May 30, 2017

Article 29 Working Party has "grave concerns" about the proposed e-Privacy Regulation

Attorneys
Rohan Massey

The Article 29 Data Protection Working Party has adopted Opinion 01/2017 on the Proposed Regulation on Privacy and Electronic Communications. The draft Regulation was proposed by the European Commission in January 2017. In general, the Working Party welcomes the Commission's proposal. In particular, it likes the fact that the Commission has chosen a Regulation as the regulatory instrument, and it is in favour of extending the scope of the rules to cover all electronic communications providers, not just traditional telecoms providers. It also welcomes what it calls "the attempt" to modernise the rules applicable to tracking in the online world. However, the Working Party has four points of "grave concern" relating to: (i) "WiFi tracking"; (ii) analysis of content and metadata; (iii) tracking walls; and (iv) privacy by default regarding terminal equipment and software. In the Working Party's view, the proposed Regulation in its current form would lower the level of protection enjoyed under the new General Data Protection Regulation (2016/679/EU)("GDPR"), which will come into force in May 2018, in these areas. Accordingly, the Opinion sets out specific suggestions to ensure that the e-Privacy Regulation will guarantee the same, or a higher, level of protection appropriate to the sensitive nature of communications data (both content and metadata). It also includes various points on which the Working Party says it would appreciate clarification.

Points of grave concern

There are four issues about which the Working Party is "highly concerned". These are provisions that the Working Party says "undermine the level of protection accorded by the GDPR" and are set out below.

Tracking terminal equipment ("WiFi tracking")

These provisions should, the Working Party says, comply with the GDPR and require consent. However, Article 8(2)(b) of the proposed Regulation gives the impression that organisations can collect information from terminal equipment to track the physical movements of individuals (i.e. "WiFi-tracking" or "Bluetooth-tracking") without the consent of the individual concerned. Under the current proposal, it appears that it is sufficient for the party collecting the data to comply by simply telling users to switch off their devices when they do not want to be tracked. In the Working Party's view, such an approach would be "contrary to a basic goal of the telecommunications policy of the European Commission to provide high-speed mobile internet connectivity with strong privacy protections at a low cost to all Europeans, across borders".

In addition, the Working Party says, the proposed Regulation does not impose any clear limitations with regard to the scope of the data collection or subsequent processing. The level of protection of personal data is therefore "significantly lower than under the GDPR", under which such tracking would need to be fair and lawful, as well as transparent.

The Working Party says that that simply providing an individual opt-out in respect of each organisation that collects such data would pose "an unacceptable burden on citizens", given the increase in the deployment of such tracking technologies by both private and public sector organisations.

Therefore, the Working Party calls on the Commission to "promote the development of technical standards for devices to automatically signal an objection against such tracking and to ensure that adherence to such a signal is enforceable".

Analysis of content and metadata

Article 6 of the proposed Regulation provides for different levels of protection for metadata and content. The Working Party says that it does not support this difference, as both categories of data are highly sensitive and should be accorded the same high level of protection. The starting point should thus be that it is prohibited to process metadata as well as content without the consent of all end users (i.e. sender and recipient).

However, in the Working Party's view, certain processing should be allowed without consent if it is "strictly necessary" for certain purposes, including:

i. spam detection/filtering and botnet mitigation techniques for the detection and termination of abusive use of electronic communications services;

ii. analysis of communications data for customer service purposes, such as billing; and

iii. providing services explicitly requested by an end user, such as search or keyword indexing functionality, virtual assistants, text-to-speech engines and translation services.

This means, the Working Party says, that the analysis of content and/or metadata for all other purposes, such as analytics, profiling, behavioural advertising or other purposes for the (commercial) benefit of the provider, should require consent from all end users. However, and unhelpfully, no explanation is given as to how such consent can practically and effectively be obtained.

Finally, the Working Party says it should be clarified that the processing of data of people other than end users (e.g. the picture or description of a third person in an exchange between two people) also needs to comply with all relevant provisions of the GDPR.

Tracking walls

"Tracking walls" is the practice whereby access to a website or service is denied unless individuals agree to be tracked on other websites or services. The Working Party says that the practice should be explicitly prohibited by the Regulation, as such processing can "seriously intrude upon the privacy of these users". An individual's ability to access content online should not be dependent on acceptance of the tracking of activities across devices and websites/apps. The Regulation should therefore specify that access to such content may not be made conditional on the acceptance of intrusive processing activities, regardless of the tracking technology applied, whether it be cookies, device fingerprinting, injection of unique identifiers or other monitoring technique.

Privacy by default for terminal equipment and software

Though the proposed Regulation obliges the providers of electronic communications software to give consumers the option of choosing to prevent a limited form of interference with terminal equipment and, upon installation, obliges providers to require consent from end users, "such a choice does not equal privacy by default". The Working Party notes that providing such a choice already currently exists, but that to date it has not resulted in addressing the problem of unwarranted tracking. This is exactly why, it says, under the GDPR, a conscious policy choice was made to introduce the principles of data protection and privacy by design and by default. In the Working Party's view, the proposed Regulation undermines these principles.

In the Working Party's view, terminal equipment and software must by default offer privacy protective settings and guide users through configuration menus allowing them to deviate from such default settings upon installation if they so wish.

Other points of concern

The Opinion also identifies areas of concern in relation to territory and scope. With regard to scope the Working Party is concerned that the term "metadata" is too narrowly defined. As currently drafted, the term could be interpreted to mean that data generated in the course of the provision of an OTT-service would be excluded. On territorial scope, the regulation should include providers of publicly available directories, software providers permitting electronic communications and persons sending direct marketing commercial communications or collecting information related to or stored in end-users' terminal equipment, whenever their activities are targeted at users in the EU, irrespective of the provider's geographic establishment.

The Opinion also comments on a number of other issues, including direct marketing, the use of non-specific browser settings to obtain consent, which the Working Party does not agree with, and issues around the meaning of "web audience measurement" and exceptions on consent requirements.

Comment

Recital 5 of the proposed Regulation specifically states that the Regulation does not lower the level of protection enjoyed under the GDPR. The intention is therefore clear, but the Working Party does not agree that it has been achieved, as its four points of "grave concern" make clear. The points that are particularly worrying are the tracking of devices and the missing principle of privacy by default, the Working Party says. It suggests that, as a minimum, the text of the proposed Regulation should clarify that:

i. the prohibitions under the e-Privacy Regulation take precedence over permissions under the GDPR;

ii. when processing is allowed under any exception (including consent) to the prohibitions under the e-Privacy Regulation, where such processing concerns personal data, it must comply with all relevant provisions in the GDPR;

iii. when processing is allowed under any exception to the prohibitions contained in the e-Privacy Regulation, any other processing on the basis of the GDPR is prohibited. This would not prevent controllers from asking for additional consent for new processing operations, and neither would it prevent legislators from providing additional, limited and specific exceptions in the e-Privacy Regulation to allow processing for scientific or statistical purposes or to protect the "vital interests" of individuals under the GDPR.

Overall, the Working Party says, the e-Privacy Regulation should be "interpreted in such a way as to ensure that it affords at least the same and where appropriate higher level of protection as under the GDPR". This is typical Working Party, taking a robust privacy approach without balancing commercial interests. Direct marketers, for example, must look elsewhere for support for their calls to relax the Commission's proposal to restrict the soft opt-in to customer's contact details obtained as a result of a sale, as opposed to sale or negotiation for a sale. Similarly, concerns remain over browser consents for cookies; rather than simplifying the consent process, this potentially complicates matters by luring consumers into a "default to reject" mind-set.

It would appear, therefore, that there is still a fair amount of work to be done on the e-Privacy Regulation. The Commission's idea is that the new e-Privacy Regulation will take effect at the same time as the GDPR, i.e. in May 2018. As well as any amendments made further to the Working Party's Opinion, however, the text will also have to be approved by both the European Parliament and the Council before that can happen. The Commission has called on these institutions to "work swiftly" to ensure the Regulation is ready by May 2018, but it may well have to go

through its own amendment process first. The intention is to provide citizens and businesses with "a fully-fledged and complete legal framework for privacy and data protection in Europe by [May 2018]". The legislature certainly has its work cut out.