The future under the e-Privacy Directive

Yuli Takatsuki, Director at Fieldfisher (Silicon Valley), ***explores the key reforms on the horizon under the e-Privacy Directive and what this means for the future of the electronic communications sector***

As part of its development of the Digital Single Market Strategy and the adoption of the General Data Protection Regulation ('GDPR'), the European Commission is undertaking a review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ('the e-Privacy Directive'). As many readers will know, the e-Privacy Directive currently provides a patchwork of different EU rules, primarily directed at telephony and internet access providers, relating to confidentiality of communications, direct marketing, processing of traffic data, location data, and the controversial 'cookie consent rule'.

The review seeks to modernise and update the e-Privacy Directive 'to make sure it is up to date with the new challenges of the digital era' and to ensure consistency with the GDPR. The Commission opened its consultation on the e-Privacy Directive between April and July 2016. The consultation gathered a total of 421 replies from stakeholders inside and outside the EU. The largest number of responses came from Germany (25.9%) and the UK (14.3%).

The responses were, predictably, highly polarised. Responses from citizens, civil society organisations and public authorities argued for the privacy rules for the electronic communications sector to be further reinforced and strengthened. Respondents from industry, on the other hand, were generally against the extension of the current rules. The summary report of the public consultation is now available on the Commission's website and a full in-depth analysis is due to be published in the Autumn.

In this article, we focus on the key recommendations of the Article 29 Working Party, which published its Opinion on the e-Privacy Directive on 19th July 2016. The Opinion provides valuable insight into how European DPAs are likely to interpret and apply the existing e-Privacy Directive rules and although the Opinion is non-binding, will no doubt be highly influential in shaping the Commission's final analysis.

The main recommendations of the Working Party are categorised into the headings below.

Scope extension

One of the key concerns about the current framework is that its application is mostly limited to traditional electronic communications services, such as ISPs and telcos. Its most privacy protective provisions do not apply, for example, to internet telephony (VoIP), email or instant messaging providers. This partly stems from the fact that the e-Privacy Directive was last updated in 2009.

In the past few years, dramatic changes have taken place in the electronic communications sphere with the proliferation of internet-based communications services. From the perspective of users, there is 'functional equivalence' between all these types of communications services. In other words, it makes no difference to them whether they communicate through traditional telephone networks, VoIP or messaging apps. Private communications ought to remain private, whatever the method of transmission.

To address this, the Working Party recommends that the e-Privacy rules should apply equally to new players in the communications market, such as virtual network operators, unmanaged VoIP, instant messaging, webmail and messaging in social networks. The specific recommendation (on page 6) is to extend the scope to all services 'which allow individual communication' and 'where service providers take the functional position of neutral carriers of the communication'. This would quite likely bring services like Whatsapp, Gmail, LINE, Skype and Facebook Messenger within its scope.

In terms of whether any type of communications networks would be exempt from the regime, the Working Party states that only the following should be exempt:

- those occurring in an official or employment situation solely for work-related or official purposes;
- technical communications solely in order to control work or business processes; and
- use of services for exclusively domestic purposes.

(Continued on page 4)

(Continued from page 3)

Confidentiality

Article 5(1) of the current e-Privacy Directive provides a general prohibition on the interception, surveillance and monitoring of the content of electronic communications. It is proposed that in future, this will be extended to all the types of electronic communications service providers referred to above.

The Working Party is of the view that the processing of content and related traffic data should almost always require prior consent. It acknowledged, however, that there are legitimate uses of such data which the current Directive does not expressly call out, and for which there should be clearer exemptions.

In addition to the consent exemption, the Working Party suggests introducing two further exemptions: firstly, 'transmission' — if the data are strictly necessary for the transmission of the electronic communication requested by a user; and secondly, 'security' — if the processing is strictly necessary to proactively and defensively maintain and manage the security of a network or service.

The latter security exemption would be a welcome addition for industry, as it would provide greater clarity on the legitimacy of certain technologies, like spam/fraud detectors. Until now, it has not been clear whether services that automatically scan or monitor the content of communications to detect spam or fraud are technically legal, and regulators have taken varying approaches to this in different jurisdictions.

"The proposed rules relating to the legitimate use of content, traffic and location data, seem at first glance to cut across the broader rules of the GDPR that govern the processing of personal data on other grounds, and the proposed rules relating to the processing of cookie data may cut across GDPR rules on profiling."

The Working Party also invited the Commission to consider other circumstances in which consent would not be required because the processing would have little or no impact on the privacy rights of users. Such circumstances include where the data are immediately anonymised during collection, or where data collection is strictly limited to statistical analysis of the quality of the delivered service.

Nevertheless, the Working Party made it clear that the use of content or related traffic data for the purposes of advertising, marketing, research and/or audience measurement should never be allowed to override the prior consent requirement.

Cookie consent rules

The Working Party recommends broadening the cookie consent rules so that they are technologically neutral and capture all tracking techniques used on smartphones and Internet of Things apps. It believes that the rules should not depend on the type of device or object owned by the user, or on the technology deployed by the organisation. However, whilst clarifying the broad scope of the consent requirement, it stated that the Commission should also create more specific exceptions — for example, to allow for the processing of data that causes little or no impact on the privacy rights of users.

Merging of traffic and location data

The Working Party considers that, over the years, the boundary between traffic and location data has become blurred. Such data have the potential to reveal highly intrusive details about a person's private life, including home addresses, work addresses, social patterns and relations between users. They may even reveal sensitive personal data (for example, website traffic data may reveal a person's sexual orientation or political affiliations). The Working Party therefore recommends that the separate provisions on traffic and location data in the e-Privacy Directive should be merged, and there should be a harmonised set of rules for the processing of all 'metadata' — though it is not clear what this definition would encompass.

As with content data, the primary requirement for the processing of such metadata should be based on consent. However, there should also be similar exceptions based on transmission and security, and also where the processing of metadata is strictly necessary for billing purposes.

Strengthening 'consent'

The Working Party further recommends that the new e-Privacy rules should specifically prohibit 'take it or leave it' approaches to consent that do not give users real choice regarding the processing of their data. For example, it refers to so called 'cookie walls' — websites which deny access to users that do not accept cookies.

It further recommends that the onus for cookie compliance should not only rest with publishers. Manufacturers of browsers and other software or operating systems should develop and offer control tools (such as Do Not Track) within the browser that empowers users to effectively express and withdraw their consent.

Data breach rules

The Working Party recommends deleting the rules for telcos and ISPs relating to the notification of data breaches, as this overlaps with obliga-

(Continued from page 4)

tions under the GDPR. All personal data breaches should be governed under the GDPR only to avoid confusion and duplication.

Unsolicited marketing

The Working Party recommends that the rules relating to unsolicited marketing should be updated to require prior consent for all types of unsolicited communications, independent of the means (e.g. email, behavioural advertising, calls, fax, text and direct messaging). It should be as easy to withdraw consent as it is to give it, and users must be able to revoke consent free of charge via simple means that have to be indicated in each subsequent communication.

The categories of products for which marketing may be sent and the categories of recipients should be clearly defined before obtaining the consent. Although such requirements can clearly work for most forms of direct marketing, it is not so clear how such rules can apply easily to behavioural advertising.

The Working Party further states that where possible, users should be given the ability to express and revoke consent across a range of organisations or particular sectors, and to provide an easy one-stop mechanism for withdrawing consent from third party marketing where marketing lists have been sold onto large numbers of unknown third parties.

Caller ID

The Working Party recommends that the integrity of call line identification (CLI) transmitted between interconnecting networks should be maintained (such that a user's request to display or withhold CLI is maintained) and to ensure that it cannot be spoofed or falsified.

Enforcement

The Working Party believes that to ensure consistent and coordinated regulation and enforcement across the board, national data protection authorities should be the competent authorities with regard to the new e-Privacy rules. It also recommends that sanctions should be harmonised to match with those provided in the GDPR.

What does this mean for the future?

The Working Party's Opinion proposes a vast suite of reforms under the e-Privacy Directive, some of which will have significant ramifications for electronic communications providers. The broadening of the scope of the e-Privacy Directive to include all types of communications service providers will mean that many online social networks, webmail services and messaging apps will need to review very closely how they currently use communications metadata, such as traffic and location data. For example, they will need to ensure that clear user consent mechanisms are in place when using any such data to carry out activities like targeted advertising, marketing or analytics.

Further, although one of the key objectives of the review is to prevent any overlap or duplication with the rules of the GDPR, it is not clear whether the proposed reforms will achieve this. For example, the proposed rules relating to the legitimate use of content, traffic and location data, seem at first glance to cut across the broader rules of the GDPR that govern the processing of personal data on other grounds, and the proposed rules relating to the processing of cookie data may cut across GDPR rules on profiling.

Equally, however, the recommendations will provide greater privacy protection and comfort to users that their communications will remain confidential, regardless of the technology or the platform that is used to transmit them. This is no doubt a welcome advancement and, by treating all such communications carriers in the same way, the new rules will hopefully provide a simpler and more modern legal framework for the electronic communications sector and for EU citizens than that which currently exists.

Yuli Takatsuki
Fieldfisher (Silicon Valley)
yuli.takatsuki@fieldfisher.com