

No place to hide

By Henriette Tielemans and Kristof Van Quathem

Privacy regulators from all 27 EU member states gathered earlier this year for a meeting of the so-called Article 29 Working Party and issued an opinion paper on how geo-location information collected by mobile devices should be treated under the union's data protection laws.

The working party's position could impact seriously on geo-location services in the coming years. While not binding, the opinion carries considerable weight and inevitably will guide national regulators in their enforcement actions. Moreover, national regulators no doubt hope the opinion will influence the European Commission, which is currently drafting amendments to revisions of the 1995 Data Protection Framework Directive.

The working party's decision to draft an opinion on geo-location data and services dates from last autumn, when several high profile cases – in particular, an action involving Google's StreetView – caught the regulator's attention. These origins are reflected in the opinion, which is limited to two issues: the collection of geo-location data from mobile telephones; and the collection of data from wireless access points.

The difference is important as regulators seem to attach a different level of sensitivity to the two collection methods. The working party indicates that it has not examined other existing geo-tagging and geo-location technologies.

Sensitivity

Geo-location data is personal data covered by the EU Data Protection Directive. This applies both to data derived from mobile telephones and to public data captured from wireless access points.

For mobile 'phones, the working party takes the position that the combination of subscriber data and unique

numbers – such as the media access control (MAC) address, the international mobile equipment identification, the international mobile subscriber identification and other unique numbers created by application providers – are sufficient to render this data, and associated location data, as personal data.

Similarly for wireless access points, the working party considers that the MAC address

Opt-out possibilities must be provided but they are insufficient to meet legal requirements

and the service set identifier (SSID) combined with other publicly available information is sufficient to render this information as personal data.

Given the sensitivity of the processing of patterns of geo-location data generated by mobile phones, this information can only be collected for value added services on the basis of users' prior informed consent. This consent should be renewed at least annually (or more often if the purposes of the processing change) and it should be easy to withdraw. The consent must be specific for each of the different purposes for which the data is collected, and it cannot be obtained through mandatory acceptance of general terms and conditions.

Opt-out possibilities must be provided but they are insufficient to meet legal requirements. The default setting of the user's device must disable communications of geo-location data (in other words, creating privacy by default).

For data derived from wireless points, the working party seems to suggest that no consent is required provided sufficient guarantees are in place, such as an ability easily to opt-out

and no SSIDs are collected. The working party takes the position that it is excessive to collect SSIDs for purposes of offering geo-location in the framework of wireless access points.

User rights

Users must be informed about the communication of geo-location data through their mobile 'phones. The working party calls for a permanent icon to be illuminated on the device when geo-location tracking is enabled to avoid the surreptitious tracking of individuals.

Moreover, application providers and developers of operating systems should work together to ensure that the necessary information is imparted to users. Users should be in a position actively to choose the detail of geo-location information collected (on a country, city, or postal code level, for example).

Users must be granted access to their location data and any profiles created on the basis of location data. The information must be understandable to users and thus be provided, preferably on line, in the form of locations, not numbers. Users also must be granted the right to have location data deleted.

The working party calls for short retention periods as, given their sensitivity, geo-location data should not be kept longer than necessary in light of the purposes for which it was collected. Therefore, the data – as well as any profiles created on the basis of that data – should be promptly deleted.

- For a full copy of the working party's opinion, see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

Henriette Tielemans is a partner in the data privacy practice at the Brussels office of US-based law firm Covington & Burling. Kristof Van Quathem is a policy advisor at the firm