EDRi

QUICK GUIDE

on the proposal of an e-Privacy Regulation

European Digital Rights | 20 Rue Belliard, 1040 Bruxelles, Belgium | Tel. +32 2 274 25 70 | www.edri.org

On 10 January 2017, the European Commission published its proposal for a draft e-Privacy regulation (Regulation on Privacy and Electronic Communications, "ePR") to replace the 2002 e-Privacy directive (Directive 2002/58/EC, "ePD").

This paper is a brief introduction to the main topics covered in the proposal and the key issues that need to be addressed during the reform.

If you are not yet familiar with e-Privacy, we recommend you to first visit our FAQ website.

Contents

Introduction

WHY DO WE NEED THIS INSTRUMENT?

The ePR will protect confidentiality of communications and personal data in the electronic communication sector by complementing matters covered in a general way by the General Data Protection Regulation (GDPR). The ePR will also cover confidentiality of communications as this is something not specifically covered by the GDPR.

Lack of precise rules makes it more difficult for companies to develop new and innovative services. The huge economic cost of not legislating (and the competitive advantages that can be generated by good legislation) can be seen in the US government study last year, which showed that 30% of US consumers had, in the previous 12 months, refrained from certain online activities due to privacy and security fears. The Eurobarometer shows similar views in Europe.

ISN'T THE GENERAL DATA PROTECTION REGULATION (GDPR) ENOUGH?

The e-Privacy Directive was originally proposed to provide greater specificity to the general Data Protection Directive, as well as secondary law protection for confidentiality of communications. The new ePR serves the same function. Although the GDPR covers data protection on a general level, the ePR will give additional predictability in the complex area of electronic communication and will provide rules on the right to privacy and confidentiality of communications and, in particular, the right to freedom of communication, which are two distinct fundamental rights.

Key points of the e-Privacy Regulation proposal

THE OBJECTIVES OF THE REGULATION?

The European Commission has established the following key priorities for the reform contained in its draft ePR:

1. Extending the application of e-Privacy legislation to so-called Over The Top Services (OTTs) such as Skype or Whatsapp.
2. Guaranteeing the privacy of both content and metadata on electronic communication.
3. Facilitating telecoms operators to engage in economic operations with personal data obtained from communications data (using metadata, big data, Internet of Things...), on the basis of specific consent.
4. Simplifying the rules on cookies.
5. Protecting against spam, including calls.
6. Ensuring that enforcement is strong and effective.

What does the text of the e-Privacy Regulation cover? (Article 3, Recitals 9-13)

The regulation would apply to the provision of electronic communication services to end-users in the EU, to the use of these services and to the protection of information related to terminal equipment of end-users in the EU. These end-users may be natural persons or legal persons, as Recital 3 clarifies.

The proposal would extend the protection of confidentiality of electronic communication to "over-the-top" providers (Voice over IP, messaging services, web-based email services, and interpersonal communications services (ICS) that are "ancillary to another service", Recital 11.)

In a very welcome and timely development, the draft proposal clarifies that protection of confidentiality applies also to the Internet of Things.

Finally, the proposal recognises that public internet access via wireless networks requires measures to protect confidentiality of electronic communication taking place through such networks (Recital 13).

What are "electronic communication data"? (Article 4, Recital 14)

The proposal notes that electronic communication data should be defined broadly and in technological neutral way (Recital 14). However, many key definitions contained in the draft regulation refer to the definitions in the yet to be adopted European Electronic Communications Code (see image on page 3).

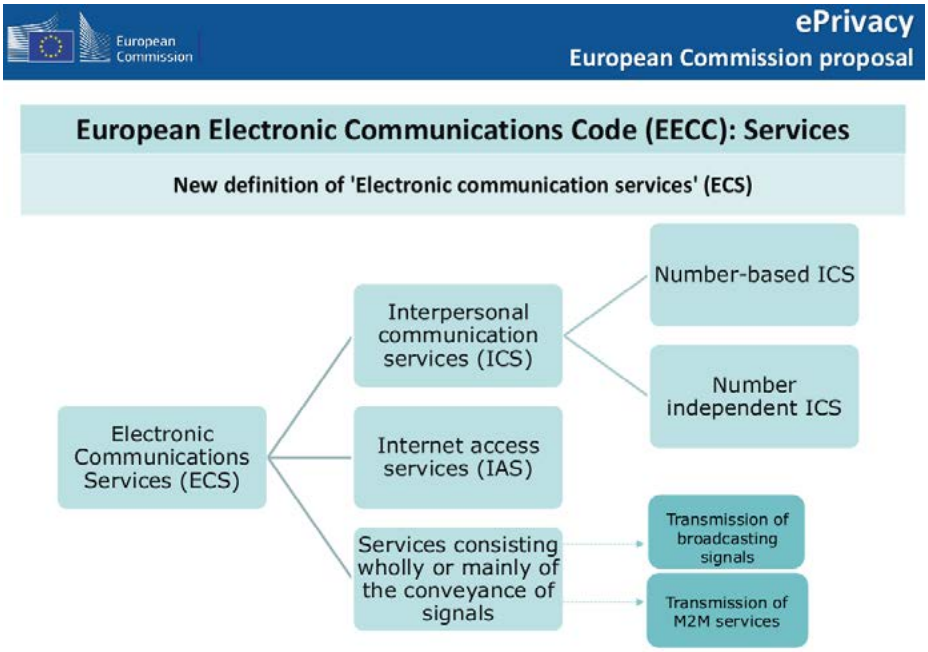
The draft regulation defines 'electronic communications content' as "content exchanged by means of electronic communication services, such as text, voice, videos, images, and sound." (Article 4.3b)

Article 4.3c contains an extensive definition of 'electronic communication metadata' but there is no reference to terminal equipment data which was contained in the definition in the leaked December version. (The omitted sentence read: *"It [electronic communications metadata] includes data broadcasted or emitted by the terminal equipment to identify end-users' communications and/or terminal equipment in the network and enable it to connect to such network or to another device."*) This creates unwanted ambiguity.

CONFIDENTIALITY OF COMMUNICATIONS: CONTENT, METADATA, TRACKING

Protection of confidentiality of electronic communication data (Article 5, Recital 15)

The draft e-Privacy Regulation states that "electronic communication data shall be confidential" (Article 5) and protected against unlawful interception or processing. This applies both to interference carried out by individuals and through automated processing by machines (Recital 15).



To what extent can my communications data, including the contents of my communications be used ("processed") by others? (Article 6.1)

In principle, this may only be done if necessary for the transmission of the communications or to maintain/restore the security of the networks and services or detect faults. Compared to the current ePD, Article 6.1b and recital 16 increase the scope for processing and storing metadata for security and quality of service (QoS) purposes.

And what about information about who I communicate with or which websites I visit (my metadata)? (Article 6.2)

This information can be processed for a limited number of purposes, including maintaining the security of the networks or for billing purposes or to detect fraudulent use of the service. This data may also be processed for other purposes, on the basis of consent by the user. However, it will be needed to avoid invalid forms of consent that are not permitted by the GDPR, for example, under over-broad terms and conditions, or through pre-ticked boxes.

When can the content of communications be used by (some) third parties? (Article 6.3)

The content of communications can only be used ("processed") if the user "consents" to it. Again, we feel that the quality of this "consent" needs to be carefully checked, specifically as to whether, in the challenging context of the digital environment, the user is offered a genuine, free and fully informed choice. Furthermore, consent should be required for all communicating parties in the communication, except for narrowly defined IT-security purposes of protecting the recipient against computer viruses and clearly unsolicited messages (spam). Regarding safeguards, Recitals 18-19 have important restrictions which need to be put in the article. In any case, the use of consent for the processing of the content of communications should be for exhaustively listed purposes that the legislature considers legitimate, that do not interfere with the right to private communications and that clearly benefit individuals and without being in the detriment of their communications with their contacts.

Will my data be deleted or anonymised? (Article 7)

The draft regulation requires the erasure or anonymisation of electronic communication content and metadata. However, erasure is not required if the metadata is processed for billing of the end-user, network security and QoS purposes as well as services to which the end-user has given his or her consent. Free consent (rather than a de facto obligation) in order to be able to use, or continue to use a service would not, for example, be free consent. Finally, the increased scope for storing metadata could lead to voluntary data retention by providers of electronic communication services.

MY DEVICE IS MY CASTLE: ACCESS TO TERMINAL EQUIPMENT AND DEVICES (COOKIES AND OTHER TRACKING METHODS)

Regulating access to our devices (Article 8, Recitals 20-25)

The draft regulation seeks to clarify the scope of protection afforded to individuals. The text stipulates that devices such as mobile phones, computers, but also e-fitness or other Internet of Things devices are part of the individual's private sphere. This applies also to any information stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device (Recital 20).

Will we get rid of unnecessary cookie banners while banning intrusive tracking ones?

The Commission's proposal is likely to reduce the number of cookie banners and alleviate the burden on websites, particularly with regard to first party cookies and analytics. However, choices for end-users may become more confusing, and by relying on the handling of consent for cookies to the browser (which the Commission believes is a "gatekeeper" between the end-user and the website), the end-user is essentially left with the responsibility of defending herself or himself against tracking by blocking cookies.

Location tracking based on identifiers emitted from the device (Article 8.2)

Location based tracking based on identifiers emitted from the end-user device, for example the WiFi MAC address, poses the same privacy problems as equivalent services offered by a provider of electronic communication networks (ECNs). The draft Regulation requires explicit consent for the latter, whereas, for the former, notification of the end-user is required.

PROTECTION AND ENFORCEMENT: CONSENT, PRIVACY BY DESIGN AND BY DEFAULT, SANCTIONS AND COLLECTIVE REDRESS

Has consent changed in the e-Privacy proposal compared to the GDPR?

The definition and conditions for consent are cross-referenced to the GDPR, which will ensure a harmonised definition. The text in the ePR would allow, for example, to give or deny consent by the use of specific privacy settings in a browser.

Have privacy by design and by default been abandoned? (Article 10)

The leaked draft of the ePR from December 2016 required "privacy by design" for all components of the terminal equipment and electronic communication software. This has been replaced by the obligation for any software that permits electronic communication to offer different options, without having any option (i.e. the more privacy friendly) by default. Furthermore, the proposed Article 10 only covers software and not the components of the devices.

Who will be in charge of making sure that these norms are respected? (Article 18)

The proposal suggests that Data Protection Authorities (DPAs) will be in charge of monitoring the application of this regulation. This is an improvement on the earlier (leaked)

version, which allowed for supervision to be also placed in the hands of other regulators, such as telecommunication regulators.

Will civil rights groups and consumer groups be able to defend my privacy? (Article 21)

Although Article 21.2 refers to this possibility for individuals or legal persons "having a legitimate interest", both the concept of legitimate interest and the inexplicable absence of a reference to Article 80 of GDPR require further clarification.

Are fines and sanctions strong enough? (Article 25)

Fines for infringements of the main requirements of the regulation are the same as under the GDPR: up to 20 million Euro or up to 4% of the worldwide annual turnover of the organisation found in breach of the regulation.

EXCEPTIONS

Restrictions of the scope and rights and obligations for Member States (Article 11)

Article 11 of the ePR allows Member States to "restrict" – i.e. to provide by law for exemptions from the most important rights and obligations provided for in the Regulation, including the right to confidentiality of communications.

Consequently, these exemption clauses in the regulations again leave these matters first and foremost to be determined by Member States' laws. We feel this is a highly serious matter that must be urgently addressed in better, clearer rules than the vague derogation clauses in the draft ePR.

Conclusions

The e-Privacy Directive is a necessary legislative instrument in need of an urgent update, especially in light of the developments of modern communications technologies and the adoption of the GDPR. During 2016 the European Commission launched a series of consultations, impact assessments and surveys which were carefully prepared and which allowed for all stakeholders, including a great number of citizens and civil society groups, including EDRi, to express their opinion about how important privacy is for them and what needs to be done to update the current rules. The Commission has rightly addressed some of the key issues, although it seems to have watered down the text considerably, compared to the earlier version that was leaked in December 2016. The official draft proposal released in January 2017 falls far short of that earlier text in certain key areas.

Although the intentions of the Commission are laudable, the current text will need thorough work to ensure that the privacy, data protection and other fundamental rights in the EU (including the rights to confidentiality of communications and inviolability of the devices) are fully respected in the digital environment, also by providers of e-communication networks and services and OTT providers. Businesses and citizens also need clear, trust-inspiring rules, in order to avoid trust being destroyed by businesses exploiting legislative weaknesses for short-term profits.

A significant number of articles and recitals will have to be substantially modified if individuals' rights are to be appropriately protected and individuals' trust in the digital environment – and thus in the Single Digital Market – is to be assured. We hope the co-legislators will not fail individuals and businesses, with unforeseeable negative consequences. Given the quick development of certain technologies (Big Data, the Internet of Things), the European institutions need to make an extra effort to ensure that privacy and confidentiality of communications of European citizens are not considered as a disposable asset, but as a right to be strongly protected.

EUROPEAN DIGITAL RIGHTS

European Digital Rights | 20 Rue Belliard, 1040 Bruxelles, Belgium | Tel. +32 2 274 25 70 | www.edri.org