International Working Group
on Data Protection
in Telecommunications

675.29.8 19 November 2004

Common Position
on
Privacy and location information in mobile communications services

- adopted at the 29th meeting on 15-16 February 2001 in Bangalore -
- revised at the 36th meeting on 18-19 November 2004 in Berlin -

Location information has been processed in mobile communications networks from the very beginning. As long as this information was only generated and used for establishing and maintaining a connection to the mobile device, location information resided only with the operators of telecommunications networks, which are in most countries bound very strictly by telecommunications secrecy legislation. The precision of the location information was dependent upon the size of the respective cells in the cellular networks.

Partly driven by legal obligations to make more precise location information about mobile devices available for use by emergency services, network operators have started to modify the technical infrastructure of their networks to conform with these obligations. This means that much more precise information about the location of any mobile device will become available in the near future. Equipment manufacturers claim that even today a precision of up to 5 meters is technically feasible when using GPS-assisted systems. At the same time it is envisaged that the developing mobile electronic commerce will lead to the creation of a wealth of new services based on knowledge about the more precise location of the user. However, such services will most likely not only be provided by telecoms operators, but also by third parties which may not be legally bound by the restrictions of telecommunications secrecy.

The enhanced precision of location information and its availability to parties other than the operators of mobile telecommunications networks create unprecedented threats to the privacy of the users of mobile devices linked to telecommunications networks. Accordingly, the Working Group recommends that the technology for locating mobile devices should be designed to be minimally invasive to privacy.

The following principles should be observed, with respect to the provisions of value added services:

1. The design and selection of technical solutions to be used for such services must be oriented to the goal of collecting, processing and using either no personal data at all or a minimal amount of personal data.

2. Precise location information should not normally be generated as a standard feature of the service, but only "on demand" where it is needed to provide a certain service that requires knowledge of the location of the user's device.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

3. The user must remain in full control of the generation of precise location information within the network. In this respect, handset-based solutions where the creation of precise location information is initiated by the mobile device appear to offer a better degree of privacy than network-based solutions where location information may be generated as a standard feature and the user control is limited to the extent to which it may be communicated to third parties. However, the mobile subscriber should always be able to control both the possibility of using any location services or specific location services. The provider should give the subscriber the opportunity to opt-in to the possibility of the use of any location services when presenting the subscriber contract. The subscriber may opt-in at this point or at any future time and may opt-out of all location services at any time. Where the mobile subscriber may have opted in, the mobile user should be free to give consent or to opt out of the service.

4. The telecommunication provider may only deliver location information to a third party in cases where the mobile subscriber has given his informed consent to the operator on the alternative use of location information.[1] Users should be able to disable the precise determination of their location at any time without disconnecting their device from the network. Users or mobile subscribers should also be able to enable the disclosure their location information at a chosen level of precision (e.g. building, street, city or state level).

5. Location information should only be made available to providers of value added services where the user has given his informed consent to such disclosure. Consent may be restricted to a single transaction or to certain providers of value added services. The user must be able to access, correct and delete his or her preference data whether such data stored on the mobile device or within the network.

6. The creation of movement profiles by telecommunications service providers and providers of value added services should be strictly forbidden by law other than where necessary for the provision of a certain service and conditional on the user's informed, unambiguous consent.

7. Location information is a highly sensitive category of information. Access, use and disclosure of such information should be subject to the same or similar controls as for content data that are protected by telecommunications secrecy. The Working Group refers to its Common Position on Public Accountability in relation to Interception of Private Communications (Hong Kong, 15.04.1998; http://www.datenschutz-berlin.de/doc/int/iwgdpt/inter_en.htm).

8. Wherever possible, mobile network operators should not communicate location information together with personally identifiable information about the user to providers of value added services. Instead, pseudonymous information should be used. Personally identifiable information (e.g. the ID of the mobile device) should only be made available to providers of value added services with the user's informed consent. Any location information should be deleted by the service provider when no longer necessary for the provision of that service.

9. A provider must not make the rendering of a service or the terms of the service conditional upon the consent of the user to the effect that his or her personal localisation data may be processed where such data are not necessary for the provision of the service.

[1] Cf. Art. 6 and 9 Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).