Privacy & Security Law Report™

May 23, 2011

EU Data Protection

Art. 29 Party Opinion Parses Data Protection Rules Application to Geolocation Information

by Donald G. Aplin

The geolocation information of individuals is personal, and companies that collect such data from mobile devices must comply with the privacy requirements of the EU Data Protection Directive (95/46/EC), the Article 29 Working Party said in an opinion made public May 18.

Protecting location data is an important privacy concern because, among other things, it can be used to create behavioral profiles of individuals that reveal intimate information, such as places of worship or healthcare centers frequented by the data subject, the Art. 29 Party said. Art. 29 is made up of data protection officials from each of the EU member states.

Location information is personal data regardless of whether it is collected via wireless internet connections (WiFi), global positioning satellite (GPS) systems, or base stations (cell antenna sites), the opinion said, and thus must meet user consent, data collection, and data use restrictions of the Data Directive, the opinion said.

In addition, location information gains protected status regardless of whether it can be tied by name to an individual, the opinion said, so long as it can be linked to a specific mobile device.

Eduardo Ustaran, a partner at Field Fisher Waterhouse LLP, in London, counseled in a May 18 firm blog post that the Art. 29 Party's conclusion that location data is personal data "is a massive generalisation of the multiples modalities of geolocation services, many of which will rely on anonymous data or, at least, data which is not meant to identify or affect a particular user."

Ustaran said that the Art. 29 Working Party's stand requiring mobile device user consent for collection and use of nearly all geolocation data "may go further than what the EU legal framework intended."

User Consent Burdens on Businesses

As to user consent, the opinion, which was approved May 16, sets forth a list of best practices, including consent to be confirmed every year if an individual has not used a location application within the last 12 months and the display of an icon on the mobile device screen whenever a location data collection program is operating, so users can choose to turn off or permanently opt out of the collection of their location data.

"In line with the opinion of the Working Party, providers of geolocation applications and services may need to revisit existing consent forms to ensure that the consent obtained from customers is sufficiently specific. The Working Party's recommendation to renew customer consent each year can prove particularly burdensome in practice," Wim Nauwelaerts of Hunton & Williams in Brussels told BNA May 18.

"The Working Party promotes as a best practice that providers of geolocation applications implement technical features (such as icons) that warn users when location services are on. It will therefore be important for providers of geolocation applications to take account of privacy concerns as early as possible in the design stage of these applications," Nauwelaerts cautioned.

In fact, the opinion encourages geolocation applications providers and mobile device operating system makers to actively incorporate privacy by design to protect geolocation data as they are planning new services and operating systems.

The Working Party said the opinion does not consider the applicable legal frameworks or privacy implications of so-called "geotagging," in which social networking sites integrate users location data or the use of location data in small closed environments, such as a shopping center or airport, through the use of connections like Bluetooth or radio frequency identification tags.

Special Consent Situations, e-Privacy Directive

The opinion emphasized that collecting workplace location data on employees presents special challenges and encouraged employers to balance the need for such information with the long term impact in undercutting worker privacy.

The Art. 29 Party said that although technology has changed dramatically since its 2001 opinion on the processing of personal information in the employment context (Opinion 8/2001), the principles regarding the balance of legitimate employer need for the data and worker privacy are still valid.

Gaining the consent of children to the collection of location data also drew special attention from the Working Party, which again said that—like employers and workers—a balance is at play between legitimate uses of such data by parents and others and the right of data subjects to have their privacy protected. The Art. 29 Party pointed to its 2009 opinion on the protection of personal information of children (Opinion 2/2009) as a starting point for evaluating the required balance (8 PVLR 343, 3/2/09).

In addition to complying with the Data Protection Directive, telecommunications providers that collect location data from base stations used to operate their telecommunications service are covered by the amended e-Privacy Directive (2009/136/EC). The Working Party noted that it had said in 2005 (Opinion 5/2005-WP 115) that telecoms could access base station data to provide "value-added services" based on location information.

Telecoms that offer so-called “hybrid” location-base services through the use of WiFi and/or GPS location data in combination with location data from base stations would also be required to comply with the e-Privacy Directive which requires, among other things, that explicit prior user consent be gained before gathering location data.

In general, however, non-telecom firms, such as mobile device application makers and that use location data collected via WiFi, are classified as “information society services” and are exempt from the e-Privacy Directive prior consent requirement. Nevertheless, the opinion said that if developers “actively process geolocation data” they must seek the prior informed consent of users to the collection of their location data.

The opinion also discusses data retention issues related to geolocation information and concludes that services should retain location data for “no longer than is necessary for the purposes for which the data are collected.” Even for information tied only to a unique device identifier, collected location data must be retained no longer than 24 hours unless it is anonymized, the opinion instructed.

Meanwhile, in the United States, a Senate subcommittee heard testimony May 19 from representatives of Google Inc., Apple Inc., and Facebook Inc. on privacy issues related to mobile device applications, including the collection of user location data (see related report in this issue).