

Geolocation services — where does the Article 29 Working Party stand?

Philip Nolan, Partner, and Oisín Tobin, Trainee Solicitor, at Mason Hayes + Curran, examine data protection aspects of the processing of location data, drawing from the recent Working Party Opinion

Over the last few years, privacy lawyers have faced the daily challenge of applying the European Data Protection Directive 95/46/EC (‘the Data Protection Directive’) to situations that fall far outside the intent or conception of the original drafters. The development and increasing popularity of location based services, resulting from the proliferation of smart phones, brings still further challenges. Geolocation technology has immense commercial potential for organisations. The ability to tailor services and advertisements to a user’s precise whereabouts represents a quantum leap forward for marketing.

Despite these advantages, location data is highly problematic from a privacy perspective. Smart phones and their users are rarely parted. The full suite of location data generated by such a device provides an intimate picture of the user’s professional and home life.

In its recent Opinion, WP13/11, (‘the Opinion’) the Article 29 Working Party (‘the Working Party’) has waded into the location based data debate. As national Data Protection Authorities frequently take their lead from the positions set out in the opinions of the Working Party, the Opinion calls for careful study. The Opinion represents a thorough and technical consideration of both the law surrounding location based data, and the underlying technology. However, a number of the positions set out in the Opinion are difficult to reconcile with the text of the Data Protection Directive, and, if strictly implemented, could unduly hinder the availability of location based services. This article considers some of the most interesting points in the Opinion.

The interaction between the Data Protection Directive and the e-Privacy Directive

The use of location based data is regulated by two separate Directives: the Data Protection Directive and Directive 2002/58 on Privacy and Electronic Communications as amended by Directive 2009/136 (‘the e-Privacy Directive’). In certain circumstances, location data can constitute personal data for the purposes of the Data Privacy Directive. However, under Article 2(c) of the e-Privacy Directive, ‘location data’ is also given the

specialised and technical definition: ‘any data processed in an electronic communications network or an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service’. ‘Location data’ for the purposes of the e-Privacy Directive is subject to a more onerous regime than personal data. Most notably, there are requirements for prior user consents, and an ability for a user to refuse processing.

There has been some confusion as to whether or not location data under the e-Privacy Directive includes information generated via GPS, or information sent over the internet. The Working Party appears to have taken the view that ‘location data’ merely refers to base station data generated by cell towers. In addition, it appears that the Working Party is of the view that the legal obligations only fall on the telecommunications companies, and not persons who use the location data further down the line. This position should come as a relief to users of location based data, as it limits their privacy obligations to those set out in the Data Protection Directive.

Wi-Fi data

In the Opinion, the Working Party, possibly influenced by recent issues concerning Google’s Street View service, takes a surprising, and perhaps somewhat heavy handed, approach to businesses that offer location based services using maps of Wi-Fi hot spots.

The Working Party is of the view that all information concerning hot-spots should be treated as personal data. This is the case notwithstanding the fact that, as the Working Party acknowledges, relating a given Wi-Fi router to an identifiable living person can be an exceptionally difficult, and occasionally impossible, task. One would have to analyse the strength of the signal until one identified the likely whereabouts of the router. One would then have to search public records, directories, etc., to try to determine the occupier of the premises containing the router — no small undertaking.

(Continued on page 8)

(Continued from page 7)

The Working Party does acknowledge that such a WiFi mapping service could be rolled out in reliance on the 'legitimate interest' justification for processing, in the Data Protection Directive.

It is difficult to see how having all information concerning hot-spots defined as personal data could operate in practice. In such a case, the data controller would be under quite heavy (and possibly insurmountable) obligations concerning the deletion of data. As noted above, relating a given WiFi signal and MAC address to an identifiable living individual involves a considerable amount of work. It is not clear how such a data controller, faced with a demand that they delete information they hold about a certain WiFi network, could verify that the person making the request is genuine, without requiring additional personal data, such as a proof of address.

Child monitoring devices

Perhaps controversially, the Working Party appears to take the view that the Data Protection Directive imposes limitations on the ability of parents to use geolocation technology to monitor the whereabouts of their children's phones. The Working Party notes that use of such applications is problematic and that "at the very least, if the parents judge that the use of such an application is justified in the circumstances, the children must be informed and, as soon as reasonably possible, allowed to participate in the decision to use such an application."

It is somewhat difficult to see how this use, which clearly falls within the 'household exemption', is governed by the Data Protection Directive in the first place.

Employee monitoring

In line with its previous Opinions, the Working Party has taken the view that employee 'consent' to monitoring should be treated with suspicion. This is due to the inequality of bargaining power between employers and their employees, and the consequent likelihood that any consent obtained as not been 'freely given'.

Consequently, employers ought to rely on their 'legitimate interests' as a justification for processing employee location data. Interestingly, the Working Party suggests that employers cannot use vehicle tracking devices to monitor the quality of their staff's driving.

Substantive obligations

The Opinion provides considerable guidance as to the steps that a data controller should take to properly process location data. However, it is noteworthy that the Opinion draws no distinction between location data that are personal data, and location data that are sensitive personal data (for example, one's location at a given place of worship). The position taken in the Opinion, particularly on the nature of consent, seems to go beyond the wording of the Data Protection Directive, and takes no account of the fact that consent to the processing of non-sensitive personal data can arguably be obtained implicitly (for example, through the very act of using a location based service).

The Working Party correctly stresses the importance of giving users proper information about the nature of the processing. Information must be provided which is "clear, comprehensive, understandable for broad non-technical audience and permanently and easily accessible." However, later in the Opinion, the Working Party takes the view that location based data can, as a general matter, only be processed on the foot of an express opt-in consent. This position is difficult to reconcile with the wording of the Data Protection Directive, which arguably allows for implied consent for the processing of non-sensitive personal data.

The Opinion also suggests that a user should be able to consent 'granularly' to various functions of the location based service. An overall 'take-it-or-leave-it' consent to the use of location based data by a given application appears to be insufficient.

Depending upon its implementation, this approach may cause difficulties for the developers of location based applications. If a user is able to opt-in to the use of location based data to enjoy the functionality of an application, but opt-out from the location based advertising that

supports that application, it is difficult to see how certain location based technologies could be economically viable.

Conclusion

It is no overstatement to say that the growth in the use of location based data represents one of the greatest privacy challenges ever faced, so the Opinion of the Article 29 Working Party is to be welcomed. Though certain positions taken by the Working Party may be controversial, it can only be positive to see regulators directly facing the new challenges created by technological innovation.

**Philip Nolan and
Oisín Tobin**

Mason Hayes + Curran
pnolan@mhc.ie
otobin@mhc.ie
