ReedSmith

Article 29 Working Party Opinion 13/2011 on geo-location services on smart mobile devices: Where do we go from here?

Author: Cynthia O'Donoghue, Partner, London
Author: Nick Tyler, Associate, London

Publication Date: May 31, 2011

Introduction

On 16 May 2011, the Article 29 Working Party ("Working Party"), the influential group of European Union national data privacy regulators, adopted Opinion 13/2011 on geo-location services on smart mobile devices (the "Opinion").

The Opinion aims to clarify the legal framework applicable to geo-location services, such as: maps and navigation, geo-personalised services, augmented reality, geotagging of Internet content, tracking the whereabouts of friends and location-based advertising.

The Opinion describes the technology involved, assesses the privacy risks and explains how the legal framework of the European Data Protection Directive 95/46/EC (the Data Protection Directive) and related laws apply to a broad range of parties involved in the development, manufacture, operation and provision of geo-location services and infrastructure.

Geo-location Data & Services

Geo-location data relies on various types of an infrastructure to determine the geographic location of a transmitting device, whether it be an individual's mobile phone, laptop or a WiFi access point used by his/her home computer. Information gathered from various infrastructures can be used, either alone or in combination, to create geo-location data:

- GSM Base station data derived by a mobile device when it connects to the base station antenna within a grid or 'cell'. Location can be calculated by a telecom operator registering the links between the mobile device and each base station to which it links; however, this method only provides a rough indication of location, and its ability to pinpoint location can vary from 50 metres in urban to several kilometres rural areas

- GPS (Global Positioning System) can calculate location of a smart mobile device to within a few metres when the device is equipped with a GPS receiver chip that reads satellite transmissions
- WiFi access points rely on a unique MAC address either from a base station or a WiFi access point and continuously broadcast their existence. These access points are automatically detected by mobile devices either actively (by sending a request to a WiFi access point and recording the answers) or passively (by recording scanning and recording access points), resulting in continuous measurements that lead to increasingly accurate location
- Bluetooth, RFID, ZigBee or other similar devices that calculate proximity within a relatively small area by interconnecting devices typically within a range of up to 30 metres

Geo-location data has created the ability to determine the position, speed and direction of travel of a mobile device by constantly monitoring location data, and has resulted in a wealth of services being offered based on calculating the location of a mobile device and which the Opinion highlighted, such as monitoring the location of children, identifying the location of friends or local services such as restaurants, the geo-tagging of photographs to show where the image was taken and the ability to track and recover lost or stolen goods.

The Working Party identified the key privacy risk as being the intimate link between the mobile device and its owner or user, noting that mobiles are rarely lent to other persons, and that such devices contain highly personal information such as email, pictures, contact lists and browsing history. The constant monitoring of geo-location through smart mobile devices allows the collection of about the mobile owner's habits and patterns of behaviour, for example, by deducing a sleeping place from a pattern of inactivity at night, or by deriving data about the movement patterns of friends based on a 'social graph'. A social graph indicates the visibility of friends in social network sites allowing their behavioural traits to be deduced. The Working Party also highlighted the unintentional consequences of making geo-location data available on the Internet when an owner of a mobile device uses geo-tagging services which may result in data theft, burglary or physical assault. Another major risk highlighted by the Working Party was

'function creep', where as new technology emerges new purposes new purposes for processing location data are developed that were not anticipated at the time of collection.

Legal Framework

The Data Protection Directive applies in every case where personal data is being processed as a result of the processing of location data. Personal data has a very broad definition that encompasses any information relating to a natural person, including pieces of information which, taken together, can reasonably lead to the identity of an individual[1]. All entities that process personal data must comply with the obligations of a data controller, such as fair and lawful processing, processing for a specific purpose and limiting the uses of data in a manner consistent with that purpose, and enabling individuals to exercise their data privacy rights.

EC Directive 2002/58/EC (as revised by Directive 2009/13/EC) (the e-Privacy Directive) applies to the processing of base station data[2] by telecom operators[3], including the provision of WiFi hotspots.

Applicability of the Data Protection Directive

The Opinion found that the inextricable link between a mobile device and its owner can lead to both the direct and indirect identity of an individual and identified a broad range of controllers and other entities that collect and process location data:

- **Telecom operators** when processing base station data (or a hybrid geo-location service based on processing other types of location data such as GPS or WiFi data) and other value-added services. Excluded are activities related to the transmission of GPS data over the Internet transmitted via an Internet application, such as when an individual accesses navigational services over the Internet because the telecommunication service provider is a conduit rather than a collector of data, unless that provider is using deep packet inspection.
- **Information society services** (providers of location services and applications based on a combination of base station, GPS and WiFi data) are expressly excluded from the e-Privacy Directive but remain subject to the Data Protection Directive, when they collect personal data through any of the following activities or combination of activities:

- **Controllers of geo-location infrastructure** that operate databases that map WiFi access points and calculate the location of a smart mobile device
- **Providers of specific geo-location applications** (apps) that process geo-location data from a mobile device, by offering information relevant to the area in which a person is located or by accessing information through a browser, such as the use of a online map
- **Developers of operating systems of smart mobile devices** through interacting directly with a user and collecting personal data, or if the device has a 'phone home' function for its whereabouts, or by offering an advertising platform or a webshop-like environment that permits the processing of personal data independently from the app provider

- **Browsers, social networking sites or communication media** that embed geo-location capabilities in their platform, such as geotagging

The Working Party cautioned that as people disclose more and more personal location data on the Internet by publishing the location of, for example, their workplace, and as the disclosure of geo-location may occur without their knowledge, such as when they are geotagged by other people, it becomes easier to link a location or behavioural pattern to a specific individual even if his/her real name is not known.

In addition, the Working Party opined that data about WiFi access points could also lead to the indirect identity of the owner of the access point through collection of the WiFi MAC address in combination with its calculated location, especially in sparely populated areas where a MAC address could point to a single house from which it would then be easy to directly identify an individual through, for example, a property registry. As population density increases, it may be increasingly difficult to identify individuals directly, but by combining the MAC address with signal strength or an SSID (service set identifier, i.e., the name of a wireless network), it may be possible to identify individual(s) living in a house or flat where the access point is located. Notwithstanding the Working Party's admission that in urban areas, it may not be possible to identify individuals without going to unreasonable efforts, the Opinion concludes that the combination of a MAC address and a WiFi access point should be treated as personal data

because a data controller will be unlikely to distinguish between those cases where the owner of the WiFi access point is identifiable and those where he/she is not.

Recommendations of the Working Party

Consent is at the heart of the Opinion. In accordance with the Data Protection Directive[4], consent must be 'freely given, specific and informed indication of the data subject's wishes'. The availability and provision of clear, comprehensive and easily understood information about the purposes for which geo-location data will be collected and used is fundamental to achieving valid consent. Such information must be capable of being understood by a broad, non-technical audience and needs to be permanently and easily accessible.

Other key points to note:

- Consent cannot be obtained through general terms and conditions
- Consent must be specific for the different purposes that data are being processed for and any material change will require 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 both employees and children
- The Working Party recommends limiting the scope of consent in terms of time and reminding users at least once a year of the nature of the processing, providing users with an easy means to opt-out
- Data subjects must be able to withdraw their consent easily without any negative impact on their use of their device
- The ability of individuals to exercise their right of access to location data (in a human readable format) and profiles based on such data, as well as rights of rectification and erasure, must be capable of being exercised - the Working Party recommends the creation of secure online access

- Providers of geo-location applications or services should implement retention policies which ensure that geo-location data, or profiles derived from such data, are deleted after a justified period of time

Final Thoughts

The Opinion is not designed to make any radical change to what is covered by the Data Protection Directive. The Opinion emphasizes that compliance is triggered by the scope of data collected and whether is it included within the definition of 'personal data', even though the Working Party also acknowledges that it is increasingly hard for data to be anonymised. As is so often the case in the area of data protection compliance, prior, informed consent offers the principal route to compliance for all those involved in the development and provision of geo-location services across Europe, and it is clear from the Opinion that mentioning the possible collection of data about WiFi access in a privacy statement is not enough.

The compliant route will present significant practical challenges to a broad range of enterprises seeking to innovate and benefit from rapidly evolving geo-location technology, and the services and opportunities it enables. It may also have a knock-on effect on users' abilities to access and use the services they desire.

Obtaining the required consent is not a straightforward one-off exercise but rather a vehicle for delivering continuing compliance that needs checking, maintenance and refueling to keep it roadworthy.

The full Opinion is available here.

---

1. Article 2(a) of the Data Protection Directive states - *'... 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'.*

2. Article 2(c) of the e-Privacy Directive states - *'"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'.

3. Article 2(c) of the e-Privacy Directive defines 'electronic communications service' as *'...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 exercise editorial control over, content transmitted using electronic communications networks and services; it does not include information society services ... which do not consist wholly or mainly in the conveyance of signals on electronic communications networks'.*

4. at Article 2(h)