2130/05/EN
WP 115

Working Party 29 Opinion on the use of location data with a view to providing value-added services

November 2005

☒ **Discussion**
☒ **Adoption**
☒ **Adoption**

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA,

Set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

Having regard to Article 29, Article 30(1)(a) and Article 30(3) of the above Directive and Article 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

Having regard to its rules of procedure, and in particular Articles 12 and 14 thereof,

Has adopted the following opinion:

The Working Party notes that issues relating to the use of location data are very topical. Such data are defined as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service" (Article 2 of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector).

Background and purpose:

There has been a spectacular increase in the use of location data in the last 20 years, driven by two main factors.

The first is the explosion in the use of satellite location data, which today can be extremely precise and often very valuable, particularly when it comes to assisting individuals in distress.[1] However, such systems are available only to those equipped with the appropriate terminals.

The second factor is the unprecedented spread of mobile telephony, where each user constantly carries about a device through which he or she can be potentially located.

Generally speaking, there are many ways of locating individuals, primarily using "traces" left by the use of new technologies: automatic ticket machines in the transport sector, GPS, bank cards or electronic purses, or, in the case at issue, mobile telephones. At first, location data were regarded as purely technical data required for making or receiving a call from a mobile telephone and available only to electronic communications operators. The term "traffic data" is used in this connection. Such data merely result from the use of a given technology and are no different from other "traces" created every day.

Nevertheless, location data, insofar as they provide key information about an individual (in short, who is where), quickly came to be viewed as a potential source of revenue. Firms have developed a wide variety of services drawing on such data.

---

[1] Satellite geolocalisation is at present offered only by the GPS (Global Positioning System) developed by the US army, the results of which have been made available for civilian uses, primarily marine navigation. The location data are calculated by triangulation and supplied directly to the person who has a GPS receiver. They can then be sent to a third party via an electronic communications network (GPS/GSM combination).

The first such services offered information to individuals on, for example, the nearest chemist or restaurant to their position. Next, services based on the one-off use of location data (providing information at a given moment in time) were supplemented by services based on continuous use of the data (navigational assistance).

This first stage has now given way to a second stage, with the development of services that are no longer based on locating people at their own request (users wishing to avail themselves of a service), but on their being located (at the request of a third party). Tracking and search services have developed whereby individuals can be located via their mobile phones even if they are not using them, but provided that are switched on.

The key issue for the processing of location data has thus moved on from being a question of storage (essentially: on what conditions should location data be stored by electronic communications operators?) to being a question of use (how can we ensure that data are used for supplying value-added services in accordance with the principles applicable to the processing of personal data?).

Legal framework:

Since location data always 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.

Given that the processing of such data is a particularly sensitive matter involving the key issue of the freedom to come and go anonymously, the European legislature, taking into account the considerations of the European data protection authorities, has adopted specific rules requiring that the consent of users or subscribers be obtained before location data needed for supplying a value-added service are processed, and that users or subscribers be informed about the terms of such processing (Article 9 of Directive 2002/58/EC of 12 July 2002).

Article 2 of Directive 2002/58/EC defines traffic data as "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for billing thereof*" and location data as "*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*".

While the two Directives referred to above lay down a satisfactory framework for the processing of location data, the Working Party wishes to spell out how some of their provisions should be applied and to highlight specific aspects of some of the services on offer.

This opinion is not concerned with the conditions governing the processing of location data pursuant to Article 13 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC, i.e. where location data are processed by way of exception to the principles laid down by those Directives, as a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and for the prevention, investigation, detection and prosecution of criminal offences. Given its importance, the Working Party has already expressed its views on this issue on numerous occasions.[2]

[2] See Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications; Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of

1. General conditions governing the use of location data with a view to providing value-added services

The Working Party would point out that, when processing personal data, the various parties involved in providing a value-added service based on the use of location data, whether they are electronic communications operators who process location data or third parties providing the value-added service on the basis of location data sent to them by operators, must comply with their obligations under data protection legislation on protecting personal data.

1.1 The applicable national law

The Working Party has observed the development of value-added services that are based on the processing of location data from electronic communications services, but are provided by companies (e.g. via a website) not established on the territory of the individual concerned, i.e. the data subject.

Under Article 3 of Directive 2002/58/EC, this Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community. Under Article 4 of Directive 95/46/EC, the applicable national law is that of the Member State where the controller is established. This latter provision means that, within the Community, the processing of location data is subject to the national law of the Member State where the controller is established and not the Member State of which the data subject is a national.

Where the controller (the provider of the value-added service) is not established in a Member State, the location data may be transferred from the electronic communications operator to the controller only on the terms laid down in Chapter IV of Directive 95/46/EC on the transfer of personal data to third countries. Such terms include the requirement that the data protection laws in the third country be found adequate by the European Commission or else that the transfer be based on other legitimating grounds — in particular, the data subject's consent, the existence of a contract concluded in the data subject's interest, the existence of a superior public interest, the establishment or defence of a judicial claim, or the need to safeguard the data subject's vital interests.

1.2 Informing the data subjects

The Working Party would point out that Directives 95/46/EC (Article 10) and 2002/58/EC (Articles 6 and 9) require that the subjects of location data to be processed be informed about:

- the identity of the controller and of his representative, if any;
- the purposes of processing;

---

the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000, COM(2000) 385; Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime; Opinion 10/2001 on the need for a balanced approach in the fight against terrorism; Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data; Opinion 1/2003 on the storage of traffic data for billing purposes; and Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)].

- the type of location data processed;
- the duration of processing;
- whether the data will be transmitted to a third party for the purpose of providing the value-added service;
- the right of access to and the right to rectify the data;
- the right of users to withdraw their consent at any time or temporarily refuse the processing of such data, and the conditions on which this right may be exercised;
- the right to cancel the data.

The Working Party takes the view that this information should be provided by the party collecting the location data for processing, i.e. by the provider of the value-added service or, where the provider is not in direct contact with the data subject, by the electronic communications operator.

The information could be provided either in the general terms and conditions for the value-added service or directly each time the service is used. In view of the very sensitive nature of the processing of location data, the Working Party would draw the attention of service providers to the need to provide clear, complete and comprehensive information on the features of the service proposed.

Where information is provided in the general terms and conditions for the service, the Working Party recommends that the service provider should give the individuals concerned the opportunity to consult the information again at any time and by a simple method, such as via a website or while using the service (e.g. by telephoning a dedicated number).

1.3 Consent

Obtaining consent

In accordance with standard practice for personal data protection when sensitive data are processed, European legislation requires prior consent to be obtained for processing location data other than traffic data.

Accordingly, the Working Party wishes to spell out the conditions for obtaining consent.

Article 2(h) of Directive 95/46/EC defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

This definition explicitly rules out consent being given as part of accepting the general terms and conditions for the electronic communications service offered. In this regard, reference may be made to the clarification provided by the Article 29 Working Party in its Opinion No 5/2004 on unsolicited communications for direct marketing purposes, which is particularly relevant in this context.

However, depending on the type of service offered, consent may relate to a specific operation or may constitute agreement to being located on an ongoing basis.

Offering a service that requires the automatic location of an individual (e.g. the possibility of calling a specific number to obtain information on the weather conditions at one's location) is acceptable provided that users are given full information in advance about the processing of their location data. In this case, calling the relevant number would amount to consenting to being located.

Entities required to obtain the data subject's consent

A value-added service based on location data may be provided either directly by the electronic communications operator (the individual concerned contacts the operator, who then provides the service on the basis of the location data obtained from his system) or via a third party (the individual concerned contacts a third party, who then provides the service on the basis of the location data obtained from the operator). In the second case, it is the service provider who must obtain the data subject's consent. Except where the location data is produced by the terminal equipment itself, this requires operators to systematically send location data for an identified individual (the person who contacted the third party in order to use the service) to a third party at the latter's request.

In view of the increase in the number of service providers, the Working Party notes that a high degree of protection in the processing of personal location data could be achieved if operators were to centralise requests to use a value-added service based on location data (customers calling a number managed by the operator) and transferring the requests to the third parties responsible for providing the service in such a way that the service provider cannot identify the customer (e.g. by using an alias[3]). Under this arrangement, the service provider can deliver the service required (e.g. the name of the nearest restaurant) via the operator without being able to identify the person requesting the service.

The Working Party notes also that the end-user terminal could also provide a high degree of protection with its own built-in location capability. The location data can then be processed by an Identity Management System to deliver pseudonyms to multiple service providers. Alternatively, and in view of constantly growing mobile bandwidth and storage capacities, the end-user device could for example download the full list of restaurants in a city and search locally in this list using not only the location data but the user's preferences as well (French cuisine, vegetarian menu, etc.). With these examples, the Working Party underlines the need to consider Privacy Enhancing Technologies as efficient and complementary elements in providing a high and satisfactory degree of protection to users of geolocalisation services.

In any event, the Working Party would draw operators' attention to the need to introduce effective measures to verify and authenticate requests for access to location data made by third parties offering a value-added service.

Measures to ensure that consent is valid

The Working Party takes the view that providers of value-added services must take appropriate measures when obtaining consent to ensure that the person to whom the location data relate is the same as the person who has given consent. Where the processing of location data is ongoing (e.g. services such as *Find-a-friend*), the service provider must:

[3] By "alias" we mean the technical data allowing the service provider to supply the service corresponding to an individual's location data without being able to identify the person by name; only the operator can link the alias to the individual concerned.

- confirm subscription to the service by sending a message to the user's terminal equipment after consent has been received, and
- if necessary, request confirmation of the subscription.

This is to avoid cases of fraudulent subscription without the individual's knowledge (temporary removal of a person's terminal equipment in order to subscribe to the service).

The person whose consent is required

Article 6 and Article 9 of Directive 2002/58/EC refer to the consent of users or subscribers. The Working Party takes the view that, when a service is offered to private individuals, consent must be obtained from the person to whom the data refer, i.e. the user of the terminal equipment.

1.4 Exercising the right to withdraw

Under Article 9 of Directive 2002/58/EC, people who have given their consent for the processing of location data other than traffic data may withdraw consent at any time and must have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data.

The Working Party regards these rights — which can be taken as implementing the right to object to the processing of location data — as essential given the sensitive nature of location data.

The Working Party believes that it is a precondition for the exercise of these rights that individuals are kept informed, not only when they subscribe to a service but also when they use it. Where a service requires ongoing processing of location data, the Working Party takes the view that the service provider should regularly remind the individual concerned that his or her terminal equipment has been, will be or can be located. This will allow that person to exercise the right to withdraw under Article 9 of Directive 2002/58/EC, should he or she wish to do so.

1.5 Data storage time

Location data may be processed only "for the duration necessary for the provision of a value-added service" (Article 9(1) of Directive 2002/58/EC).

This means that, once the service has been provided, the service provider may not in principle store individuals' location data, unless they are needed for billing and interconnection payment purposes.[4]

Should service providers wish to keep a record of the locations of their service's users, they must first render the data anonymous.

[4] In this connection the Working Party would refer to its recommendations on the storage of traffic data for billing purposes (Opinion 1/2003 of 29 January 2003).

1.6 Security measures and transmission to third parties

The Working Party would draw the attention of electronic communications operators and providers of value-added services based on the processing of location data to the need to introduce security measures designed to ensure the confidentiality and integrity of the location data processed.

Under Article 9(3) of Directive 2002/58/EC, location data to be processed for providing a value-added service may not be transmitted to third parties other than those who provide the value-added service. Only persons acting under the authority of the third party providing the value-added service may process the data, to the extent and for the duration necessary for providing the service. Accesses by such persons to the location data should also be logged.

2. Conditions for implementing certain location services in the light of their purpose

Apart from complying with the specific provisions laid down in Directive 2002/58/EC, location services, because they use personal data, must meet the requirements of Article 6 of Directive 95/46/EC, which stipulates that personal data may be used only "for specified, explicit and legitimate purposes". The Working Party would therefore like to examine the conditions under which certain location services may be implemented, in particular in the light of their purpose.

2.1 Location of minors

The Working Party has observed the development of location services designed for parents, allowing them, for example, to connect to a website in order to ascertain the location of their children, to whom they have given a mobile telephone. This type of service raises a number of problems, related in particular to the need for striking a balance between the different interests and rights at stake.

A service whereby children can be located via a mobile telephone may well meet the wishes of some parents.

Media coverage of criminal cases involving children, the need to monitor children affected by certain illnesses or the emergence of an increasingly "nomadic" lifestyle may lead some parents to seek to be "reassured" by the possibility of locating their children at any time without having to call them direct. This new use of the mobile telephone for the benefit of parents, and at their expense, can be viewed as a sort of family "contract": greater independence of communication for the child in exchange for the possibility of being located by the parent.

In this respect, such services may meet an identified modern "need" and reflect a desire on the part of service providers to position themselves on a market which is likely to expand and which represents a new example of how the possibilities offered by location data are marketed.

However, this service could equally be looked at the other way around: from the point of view not of the parent, however understandable that point of view may be, but that of the child.

The Working Party would recall that Articles 3 and 18 of the International Convention on the Rights of the Child state that the "best interests of the child shall be a primary consideration" in any decision concerning children. In the case at issue, one should also consider that Article 16 of the Convention provides that “no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence”.

Questions thus arise with respect to the use of this kind of service, which may possibly upset the normal relations of mutual trust between parents and their children and prevent children from gaining the necessary distance between themselves and their parents as they become more independent. Moreover, might not such a system, perversely, cause some parents to abandon their responsibility while maintaining the illusion of controlling — or at least monitoring — their children's activities? From a societal point of view, might not the development of this kind of service also help to accustom individuals from a very young age to a semi-permanent form of monitoring which they will no longer even perceive as intrusive?

Lastly, there is a risk that parents will confuse knowing where their child's mobile telephone is with knowing what the child is actually doing.

The Working Party therefore calls at least for vigilance in the use of this type of service and would point out that it must be implemented in accordance with the rules on the processing of location data and in accordance with specific national legislation regarding the age of the minors concerned.

Service providers must accordingly introduce appropriate procedures for identifying people who register as parents and for limiting access to the service to those people alone.

In addition, there is the question of the minor's consent to being the subject of a location request.

In this connection, the Working Party notes that it is impossible to verify, when a location request is made, that the person using the telephone is the minor concerned and not someone else, perhaps an adult, to whom the subscriber to the service has entrusted the relevant telephone. It therefore recommends that the consent of the telephone user should be obtained, at least when the service is subscribed to. In order to prevent the fraudulent registration of telephones, service providers should, for instance, send messages to the relevant telephone specifying that it has been the subject of a location request, so that the telephone user can in particular exercise the right to withdraw pursuant to Article 9 of Directive 2002/58/EC.

2.2 Location of employees

The Working Party has already addressed the issue of the processing of personal data in the employment context.[5] It stressed that surveillance of workers must be carried out in the least intrusive way possible.

Data processing which allows an employer to collect data on the location of an employee, either directly (location of the employee him/herself) or indirectly (location of the vehicle used by the employee or of a product or asset in his/her charge) involves the use of personal data and is subject to the provisions of Directive 95/46/EC.

---

5 Opinion 8/2001 of 13 September 2001 on the processing of personal data in the employment context.

The Working Party has observed the development of systems allowing companies to identify the geographic position of their staff at a given moment in time or continuously by locating objects in their possession (badge, mobile telephone, etc.) or use (vehicles).

This information can be based on the processing of data from satellites (GPS), from an electronic communications network (mobile telephone, Wi-Fi network) or from any other device (such as an RFID tag located by a reader). It is increasingly being supplemented by data from various sensors which go beyond location data in the strict sense, e.g. data on the length of time for which a machine or vehicle is used, the number of kilometres covered or the speed at which a vehicle has travelled.

Such processing raises two issues: the dividing line between work and private life and the degree of monitoring and permanent surveillance to which it is acceptable to subject an employee.

The Working Party would like to recall, from a data protection point of view, that the lawfulness of such processing operations should not rely exclusively on the employee's consent, which must be "freely given" under the Directive. As already pointed out by the WP in its working document on data protection in the employment context, the issue of consent should be addressed in a broader perspective; in particular, the involvement of all the relevant stakeholders (as envisaged in the legislation of several Member States) via collective agreements might be an appropriate way to regulate the gathering of consent statements in such circumstances.

Given the requirement that data be processed for specific purposes, the Working Party takes the view that the processing of location data on employees must correspond to a specific need on the part of the company which is connected to its activity. Processing location data can be justified where it is done as part of monitoring the transport of people or goods or improving the distribution of resources for services in scattered locations (e.g. planning operations in real time), or where a security objective is being pursued in relation to the employee himself or to the goods or vehicles in his charge.

Conversely, the Working Party considers data processing to be excessive where employees are free to organise their travel arrangements as they wish or where it is done for the sole purpose of monitoring an employee's work where this can be monitored by other means. In these two cases, its purpose does not justify the use of undeniably intrusive processing given the type of data collected. This is compounded further by the existence of national legislation expressly prohibiting the distance monitoring of employees to assess their performance.

In any event, the purpose requirement means that an employer should not collect location data relating to an employee outside the latter's working hours. The Working Party therefore recommends that equipment made available to employees, especially vehicles, which can also be used for private purposes be equipped with a system allowing employees to switch off the location function.

Location data relating to an employee must be kept for as long as is appropriate in view of the purpose advanced as justification for processing such data. Given the possible justifications for processing location data, processing will essentially be done in real time. In any event, the Working Party recommends that the location data retention period be reasonable, i.e. no longer than two months.

Where an employer wishes to process location data for longer than two months (e.g. to establish a historical record of journeys in order to optimise rounds), the Working Party recommends that the data first be rendered anonymous.

Access to location data must be restricted to persons who, in the course of exercising their duties, may legitimately consult them in the light of their purpose. Employers must therefore take all necessary precautions in order to keep such data secure and to prevent unauthorised access to them, in particular by introducing verification and identification measures.

Lastly, the Working Party would highlight the obligation to inform the employees concerned and would draw companies' attention to the need to introduce location systems in such a way that staff are made aware of their existence.

Done at Brussels, on 25 November 2005

For the Working Party

The Chairman
Peter Schaar