Privacy Law Watch™

August 07, 2017

Bloomberg BNA

Telecommunications

European Parliament LIBE Committee Joins Chorus of Disapproval Over Aspects of the Proposed ePrivacy Regulation

ePrivacy Regulation

The e-Privacy Regulation proposed by the European Commission would expand privacy protections to all electronic communications providers, but the European Parliament committee reviewing the draft concluded it would provide weaker protections than the forthcoming new EU General Data Protection Regulation, meaning a busy summer of negotiation and clarification may be needed, the author writes.

By Rohan Massey

Rohan Massey is a partner at Ropes & Gray LLP in London and leads the firm's privacy and data security practice in Europe.

By Rohan Massey

The European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) has published a “Draft report on the European Commission's proposed new Regulation on Privacy and Electronic Communications,” which would repeal the current e-Privacy Directive (2002/58/EC). Essentially, the draft report finds that, although the new e-Privacy Regulation is not supposed to lower the level of protection afforded by the new General Data Protection Regulation (2016/679/EU), which comes into effect in May 2018, it does in fact, in some areas, do precisely that. This was also the finding of the Article 29 Data Protection Working Party (WP29), which expressed “grave concerns” that the Commission's proposals will undermine the level of protection accorded by the GDPR in its Opinion 01/2017, and the European Data Protection Supervisor. Accordingly, the report finds that the proposed text needs to be amended in order to ensure that it will deliver a high level of protection corresponding at least to that offered by the GDPR.

Some 800 amendments to the e-Privacy regulation have been offered.

Background

The Commission published the official version of the proposed e-Privacy Regulation in January 2017, saying that the primary aim of the new rules was to extend their scope to all electronic communications providers, not just traditional telecoms providers. The Regulation also aimed “to create new possibilities to process communication data and reinforce trust and security in the Digital Single Market.” At the same time, the proposal's goal was to align the rules for electronic communications with the new GDPR. The idea is that the new e-Privacy Regulation will come into effect at the same time and the Commission has called on the European Parliament and Council to “work swiftly” to ensure the Regulation is ready by May 2018. However, the proposal has already received criticism from various quarters, including the WP29 and the Euroepan Data Protection Supervisor (EDPS). LIBE now adds its voice to the chorus.

The Draft Report

The report notes that the proposed e-Privacy Regulation together with the GDPR seek to establish a data protection framework that takes account of the important technological and economic developments in the electronic communication sector since the adoption of the e-Privacy Directive in 2002. Nowadays, new communications services (Over-The-Top (OTT) providers), as well as machine-to-machine communications and the "internet of things" (IoT) coexist in parallel with traditional communication services. These new technologies present various challenges in terms of protecting people's privacy and personal data. The new proposal takes all this into account, as well as what the draft report calls the "experience gathered over the years" in relation to cookies and other tracking tools, which seriously affect people's private lives and the confidentiality of their communications. The new proposal also takes stock of the recent case law of the Court of Justice of the European Union.

Relationship With the GDPR

The report notes that, as with the e-Privacy Directive and the Data Protection Directive (95/46/EC), the proposed e-Privacy Regulation is supposed to particularise and complement the GDPR.

The rules of the proposed e-Privacy Regulation should not, therefore, lower the level of protection afforded by the GDPR. However, the report notes, the opinions of both the WP29 and the EDPS, as well as numerous academics and stakeholders consulted in the preparation of the report, conclude that several provisions of the Commission's proposal "would actually lower the level of protection currently afforded by Union law."

The report notes that communications data (both content and metadata) are "extremely sensitive" as they can reveal sensitive aspects of the private life of individuals (sexual orientation, philosophical or political beliefs, freedom of expression and information, financial situation, health condition etc). Therefore, the report says, "they deserve a high level of protection." In order not to lower the high level of protection ensured by the GDPR, the proposal "needs to be amended in order to ensure that it will deliver a high level of protection corresponding at least to that offered by the GDPR."

The Scope of the Proposed Regulation

The report supports the Commission's proposal of extending the scope of the new Regulation to cover new forms of electronic communications, such as OTT services, the IoT and machine-to-machine communications.

However, the proposal should, the report says, apply not only to the use of electronic communications services and to information related to and processed by the terminal equipment of end-users, as well as to the software allowing such electronic communications, but also to the sending of direct marketing commercial communications and the collection of information related to or stored in end users' terminal equipment by third parties.

The Regulation should also be a standalone instrument that contains all relevant provisions and is not dependent on the Electronic Communications Code (ECC).

The report would like to see a definition of "user," inspired by the current e-Privacy Directive, included in order to protect the rights of the individual using a publicly available electronic communications service, but who is not necessarily a subscriber. Accordingly, it recommends the following definition: "'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service."

The report has also included a definition of "end-user" as follows: "'end-user' means a legal entity or a natural person using or requesting a publicly available electronic communications service", to ensure that it applies to companies (legal entities) as well as people.

In addition, the report recommends amending the definition of "electronic communications metadata" to clarify these concepts.

Confidentiality of Communications (Articles 5–7)

The draft report notes that, nowadays, electronic communications data is stored by service providers long after receipt. The report therefore recommends clarifying that the confidentiality of any user-related communication is ensured, even when the data is simply being stored by the service provider in the cloud or in the IoT environment.

Further, the report says, since the right to confidentiality of communications is a fundamental right recognised by the Charter of Fundamental Rights, any interference with it must be limited to what is strictly necessary and proportionate in a democratic society. Accordingly, the report proposes various amendments to Article 6, tightening up the conditions under which lawful interference with the right of confidentiality of communications is allowed so that it is only permissible where it is "technically

strictly necessary."

Protection of Information Stored in and Related to Users' Terminal Equipment (Articles 8–10)

The report welcomes the proposal to protect information stored in the user's terminal equipment from access and to prevent the installation of software or information without the user's consent (Article 8).

However, the report says that the proposed regime does not ensure as high a level of protection as that afforded by the GDPR. Since information processed or stored in terminal equipment or processed during connection to another device or network equipment (e.g. free Wi-Fi, hotspots) can reveal sensitive personal data, the processing of that information is subject to very strict conditions under the GDPR. The report therefore proposes various amendments to ensure consistency with the GDPR.

For example, Article 8(1)(a) provides that the use of processing and storage capabilities of terminal equipment and the collection of information from users' terminal equipment is prohibited except where it is "necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network." The report recommends that the exception should apply only where it is "technically strictly necessary".

Article 8(1)(b) provides for an exception to the prohibition where the user has given his or her consent. The report wants to see the phrase "which shall not be mandatory to access the service" to ensure that providers do not deny access if a user does not consent to the provider collecting information from the user's terminal equipment.

The report in fact suggests going one step further by including the following new provision:

"no user shall be denied access to any information society service or functionality, regardless of whether this service is remunerated or not, on grounds that he or she has not given his or her consent under Article 8(1)(b) to the processing of personal information and/or the use of storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality."

Further, the amendments ensure that any use of analytics tools for web audience measuring is clearly defined to take account of the actual techniques used and to ensure that this information is used exclusively for this purpose.

The report also recommends including an exception for the provision of a security update, but only if: (i) security updates are "discreetly packaged" and do not change the user's privacy settings; (ii) the user is informed in advance each time an update is being installed; and (iii) the user can turn off the automatic installation of the updates.

The report also recommends the addition of an exception for employment relationships, where: (i) the employer provides certain equipment; (ii) the employee is the user of this equipment; and (iii) the interference is strictly necessary for the functioning of the equipment by the employee.

Article 8(2) is also amended to ensure that tracking the location of terminal equipment through Wi-Fi or Bluetooth is brought into line with the GDPR. Therefore, the user must have been informed and given consent or the data must be anonymised and "the risks adequately mitigated." In order to mitigate the risks, the report suggests including the following: "(a) the purpose of the data collection from the terminal equipment shall be restricted to mere statistical counting; and (b) the tracking shall be limited in time and space to the extent strictly necessary for this purpose; and (c) the data shall be deleted or anonymised immediately after the purpose is fulfilled; and (d) the users shall be given effective opt-out possibilities."

Article 10 of the proposal refers to options for providing privacy settings and Do-Not-Track software (DNTs) to enable users to prevent other parties from storing information on their terminal equipment, or processing information stored on the equipment.

The report shares the objective of the proposal, but considers that, in order to reflect the essential core principles of data protection law (privacy by design and by default), DNTs should be technologically neutral to cover different kinds of technical equipment and software. Further DNTs must, by default, configure their settings in a manner that prevents other parties from storing information on the terminal equipment or processing information stored on the equipment without the consent of the user. At the same time, users should be able to change or confirm their default privacy settings at any time. The DNTs should also send signals to third parties informing them of the user's privacy settings, and compliance with these settings should be legally binding and enforceable against all other parties.

Call Identification, Directories of Subscribers and Direct Marketing (Articles 12–16)

The report says that it “broadly supports” the provisions relating to call identification, incoming call blocking and publicly available directories.
As for unsolicited communications for direct marketing purposes (Article 16), the report recommends including the following:

“Unsolicited marketing communications shall be clearly recognisable as such and shall indicate the identity of the legal or natural person transmitting the communication or on behalf of whom the communication is transmitted. Such communications shall provide the necessary information for recipients to exercise their right to refuse further written or oral marketing messages.”

The idea is to clarify the scope of the provision to cover the different techniques used for direct marketing. The report wishes to make it clear that the use of direct marketing should only be allowed in relation to natural or legal persons who have given their prior consent. Further, withdrawing consent or objecting to direct marketing communications should be possible at any time and be free of charge for the user. Overall, the report's amendments are aimed at strengthening the safeguards for individuals.

Supervisory Authorities

The report agrees with the Commission's proposal that the independent supervisory authorities for ensuring compliance with the Regulation should be the data protection authorities in charge of the supervision of the GDPR. Since the Regulation complements and particularises the GDPR, entrusting supervision and enforcement to the same independent authorities will ensure consistency.

Comment

The upshot is that there is potentially much work to be done before the Regulation can be finalised. The WP29, the EDPS and now LIBE have found fault with the Regulation, which has to be approved by both Parliament and the Council before it can come into force. The Commission's intention was to provide citizens and businesses with “a fully-fledged and complete legal framework for privacy and data protection in Europe by [25 May 2018]”. The report has not ruled out the possibility of achieving this by May next year, as indicated by the author's comments at the end that she “expects her proposals to form a good basis for swift agreement in the European Parliament and negotiations with the Council in order to ensure that the legal framework is in place by 25 May 2018,” but it looks like a busy summer of negotiation and clarification lies ahead.

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com