March 2017

ETNO's views on the Proposal for an ePrivacy Regulation

On 10th January 2017, the European Commission put forward its Proposal for a Regulation on ePrivacy (hereinafter "ePR"), which will replace the current Directive 2002/58/EC on privacy in the electronic communications sector ("ePD") and will complement the General Data Protection Regulation ("GDPR").

Executive Summary

- The proposed ePrivacy Regulation strengthens the principle of confidentiality to all interpersonal communications and this is certainly a positive step for better privacy protection and for an equal level playing field of all players.

- However, the proposed ePrivacy Regulation does not foresee the desired alignment with the GDPR in terms of recognition of additional legal grounds for processing e-communications metadata.

    - Therefore, ETNO calls for EU Legislators to include in the future ePrivacy Regulation "legitimate interest" as a legal basis for processing metadata in line with GDPR.

    - In addition, the future ePrivacy Regulation should also recognize, in line with GDPR, the right to further process metadata for other purposes compatible with the initial purposes for which the data was initially collected, provided that appropriate safeguards like pseudonymisation are put in place.

- These principles are essential to ensure a level playing field in data protection, to encourage innovation in big data and to enable responsible e-communications providers to provide trusted and secure innovative data driven services in an accountable manner.

- The GDPR already provides important safeguards regarding information, transparency, right to object, possibility to withdraw consent at any time, the need for Privacy Impact Assessments and finally heavy sanctions for infringing companies. Trying to be even more protective for consumers, the future ePrivacy Regulation could actually have a negative effect on European consumers, reducing the ability for telecom operators in Europe to create the best in class products for them.

General Comments

By way of introduction, ETNO recalls that, during the past preparations of the GDPR, it has consistently pleaded for a repeal of the ePrivacy framework, while taking into account the fact that the digital world has become increasingly convergent. The GDPR provides important safeguards regarding information, transparency, right to object and the possibility to withdraw consent at any time, the need for Privacy Impact Assessments and finally heavy sanctions for infringing companies, already applicable to the telecom operators. The GDPR was indeed put forward to answer the challenges of the digital world with the aim to achieve a comprehensive framework, technologically neutral, future-proof and flexible enough to allow the development of new services in Europe while maintaining Europe's high standards in the protection of personal data. The DSM Strategy of May 2015 stated that "GDPR will increase trust in digital services". ETNO therefore believes that the ongoing review of the ePrivacy Directive must be seized in order to at last move towards a consistent privacy framework for the benefit of businesses and consumers.

We also remind that, in its Inception Impact Assessment[1], the Commission explicitly mentioned the need to consider all policy options concerning simplification of the legal framework and consistency with other legal instruments (in particular the GDPR), including repealing outdated or unnecessary provisions of the ePD as well as a total repeal of the Directive.

Already in 2015, an independent study carried out for the European Commission on the ePrivacy Directive (assessment of transposition, effectiveness and compatibility with GDPR)[2] concluded that maintaining a distinct regulatory regime for electronic communications services, information society services or audiovisual services will most probably become less and less relevant in the future.

We thus regret that the European Commission has taken the view that an e-Privacy instrument is still necessary, and has thereby missed an opportunity to make a clear option for better regulation and simplification. Maintaining a double set of rules based on an old structure of sharing of competences will stand in the way of an equal level playing field, will continue to cause confusion for businesses and consumers and will finally hamper the possibility of European telco providers to develop innovative services.

While we could understand the willingness of the European legislator to regulate the principle of confidentiality of communications, we believe that the instrument goes way too far in restricting the usage of other sorts of data processed by a provider of an electronic communications network. We provide concrete examples of this below.

[1] Inception Impact Assessment – REFIT Evaluation and Impact Assessment of Directive 2002/58/EC (October 2016)

[2] SMART 2013/0071, June 2015

Specific Comments

Insufficient level playing field

Based on the definition of electronic communication services as contained in the Electronic Communications Code, the Commission's initial proposal for the ePR expands its material scope of application to also include the so-called *over-the-top* players offering interpersonal communication services (e.g. Messenger, Gmail). While this extension is clearly to be welcomed from a non-discrimination perspective, it remains a fact that article 6 of the ePR introduces a very strict regime for processing metadata that is applicable only to electronic communications services, and not to other providers who process metadata of a similar (or even more) delicate nature, like app providers working with location data (e.g. GPS data). There is no objective justification to apply distinctive regimes to different types of service providers, bringing the app providers under the more balanced regime of the GDPR, in addition to article 8 of the e-Privacy Regulation.

Too restrictive legal basis for processing e-communications data

Article 6 of the ePR foresees a very strict regime for the processing of e-communications data ("content" and "metadata"): the general rule is consent, with few exceptions. Data can be processed:

- for the transmission of the communication;
- to maintain or restore security;
- to meet mandatory quality of service requirements pursuant to the Electronic Communications Code and the Open Internet Regulation;
- for billing, interconnection, detecting or stopping fraudulent use.

Without prejudice to the above points, metadata will need to be erased or made anonymous when it is no longer needed for the purpose of the transmission of the communication.

While we understand the willingness of the regulator to avoid abusive processing of interpersonal communications and of metadata, the proposed provisions are disproportionate and stand in the way of a range of legitimate data processing purposes:

- The processing of electronic communications data for legal obligations (such as data retention obligations imposed by national law, legal interception and other legal tasks, etc.) is not explicitly foreseen by article 6. While article 11 allows Member States by way of a legislative measure to restrict the scope of obligations and rights provided for in Articles 5 to 8, in any case, an explicit reference should be included in article 6 referring to "the fulfillment of a legal obligation".

- The provision of emergency services for the protection of vital interests.

- The use of electronic communications data for the management and improvement/roll-out of the electronic communications network, which is not explicitly foreseen by article 6.

  In practice, network engineers must be able to monitor metadata (e.g. measure the usage or throughput per mobile cell, the usage habits in a certain fixed network area) and to certain extent even content (e.g. measure which applications impact throughput) in order to be able to efficiently manage traffic, and to take rational decisions as regards network investment & roll-out (where to install more mobile antennas, when/where to acquire network nodes, which agreements to be made with app providers whose applications slow down throughput, etc.). While pseudonymisation of the analysed data may be possible, network monitoring or planning cannot be done with anonymised data. Customer or location information are precisely the data, which are essential for these purposes. If the future ePrivacy Regulation does not explicitly foresee these – which are, in our view - perfectly legitimate purposes, telecom operators will not be legally allowed to efficiently improve the quality of their services and their network.

- Article 6 does not explicitly allow the use of electronic communications data for the development of products & services.

  In order to efficiently develop products and services that correspond to the needs of our customers, telecom operators use aggregated information based e.g. on usage metadata (% of roaming, divided over various locations, % of calls to fixed/mobile numbers, development of mobile data usage, etc.). It appears clearly inefficient and disproportionate if the ePrivacy Regulation would prohibit such use of metadata.

- Article 6 does not allow the use of metadata for direct marketing or customer care purposes.

  This means that telecom operators could not, without explicit consent, propose a more adapted tariff plan to a customer whose metadata shows that his tariff plan is not well adapted to his effective service usage, for instance, when he uses most traffic abroad. It means that telecom operators could not, without explicit consent, offer adapted coverage or care solutions to customers whose usage analyses reveal low network performance at home.

- Article 6 attaches great importance to anonymisation and the recitals (notably recital 17) recommend a very strict stance on anonymisation. Such strict position would make it impossible for telecom operators to make interesting and society-valuable

location analyses that concern somewhat longer periods, benefiting for example sectors as tourism, mobility, etc. Such location analyses could however still be developed by app providers working with location data that are more precise than location data collected through the ECN, and would thereby benefit from the more balanced GDPR regime, which explicitly recognizes the possibilities of pseudonymisation. Such difference in treatment does not seem justified.

Need for thorough rethinking of Article 6 of the ePR

Consequently, the above legitimate questions and concerns should be addressed in the ePR, for example by:

a) recognising **legitimate interest** as a legal basis for processing metadata, in line with GDPR, be it with an increased balanced of interests test that takes into account the specificity of electronic communications metadata;

b) recognising the right to **further processing of metadata for other purposes compatible with the initial purpose for which the data was initially collected**, be it with appropriate safeguards like **pseudonymisation** in line with the GDPR;

a) ePR needs to recognize legitimate interest as a legal basis for processing metadata in line with GDPR.

In addition to consent, GDPR recognises other legal grounds for processing personal data like legitimate interest or performance of a contract, among others. Based on the GDPR, the data controller is asked to strike a balance between its legitimate interest and the fundamental rights and freedoms of the data subject. This is a big difference between GDPR and the ePR: the former allows/obliges the controller to undertake a thorough assessment, weighing in its interests with the interests and fundamental rights of the data subject. The controller will not be able to process the data if its interest is overridden by those of the data subject. In contrast, the ePR does not even allow any assessment on the legitimacy of interests.

If legislators decide to maintain a specific ePR in addition to the GDPR, the proposed Art. 6 ePR should be modified in order to align with Art. 6 GDPR incorporating the additional legal grounds:

- processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. This would e.g. allow the usage of metadata for care purposes (serving customers whose metadata show that they have particular needs) or legitimate direct marketing purposes. It goes without saying that, in case of electronic communications data, the balance of interests may lead to a different conclusion of appropriateness than for other types of personal data.

b) enable the further processing of metadata for other purposes compatible with the initial purpose for which the data was initially collected as in the GDPR, as an exception from the consent requirement

Art. 6.4. GDPR states that when the processing is not based on consent, further processing shall be allowed when compatible with the purpose for which the data was initially collected and appropriate safeguards like pseudonymisation have been taken. In such a case, no legal basis separate from that which allowed the collection of the personal data is required.

This is especially important for Big Data services, where enormous amounts of data from different sources are required, while it is sometimes impossible to determine the exact purpose for processing at the time of collection. Big Data analytics and innovative business models require possibilities to further process personal data for other purposes (without consent) once the compatibility test is fulfilled. For the strict compatibility test established by the GDRP, the controller, after having met all the requirements for the lawfulness of the original processing, has to take into account, inter alia:

- any link between the initial purpose and the purposes of the intended further processing;
- the context in which the personal data has been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use;
- the nature of the personal data;
- the consequences of the intended further processing for data subjects;
- and the existence of appropriate safeguards in both the original and intended further processing operations.

All these requirements can be much more effective for a real privacy protection and to mitigate risks related to data processing than overwhelming users with consent requests out of context. Introducing the same rule in the ePR would ensure enough flexibility to innovate and would eliminate a competitive disadvantage that in turn reduces consumer's choice. European telcos want to be able to innovate whilst providing European citizens with high levels of privacy protection as in the GDPR and, at the same time, a wider range of choice of trustworthy high quality data driven services.

Like the GDPR, the ePR should promote safeguards like pseudonymisation. Big Data analytics rely on markers that permit linking information from various sources without directly identifying the individual, something that is not achievable with fully anonymised data.

In this line, Recital 17 of ePR clearly recognizes that: "*To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic*

communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure…". Therefore, the use of pseudonymisation techniques is necessary to be able to provide real time traffic information as well as long term traffic management.

ETNO calls for ePR to promote appropriate safeguards like pseudonymisation by aligning the rules for further processing of metadata with Art. 6.4. of the GDPR, including its strict compatibility criteria. GDPR encourages privacy-friendly techniques such as pseudonymisation "*to reap the benefits of big data innovation while protecting privacy*" as stated by the Commission itself when the political agreement on the GDRP was reached in December 2015[3].

In addition, Art. 5 GDPR sets the basic principles relating to the processing of personal data (purpose limitation, data minimization, lawfulness, transparency, storage limitation, integrity and confidentiality) that do not need to be repeated again in the ePR.

Data and not services should be the subject matter of regulation

If the above proposed changes would be considered unacceptable, achieving a level playing field **focusing on the privacy risks associated to a specific kind of personal data** (i. e. location data), then they should include all service providers processing the same type of data, irrespective of whether these services include electronic communications.

Additional rules regarding the provision of e.g. location based services should thus not be limited to electronic communication services, but should consequently apply to all services that are processing related data (e.g. mapping app services that process location data, allowing precise conclusions to be drawn regarding the habits and activities in user's everyday life such as daily movements and activities carried out).

ETNO (European Telecommunications Network Operators' Association) represents Europe's telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For questions and clarifications regarding this position paper, please contact Marta Capelo capelo@etno.eu

[3] http://europa.eu/rapid/press-release_IP-15-6321_en.htm