS is that it has a relatively slow start.[2] Another disadvantage is that it does not work or does not work well indoors. In practice, GPS technology is therefore often combined with base station data and/or mapped Wifi access points.

2.3 WiFi

2.3.1 WiFi access points

A relatively new source of geolocation information is the use of WiFi access points. The technology is similar to the use of base stations. They both rely on a unique ID (from the base station or the WiFi access point) that can be detected by a mobile device, and sent to a service that has a location for each unique ID.

The unique ID for each WiFi access point is its MAC address (Medium Access Control). A MAC address is a unique identifier attributed to a network interface and usually recorded in hardware such as memory chips and/or network cards in computers, telephones, laptops or access points.[3]

The reason that WiFi access points can be used as a source of geolocation information is because they continuously announce their existence. Most broadband internet access points by default also have a WiFi antenna. The default setting of the most commonly used access points in Europe is that

[1] The Global Positioning System consists of satellites launched by the United States of America, for military purposes. By 2014, the European Commission intends to launch Galileo, a network of 18 satellites offering free, non-military global satellite positioning. The first 2 satellites are to be launched in 2011, another 2 in 2012. Source: European Commission, 'Commission presents midterm review of Galileo and EGNOS', 25 January 2011, URL: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&item_id=4835

[2] In order to speed up the initial detection of the GPS signal, it is possible to preload so called rainbow tables, with the expected positioning of the different satellites in the next weeks.

[3] An example of a MAC address is: 00-1F-3F-D7-3C-58. The MAC address of a WiFi access point is called BSSID (Basic Service Set Identifier).

this connection is 'on', also in case the user has connected his computer(s) only with wired cables to the access point. Comparable to a radio, the WiFi access point continuously transmits its own network name and its MAC address, even if nobody is using the connection and even in case the contents of the wireless communication are encrypted with WEP, WPA or WPA2.

There are two different ways to collect the MAC addresses of WiFi access points.[4]

1. Active scanning: sending active requests[5] to all nearby WiFi access points and recording the answers. These answers do not include information about devices connnected to the WiFi access point.

2. Passive scanning: recording the periodic beacon frames transmitted by every access point (usually 10 times per second). As a non standard alternative, some tools more broadly record all WiFi frames transmitted by access points, including those that do not broadcast beacon signals. If this type of scanning is done without proper application of privacy by design, it can lead to the collection of data exchanged between access points and the devices connected to them. This way, the MAC addresses of desktop computers, laptops and printers could be recorded. This type of scanning could also lead to the unlawful recording of the contents of communications. These contents are easily readable in case the owner of the WiFi access point has not enabled WiFi encryption (WEP/WPA/WPA2).

The location of a WiFi access point can be calculated in two different ways.

1. Statically/once: controllers themselves collect the MAC addresses of WiFi access points by driving around with vehicles, equipped with antennae. They register the exact latitude longitude of the vehicle the moment the signal is captured and are able to calculate the location of the access points based on, amongst other, signal strength.

2. Dynamically/ongoing: users of geolocation services automatically collect the MAC addresses perceived by their WiFi capable devices when they use for example an online map to determine their own position (Where am I?). The mobile device then sends all available information to the geolocation service provider, including MAC addresses, SSIDs and signal strength. The controller can use these ongoing observations to calculate and/or improve on the locations of the WiFi access points in its database with mapped WiFi access points.

[4] Active and passive scanning have been standardized in IEEE 802.11 to detect access points.
[5] In order to collect the MAC-addresses, the collector sends a 'probe request' to all access points.

It is important to note that mobile devices do not need to 'connect' to WiFi access points to collect WiFi information. They automatically detect the presence of the access points (in active or passive scanning mode) and automatically collect data about them.

Additionally, mobile phones requesting to be geolocated will not only send WiFi data, but often also any other location information they hold, including GPS and base station data. This allows the provider to calculate the location of 'new' WiFi access points and/or improve on the locations of WiFi access points that were already included in the database. This way, the collection of information about WiFi access points is decentralised in a very efficient way, without customers necessarily being aware of it.

In sum: geolocation based on WiFi access points provides a quick and, based on continuous measurements, increasingly accurate position.

3. Privacy risks

A smart mobile device is very intimately linked to a specific individual. Most people tend to keep their mobile devices very close to themselves, from their pocket or bag to the night table next to their bed.

It seldom happens that a person lends such a device to another person. Most people are aware that their mobile device contains a range of highly intimate information, ranging from e-mail to private pictures, from browsing history to for example a contact list.

This allows the providers of geolocation based services to gain an intimate overview of habits and patterns of the owner of such a device and build extensive profiles. From a pattern of inactivity at night, the sleeping place can be deduced, and from a regular travel pattern in the morning, the location of an employer may be deduced. The pattern may also include data derived from the movement patterns of friends, based on the so-called *social graph*.[6]

A behavioural pattern may also include *special categories of data*, if it for example reveal visits to hospitals and religious places, presence at political demonstrations or presence at other specific locations revealing data about for example sex life. These profiles can be used to take decisions that significantly affect the owner.

The technology of smart mobile devices allows for the constant monitoring of location data. Smartphones can permanently collect signals from base stations and wifi access points. Technically, the monitoring can be done secretively, without informing the owner. Monitoring can also be done semi-secretively, when people 'forget' or are not properly informed that location services are switched 'on', or when the accessibility settings of location data are changed from 'private' to 'public'.

[6] The 'social graph' is a term indicating the visibility of friends in social networking sites and the capacity to deduce behavioural traits from data about these friends.

Even when people intentionally make their geolocation data available on the Internet, through whereabout and geotagging services, the unlimited global access creates new risks ranging from data theft to burglary, to even physical aggression and stalking.

As with other new technology, a major risk with the use of location data is function creep, the fact that based on the availability of a new type of data, new purposes are being developed that were not anticipated at the time of the original collection of the data.

4. Legal Framework

The relevant legal framework is the data protection directive (95/46/EC). It applies in every case where personal data are being processed as a result of the processing of location data. The e-privacy directive (2002/58/EC, as revised by 2009/136/EC) only applies to the processing of base station data by public electronic communication services and networks (telecom operators).

4.1 Base station data processed by telecom operators

Telecom operators continuously process base station data in the framework of the provisioning of public electronic communication services.[7] They can also process base station data in order to provide value-added services. This case has already been addressed by the Working party in opinion 5/2005 (WP115). Though some of the examples in the opinion have inevitably been outdated by the spread of internet technology and sensors into ever smaller devices, the legal conclusions and recommendations from this opinion remain valid with regard to the use of base station data.

1. Since location data derived from base stations relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in Directive 95/46/EC of 24 October 1995.
2. Directive 2002/58/EC of 12 July 2002 (as revised in November 2009 in Directive 2009/136/EC) is also applicable, following the definition provided in article 2(c) of this directive:
   "location data" means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

If a telecom operator offers a hybrid geolocation service, that is also based on the processing of other types of location data such as GPS or WiFi data, that activity qualifies as a public electronic communication service. The telecom operator must ensure the prior consent of its customers if it provides these geolocation data to a third party.

[7] Note that the provision of public WiFi hotspots by telecom providers also qualifies as a public electronic communication service and should therefore primarily comply with the provisions of the e-privacy directive.

4.2 Base station, WiFi and GPS data processed by information society service providers

4.2.1 Applicability of the revised e-privacy directive

Typically, companies that provide location services and applications based on a combination of base station, GPS and WiFi data are *information society services*. As such they are explicitly excluded from the e-Privacy directive, from the strict definition of electronic communications service (Article 2, under c, of the revised Framework Directive (unaltered).[8]

The e-Privacy directive does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network. A user may choose to transmit GPS data over the Internet, for example when accessing navigational services on the Internet. In that case, the GPS signal is transmitted in the application level of internet communication, independently of the GSM network. The telecommunication service provider acts as mere conduit. It cannot gain access to GPS and/ or WiFi and/or base station data communicated to and from a smart mobile device between a user/subscriber and an information society service without very intrusive means such as *deep packet inspection*.

4.2.2 Applicability of the data protection directive

Where the revised e-privacy directive does not apply, according to Article 1, paragraph 2, directive 95/46/EC applies: "*The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1.*"

Based on the data protection directive personal data are *any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity* - article 2 (a) of the directive.

Recital 26 of the Directive pays particular attention to the term "identifiable" when it reads that "*whereas to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.*"

---

[8] Directive 2002/21/EC of 7 March 2002, Article 2(c): *'electronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks;*

Recital 27 of the Directive outlines the broad scope of the protection: "*whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention;*"

In its opinion 4/2007 on the Concept of Personal Data, the Working Party has provided extensive guidance on the definition of personal data.

Smart mobile devices
Smart mobile devices are inextricably linked to natural persons. There is usually direct and indirect identifyability.

First of all, the telecom operator providing GSM and mobile internet access usually has a register with the name, address and banking details of every customer, in combination with several unique numbers of the device, such as IMEI and IMSI.

Secondly, the purchase of extra software for the device (*applications* or *apps)* usually requires a credit card number and thereby enriches the combination of the unique number(s) and the location data with directly identifying data.

Indirect identifyability can be achieved through the combination of the unique number(s) of the device, in combination with one or more calculated locations.

Every smart mobile device has at least one unique identifier, the MAC address. The device may have other unique identification numbers, added by the developer of the operating system.These identifiers may be transmitted and further processed in the context of geolocation services. It is a fact that the location of a particular device can be calculated in a very precise way, especially when the different geolocation infrastructures are combined. Such a location can point to a house or an employer. Especially with repeated observations, it is possible to identify the owner of the device.

When considering the available means for identifyability, the development has to be taken into account that people tend to disclose more and more personal location data on the Internet, for example by publishing the location of their house or work in combination with other identifying data. Such disclosure can also happen without their knowledge, when they are being geotagged by other people. This development makes it easier to link a location or behavioural pattern to a specific individual.

Moreover, following Opinion 4/2007 on the concept of personal data, it also should be noted that of a unique identifier, in the context described above, allows the tracking of a user of a specific device and, thus, enables the user to be "singled out" even if his/her real name is not known.

WiFi access points
This indirect identiability applies to WiFi access points as well.[9] The MAC address of a WiFi access point, in combination with its calculated location, is inextricably linked to the location of the owner of the access point.

A reasonably equipped controller may calculate an increasingly precise location of a WiFi-access point based on the signal strength and of the ongoing updates of the location through the users of its geolocation service.

With the help of these resources, in many cases a small group of apartments or houses can be identified where the owner of the access point lives. The ease with which it is possible to identify this owner from the MAC address will depend on the environment:

- In sparsly populated areas , where the MAC address points to a single house, the owner of the residence can be determined directly with tools such as for example house ownership registries, white page directories, electoral registrations or even a simple search engine query.[10]
- In more densely populated areas, with the help of resources such as for example signal strength and/or SSID (which anybody with a WiFi capable device may detect), it is possible to determine the precise location of the access point and thus, in many cases, to ascertain the identity of the individual(s) living in the precise place (house or apartment) where the access point is located.
- In very densely populated areas, even with the help of signal strength information, the MAC address will point to several apartments as the potential access point location. In these circumstances it is not possible without unreasonable effort to ascertain precisely the individual living in the apartment where the access point is located.

The fact that in some cases the owner of the device currently cannot be identified without unreasonable effort, does not stand in the way of the general conclusion that the combination of a MAC address of a WiFi access point with its calculated location, should be treated as personal data.

Under these circumstances and taking into account that it is unlikely that the data controller is able to distinguish between those cases where the owner of the WiFi access point is identifiable and those that he/she is not, the data controller should treat all data about WiFi routers as personal data.

It is important to recall that it is not necessary that the purpose of the processing of these geolocation data is to identify the users. Whether it requires an unreasonable effort to identify the owners of the WiFi access

[9] WiFi access points may even be directly identifyable, if the internet access provider keeps a register of the MAC addresses of the WiFi routers it provides to its identified customers.
[10] The availability of such registries or directories varies per Member State.

points, is strongly influenced by the technical possibilities for the controller or any other person to identify them.

5. Obligations arising from data protection laws

5.1 Data controller

In the context of online geolocation services provided by information society services three different functionalities can be discerned, with different responsabilities for the processing of personal data. These are: controller of a geolocation infrastructure; provider of a specific geolocation application or service and the developer of the operating system of a smart mobile device. In practice, companies often fulfill many roles at the same time, for example when they combine an operating system with a database with mapped WiFi access points and an advertising platform.

5.1.1 Controllers of geolocation infrastructure

Similar to telecom operators when they process the location of a specific device with the help of their base stations, owners of databases with mapped WiFi access points process personal data when they calculate the location of a specific smart mobile device. Since they both determine the purposes and means of this processing they are controllers as defined in article 2(d) of the data protection directive.

It is important to underline that the specific device is instrumental in calculating its location, by passing its own location data (often a combination of GPS, WiFi and base station) and the unique IDs from nearby WiFi access points to the owner of the database.[11] Such a device also fulfills the criterion of article 4.1(c) of the data protection directive, *equipment situated on the territory of a Member State*.

Since the MAC address of a WiFi access point, in combination with its calculated location, should be treated as personal data, the collection of these data also results in the processing of personal data. Regardless of the way in which these data are collected (once or continuously), the owner of such a database should comply with the obligations of the data protection directive.

5.1.2 Providers of geolocation applications and services

Smart mobile devices enable the installation of software from third parties, so called *applications*. Such applications can process the location data (and other data) from a smart mobile device independently from the

[11] The mobile device can forward the different geolocation data it receives for the controller to calculate its location, or calculate its location itself. In both cases the device is essential equipment for the processing.

developer of the operating system and/or the controllers of geolocation infrastructure.

Examples of such services are: a weather-service that forecasts the chance of rain in the next few hours in a very specific region, a service that offers information about nearby stores, a lost phone identification service or a service that shows the location of friends.

The provider of an application that is capable of processing geolocation data is the controller for the processing of personal data resulting from the installation and use of the application.

Of course, it is not necessary to always install separate software on a smart mobile device. Many geolocation services can also be accessed through a browser. An example of such a service is the use of an online map to guide a person walking through a city.

5.1.3 Developer of the operating system

The developer of the operating system of the smart mobile device can be a controller for the processing of geolocation data when it interacts directly with the user and collects personal data (such as by requesting initial user registration and/or collecting location information for the purposes of improving services). As a controller the developer must employ privacy by design principles to prevent secret monitoring, either by the device itself or by the different applications and services.

A developer is also the controller for the data it processes if the device has a 'phone home' functionality for its whereabouts. Since the developer in that case decides on the means and purposes for such a data stream, it is the controller for the processing of these data. A common example of such a 'phone home' functionality is the automatic provisioning of time zone updates based on location.

Thirdly, the developer is a controller when it offers an advertising platform and/or a webshop-like environment for applications and it is able to process personal data resulting from the (installation and use of the) geolocation applications, independently from the application providers.

5.2 Responsibilities of other parties

There are many other online parties that enable the (further) processing of location data such as browsers, social networking sites or communication media that enable for example 'geotagging'. When they embed geolocation facilities in their platform, they have an important responsibility to decide on the default settings of the application (default 'ON' or 'OFF'). Though they are only controllers to the extent that they themselves actively process personal data, they have a key role to fulfill in the legitimacy of the processing of data by controllers such as the providers of specific applications, for example when it comes to the visibility and quality of the information about the processing of geolocation data.

5.2 Legitimate ground

5.2.1 Smart mobile devices

If telecom operators want to use base station data in order to supply a value-added service to a customer, according to the revised e-privacy directive they must obtain his or her prior consent. They must also make sure the customer is informed about the terms of such processing.

Given the sensitivity of the processing of (patterns of) location data, *prior informed consent* is also the main applicable ground for making data processing legitimate when it comes to the processing of the locations of a smart mobile device in the context of information society services.

According to the data protection directive, article 2(h), consent must be freely given, specific and informed indication of the data subject's wishes.

Depending on the type of technology used, the user's device plays a relatively active role in the processing of the geopositioning data. The device is able to transmit location data from different sources to any third party. This technical capacity should not be confused with the lawfulness of such data processing. If the default settings of an operating system would allow for the transmission of location data, a lack of intervention by its users should not be mistaken for freely given consent.

To the extent that developers of operating systems and other information society services themselves actively process geolocation data, (for example when they gain access to location information from or through the device) they must equally seek the prior informed consent of their users. It must be clear that such consent cannot be obtained freely through mandatory acceptance of general terms and conditions, nor through opt-out possibilities. The default should be that location services are 'OFF', and users may granularly consent to the switching 'ON' of specific applications.

Consent of employees

Consent as a legitimate ground for processing is problematic in an employment context. In its opinion on the processing of personal data in the employment context the Working Party wrote: "*where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent. (…) An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent, but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid.*"[12] In stead of seeking consent, employers must investigate whether it is demonstrably necessary to supervise the exact

[12] WP48, Opinion 8/2001 on the processing of personal data in the employment context.

locations of employees for a legitimate purpose and weigh that necessity against the fundamental rights and freedoms of the employees. In cases where the necessity can be adequately justified, the legal basis of such a processing could be based on the legitimate interest of the controller (article 7(f) of the data protection directive). The employer must always seek the least intrusive means, avoid continuous monitoring and for example choose a system that sends an alert when an employee is crossing a pre-set virtual boundary. An employee must be able to turn off any monitoring device outside of work hours and must be shown how to do so. Vehicle tracking devices are not staff tracking devices. Their function is to track or monitor the location of the vehicles in which they are installed. Employers should not regard them as devices to track or monitor the behaviour or the whereabouts of drivers or other staff, for example by sending alerts in relation to speed of vehicle.

Consent of children

In some cases children's consent must be provided by their parents or other legal representatives. This means for example that the provider of a geolocation application needs to provide notice to parents about the collection and the use of geolocation data from children and obtain their consent before collecting and further using the information about their children. Some geolocation applications are specifically designed for parental supervision, for example by continuously revealing the locations of the device on a website, or by issuing an alert if the device leaves a predesigned territory. The use of such applications is problematic. In its Opinion 2/2009[13] on the protection of personal data of children the Article 29 Working Party wrote*: It should never be the case that, for reasons of security, children are confronted with over-surveillance that would reduce their autonomy. In this context, a balance has to be found between the protection of the intimacy and privacy of children and their security.*

The legal framework provides that parents are responsible that the childrens' right to privacy is guaranteed. At the very least, if parents judge that the use of such an application is justified in specific circumstances, the children must be informed and, as soon as reasonably possible, allowed to participate in the decision to use such an application.

Consent must be specific, for each of the different purposes that data are being processed for. The controller must make it very clear if his service is limited to providing an answer to the voluntary question 'Where am I right now?', or if his purpose is to create answers to the questions 'Where are you, where have you been and where will you be next week?' In other words, the controller must pay specific attention to consent for purposes a data subject does not expect, such as for example profiling and/or behavioural targeting.

If the purposes of the processing change in a material way, the controller must seek renewed specific consent. For example, if originally a company

[13] WP160, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools).

stated it would not share personal data with any third party, but now wishes to share, it must seek the active prior consent of each customer. A lack of response (or other kind of opt-out scenario) does not suffice.

It is important to distinguish between consent to a one-off service and consent to a regular subscription. For example, in order to use a particular geolocation service, it may be necessary to switch on geolocation services in the device or the browser. If that geolocation capacity is switched 'ON', every website may read the location details of the user of that smart mobile device. In order to prevent the risks of secret monitoring, the Article 29 Working Party considers it essential that the device continuously warns that geolocation is 'ON', for example through a permanently visible icon.

The Working Party recommends that providers of geolocation applications or services seek to renew individual consent (even where there is no change in the nature of processing) after an appropriate period of time. For instance, it would not be in order to continue to process location data where an individual had not actively used the service within the previous 12 months. Even where a person has used the service they should be reminded at least once a year (or more often where the nature of the processing warrants it) of the nature of the processing of their personal data and be presented with an easy means to opt-out.

Last but not least, data subjects must be able to withdraw their consent in a very easy way, without any negative consequences for the use of their device. Independently from the European data protection directives, the World Wide Web Consortium (W3C) has developed a draft standard for geolocation API that stresses the need for prior, express and informed consent. [14] W3C specifically explains the need to respect withdrawal of consent, advising implementors of the standard to consider that "*the content hosted at a certain URL changes in such a way that the previously granted location permissions no longer apply as far as the user is concerned. Or the users might simply change their minds.*"

Example of best practice for providers of geolocation applications

An application that wants to use geolocation data clearly informs the user about the purposes for which it wants to use the data, and asks for unambiguous consent for each of the possibly different purposes. The user actively chooses the level of granularity of geolocation (for example, on country level, city level, zip code level or as accurately as possible). Once the location service is activated, an icon is permanently visible on every screen that location services are 'ON'. The user can continuously withdraw his consent, without having to exit the application. The user is also able to easily and permanently delete any location data stored on the device.

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

5.2.2 WiFi access points

On the basis of the data protection directive, companies can have a legitimate interest in the necessary collection and processing of the MAC addresses and calculated locations of WiFi access points for the specific purpose of offering geolocation services.

The legitimate ground of article 7(f) of the data protection directive requires a balance between the legitimate interests of the controller and the fundamental rights of the data subjects. Given the semi-static nature of WiFi access points, the mapping of WiFi access points in principle constitutes a lesser threat to the privacy of the owners of these access points than the real-time tracking of the locations of smart mobile devices.

The balance between the rights of the controller and the rights of the data subject is dynamic. In order for controllers to successfully let their legitimate interests prevail over time over the interests of the data subjects, they must develop and implement guarantees, such as the right to easily and permanently opt-out from the database, without needing to provide additional personal data to the controller of such a database. They can for example use software to automatically detect that a person is connected to a specific access point.[15]

Additionally, for the purpose of offering geolocation services, the collection and processing of SSIDs is not necessary. Therefore the collection and processing of SSIDs is excessive to the purpose of offering geolocation services based on mapping of the location of WiFi access points.

5.3 Information

The different controllers must make sure the owners of the smart mobile device are adequately informed about the key elements of the processing in conformity with Article 10 of the data protection directive, such as their identity as controller, the purposes of the processing, the type of data, the duration of the processing, the rights of data subjects to access, rectify or cancel their data and the right to withdraw consent.

The validity of consent is inextricably linked to the quality of the information about the service. Information must be clear, comprehensive,

[15] A possible use case is the following:
1. A data subject goes to a specific web page, on which he can enter the MAC address of his WiFi access point.
2. If the MAC address appears in the database with the mapped WiFi access points, the controller can show a verification page containing a script that asks for the ARP table of the internet device. Theoretically, the WLAN MAC-addresses can be shown through the command 'ARP –a'. With the help of code contained in the browser, such as java, this ARP table can be produced in the background.
3. If the MAC address does appear in the ARP table, it is determined that the user connected to WLAN is also the one with access to the local WLAN MAC-address. The controller thus verifies the request for deletion, in an automatic and easy way.

understandable for a broad, non-technical audience and permanently and easily accessible.

The information must be aimed at a broad audience. Controllers may not assume their customers are technically skilled persons, just because they own a smart mobile device. Information must be age-adapted if the controller knows it attracts a youthful audience.

If providers of geolocation applications intend to calculate the locations of a device more than once, they must keep their customers informed as long as they process location data. They must also enable their customers to continue or revoke their consent. In order to achieve these goals, the providers of applications should collaborate closely with the developer of the operating system. The developer is technically in the best position to create a permanently visible reminder that location data are being processed. The developer is also in the best position to control that no applications are being offered that secretly monitor the whereabouts of smart mobile devices.

If the developer of the operating system has created a phone home functionality or other means of gaining access to data stored on the device, or gains access to location data in other ways, for example through third party advertisers, he must inform the data subject in advance about the (specific and legitimate) purposes for which he intends to process these data and the duration of the processing..

The obligation to inform data subjects also applies to the controllers of databases with geolocated WiFi access points. They must inform the general public in an adequate way about their identity and the purposes of the processing and other relevant information. A mere mentioning of the possible collection of data about WiFi access points in a specific privacy statement aimed at the users of a geolocation application is not enough. There are enough means, online and offline, to inform the general public.

5.4 Data subject rights

Data subjects have a right to obtain from the different controllers access to the location data they have collected from their smart mobile devices, as well as information on the purposes of the processing and the recipients or categories of recipients to whom the data are disclosed. The information must be provided in a human readable format, that is, in geographical locations, in stead of abstract numbers of for example base stations.

Data subjects also have a right to access possible profiles based on these location data. If location information is stored, users should be allowed to update, rectify or erase this information.

The Working Party recommends that controllers seek secure ways to provide direct online access to location data and possible profiles. It is key

that such access is provided without demanding additional personal data to ascertain the identity of the data subjects.

5.5 Retention periods

Providers of geolocation and application services should determine a retention period for location data no longer than is necessary for the purposes for which the data were collected or for which they are further processed. They must ensure that geolocation data, or profiles derived from such data, are deleted after a justified period of time.

In case it is demonstrably necessary for the developer of the operating system and/or controller of a geolocation infrastructure to collect anonymous location history data for the purpose of updating or enhancing its service, extreme care must be taken to avoid making this data (indirectly) identifiable. In particular, even if the mobile device is identified with a randomly attributed Unique Device Identifier (UDID), such a unique number should only be stored for a maximum period of 24 hours for operational purposes. After that period this UDID should be further anonymised while taking into account that true anonymisation is increasingly hard to realise and that the combined location data might still lead to identification. Such a UDID should neither be linkable to previous or future UDIDs attributed to the device, nor should it be linkable to any fixed identifier of the user or the telephone (such as a MAC address, IMEI or IMSI number or any other account numbers).

With regard to data about WiFi access points, once the MAC address of a WiFi access point is associated with a new location, based on the continuous observations of owners of smart mobile devices, the previous location must immediately be deleted, to prevent any further use of the data for inappropriate purposes, such as marketing aimed at people that have changed their location.

6. Conclusions

With the help of geolocation technologies such as base station data, GPS and mapped WiFi access points, smart mobile devices can be tracked by all kinds of controllers, for purposes ranging from behavioural advertising to monitoring of children.

Since smartphones and tablet computers are inextricably linked to their owner, the movement patterns of the devices provide a very intimate insight into the private life of the owners. One of the great risks is that the owners are unaware they transmit their location, and to whom. Another, related, risk is that the consent for certain applications to use their location data is invalid, because the information about the key elements of the processing is incomprehensible, outdated or otherwise inadequate.

There are different obligations for the different stakeholders, ranging from the developers of the operating systems to application providers and

parties such as social networking sites that embed location functionalities for mobile devices in their platforms.

6.1 Legal framework

- The EU legal framework for the use of geolocation data from smart mobile devices is primarily the data protection directive. Location data from smart mobile devices are personal data. The combination of the unique MAC address and the calculated location of a WiFi access point should be treated as personal data.
- In addition, the revised e-privacy directive 2002/58/EC only applies to the processing of base station data by telecom operators.

6.2 Controllers

- Three types of controllers can be discerned. They are: controllers of geolocation infrastructure (in particular controllers of mapped WiFi access points); providers of geolocation applications and services and developers of the operating system of smart mobile devices.

6.3 Legitimate ground

- Because location data from smart mobile devices reveal intimate details about the private life of their owner, the main applicable legitimate ground is prior informed consent.
- Consent cannot be obtained through general terms and conditions.
- Consent must be specific, for the different purposes that data are being processed for, including for example profiling and or behavioural targeting purposes from the controller. If the purposes of the processing change in a material way, the controller must seek renewed specific consent.
- By default, location services must be switched off. A possible opt-out mechanism does not constitute an adequate mechanism to obtain informed user consent.
- Consent is problematic with regard to employees and children. With regard to employees, employers may only adopt this technology when it is demonstrably necessary for a legitimate purpose, and the same goals cannot be achieved with less intrusive means. With regard to children, parents must be judge whether the use of such an application is justified in specific circumstances. At the very least they must inform their children, and, as soon as reasonably possible, allow them to participate in the decision to use such an application.
- The Working Party recommends limiting the scope of consent in terms of time and remind users at least once a year. The Working Party equally recommends sufficient granularity in the consent with regard to the precision of the location data.
- Data subjects must be able to withdraw their consent in a very easy way, without any negative consequences for the use of their device.
- With regard to the mapping of WiFi access points, companies can have a legitimate interest in the necessary collection and processing of the MAC addresses and calculated locations of WiFi access points for the specific purpose of offering geolocation services. The balance of interests between the rights of the controller and the rights of the data subjects requires that the controller offers the right to easily and permanently opt-out from the database, without demanding additional personal data.

6.4 Information

- Information must be clear, comprehensive, understandable for a broad, non-technical audience and permanently and easily accessible. The validity of consent is inextricably linked to the quality of the information about the service.
- Third parties like browsers and social networking sites have a key role to fulfill when it comes to the visibility and quality of the information about the processing of geolocation data.

6.5 Data subject rights

- The different controllers of geolocation information from mobile devices should enable their customers to obtain access to their location data in a human readable format and allow for rectification and erasure without collecting excessive personal data.
- Data subjects also have a right to access, rectify and erase possible profiles based on these location data.
- The Working Party recommends the creation of (secure) online access.

6.6 Retention periods

- Providers of geolocation applications or services should implement retention policies which ensure that geolocation data, or profiles derived from such data, are deleted after a justified period of time.
- If the developer of the operating system and/or controller of the geolocation infrastructure processes a unique number such as a MAC address or a UDID in relation to location data, the unique identification number may only be stored for a maximum period of 24 hours, for operational purposes.

Done at Brussels,
On 16 May 2011

For the Working Party
The Chairman
Jacob KOHNSTAMM