e-Privacy Regulation: Good Intentions but a Lot of Work to Do

Diego Naranjo*


EU legislation on data protection is divided between general legislation - the 1995 Directive, soon to be replaced by the General Data Protection Regulation (GDPR) - and legislation specifically covering privacy in the communications sector, the e-Privacy Directive.

The ePD has two functions. Firstly, it provides additional clarity and predictability to allow the principles in the general legislation to be implemented in the complex environment of communications. Thus, as the ePD stated in its Article 1.2, one of the objectives was to ’particularise and complement’ the Data Protection Directive.¹ Secondly, it serves as the EU legislative instrument to give meaning to the fundamental right to freedom of communications.

The proposed draft Regulation contains a number of provisions which, if adopted and effectively implemented, should address some of the current gaps or lack of clarity in protection of the confidentiality of electronic communications and information stored on users devices. The process of consultation and polls have shown that citizens are concerned about their privacy and about how companies make use of their personal information online. Although the Commission has rightly identified and addressed most of the key issues and objectives in the proposal, such as online tracking and broadening the scope of Over-the-top content (OTT), strong forces seem to have watered down the text considerably compared to the earlier version that was leaked in December 2016. For example, the reference to ‘privacy by design and by default’ that was changed in Article 10 will need to be put back in order not to lower down the protections to the current ‘privacy by option’, options on the degree of online privacy that the browser would offer to the user.²

* Diego Naranjo, Senior Policy Advisor at European Digital Rights (EDRi). For correspondence: <diego.naranjo@edri.org>.

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

² art 10 of the ePR proposal states: ‘Information and options for privacy settings to be provided
1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment.
2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.’
Among the improvements needed, the European Parliament will need to make sure that the definitions of the text (cross-referenced to the European Electronic Communications Code, EECC, which is still being discussed) do not lead to a reduced scope of the e-Privacy Regulation. Furthermore, the scope of these definitions in the ePR relates to electronic communication networks, while in the leaked version it also referred to electronic communication services. This is a significant reduction in the scope of the proposed ePR. In addition to this, the mentions to ‘strictly necessary’ that appear repeatedly in the GDPR need to be applied to the relevant sections of the ePR. There are also doubts, such as the impact of recital 21 (in fine) of the ePR on ad-blockers detection.\(^3\)

Regarding the substance of the proposal, one of the key issues, the processing of content (‘what we talk about’) and metadata (‘when and with whom we communicate’), raise some concerns: both the content and the metadata, which can sometimes be more sensitive than content of our online interactions, could be used for additional purposes by, for example, our email providers, if the user has ‘consented’ to this.\(^4\) The way this consent is obtained in practice will need to be carefully addressed. If the legislator cannot avoid that, in practice, the consent is considered valid if done for example under over-broad Terms and Conditions, or through pre-ticked boxes, the e-Privacy Regulation would be going below the standards needed to effectively protect our communications.

The section on access to devices is probably the one that has drawn the most attention to the proposal, since it regulates the use of tracking technologies such as tracking cookies. The text establishes that terminal equipment of end-users (smartphones, laptops but also, arguably, an e-fitness device or any other device that is part of what we call the ‘Internet of Things’) are part of the individual’s private sphere. Access to these devices and to any information stored in or emitted by such equipment would be under the scope of the ePR. However, here too, ‘consent’ is the key that could give access to our personal devices, with the same risks commented above. Another worrying section is the one in Article 8.2 on Protection of information stored in and related to end-users’ terminal equipment. While online tracking is limited and allowed only under certain conditions in the ePR, the European Commission has decided that offline tracking seems to be acceptable and it requires only that a ‘a clear and prominent notice’ is placed saying that your movements, such as your shopping habits when you’re connected to the wifi network in a shopping mall, will be tracked.\(^5\) Finally, the

---

\(^3\) ‘(...) Information society providers that engage in configuration checking to provide the service in compliance with the end-user’s settings and the mere logging of the fact that the end-user’s device is unable to receive content requested by the end-user should not constitute access to such a device or use of the device processing capabilities.’

\(^4\) It needs to be noted that, depending on who is the end-user (the buyer or the user of the product) we could be giving employers the right to consent to data processing.

\(^5\) art 8: Protection of information stored in and related to end-users’ terminal equipment:

‘(...) 2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:
(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or
(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure’
exceptions for Member States to restrict the same protections that the Regulation is trying to provide is one of the most worrying parts of the text, along with the unexpected absence of reference to collective redress (Article 80 of the GDPR) in the article on remedies (Article 21). 6

Citizens have expressed repeatedly the need for strong protections for privacy and confidentiality of communications. However, there seems to be a lot of work ahead7 to complement and particularise the text presented by the Commission.

---

6 art 21: ‘Remedies: 1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679.’