ePRIVACY DIRECTIVE: FORTHCOMING REVIEW

March 2016

ETNO

The European Telecommunications Network Operators' Association (ETNO) represents 41 major companies, which provide electronic communications networks over fixed, mobile or personal communications systems across 35 countries. ETNO is Europe's leading trade association for telecoms. More information about ETNO can be found at: www.etno.eu.

Introduction

Europe must create an environment that encourages data driven innovation in Europe, therefore, now that the General Data Protection Regulation (GDPR) has been agreed, it is time for an urgent review of ePrivacy Directive with the aim to:

- Remove overlapping provisions with GDPR;
- Transfer consumer protection rules, not related to privacy, into more appropriate tools;
- Clarify the scope of the remaining provisions in order to achieve a true level playing field between traditional telcos and Internet based service providers in the interest of businesses and end users (as stated in the DSM Strategy).

Priorities

The short term priority must be to achieve an operational framework based on coherent horizontal and sector specific rules. This coherent framework must also be able to secure transatlantic data transfers that respect EU data protection standards.

In the long term, the priority must be to achieve a framework which enables European businesses to compete at the global level in Big Data, Cloud services, IoT and Platforms.

Timing

If deemed necessary after revision, the new ePrivacy legal instrument should be put in place at the same time as the GDPR (early 2018) at the latest, for the necessary alignment with the implementation of general regulation. Legal certainty is essential for companies to be able to prepare for the new GDPR (e.g.: notification of security breaches overlapping between GDPR and ePrivacy). It is therefore crucial to meet this timeline. Moreover, ETNO strongly believes that the review process should be aligned with the review of the telecoms framework, for the sake of coherence between all legal instruments.

Legal Instrument

Once the overlapping provisions from the current ePrivacy Directive are removed and the consumer protection rules not related to privacy protection are identified to be transferred into more appropriate tools, it is necessary to consider what would be the best instrument for the remaining rules. Whilst consumer protection provisions should be transferred into consumer protection instruments, the remaining sector specific rules, if still necessary, could be transferred into other sector specific instruments, for example, into the Framework Directive in the telecom package.

Alternatively, if the ePrivacy instrument is to be kept, even with reduced scope, in the preparation of its proposal, the European Commission will have to choose what would be the most appropriate legal instrument. As the GDPR was approved as a regulation, the revised ePrivacy rules should also be enacted in the form of a regulation according to ETNO. This would allow both to work as complementary legislative tools on privacy. ETNO is convinced that this solution would significantly facilitate the application and enforcement of the legislation.

ePrivacy : On the substance

1. General remarks

ETNO believes that there should also be an alignment with the GDPR, regarding the Territorial scope of application.

Another challenge to consider concerns enforcement. In fact, whilst in some Member States the enforcement powers belong to the telecommunications National Regulatory Authorities, in others those powers lie in the hands of the Data Protections Authorities or the competences are shared between authorities competent in telecommunications and data protection

matters. The enforcement regime should therefore be adapted, for the sake of consistency and compatibility with the system established in the GDPR.

Finally, taking into account that the ePrivacy Directive applies to both natural and legal persons, the issue of the application to legal persons should be taken into account across the whole revision. It is necessary to use the same language in both legislative instruments to ensure consistency (e.g.: The ePrivacy Directive refers to "subscribers" and "users" while the GDPR refers to "data subjects")

2. Provisions covered by GDPR

Further to the approval of the GDPR, some of the provisions of the ePrivacy Directive became redundant and should thus be eliminated. Accordingly, the following rules should be repealed: Article 4, on security of processing and data breach notification, Article 6 on traffic data, Article 9 on location data and Article 15, on the possibility for Member States to restrict the scope of rights and obligations of the ePrivacy Directive.

In fact, as these provisions are already covered by GDPR, there is no need to maintain specific sectorial rules. A recent study published by CERRE on Consumer Privacy in network industries[1] states that a future proof regulation requires a common approach to all industries and that sector-specific privacy regulations are inadequate in a dynamic environment and should be withdrawn.

In particular, Article 15, the legal basis for national measures on data retention, can be deleted as Article 21 of the GDPR already foresees restrictions to the scope of rights and obligations when such a restriction respects the essence of the fundamental rights and freedoms. In addition, it is a necessary and proportionate measure in a democratic society to safeguard national security, defence, public security, prevention, investigation, detection or prosecution of criminal offences, etc. This provision did not exist in the currently applicable Directive 1995/46/EC and had been included in ePrivacy Directive. Now that there is a general rule in the GDPR, the specific provision in the ePrivacy Directive is no longer necessary.

3. Clarify scope and impact of certain articles

The following provisions require clarification:

- Cookies (Article 5(3)) – as this already applies to all actors, it would better fit in a horizontal regulation that applies to all sectors.
- Unsolicited communications/spam (Article 13) – as this already applies to all actors, it would better fit in a horizontal regulation that applies to all sectors.

[1] http://www.cerre.eu/publications/consumer-privacy-network-industries

- Provisions on confidentiality of communications (Article 5(1)) – Whether these obligations are still relevant in the context of the GDPR and the European Charter of Fundamental Rights should be questioned. But if deemed necessary, these provisions should apply to all actors, not only to telcos and therefore should be transferred to a horizontal regulatory instrument.

4. Transferal of non-privacy-related provisions to Telecoms Framework

Regarding the remaining non-privacy related provisions - itemised billing (Article 7), calling line identification (Articles 8 and 10), automatic call forwarding (Article 11) and directories (Article 12), there should be a thorough assessment on whether they are still relevant. To the extent in which it is concluded that there is still a need to keep any of these provisions, they should be transferred to the Telecoms Package.

Privacy and DSM

The third pillar of the Digital Single Market Strategy aims at creating conditions which enable European companies to embrace the possibilities offered by the digital revolution and regain leadership in the data economy.

The DSM Strategy highlights the importance of Big Data as a catalyst for economic growth in the form of Cloud services, the Internet of Things or research and data mining.

It is important to strengthen opportunities to realise the potential value of data, pursuant to the Big Data Strategy and key Digital Single Market objectives. Everything depends on getting the framework right. The above mentioned CERRE study refers to a gap in EU Data Protection rules (including GDPR), which makes them not entirely adapted to data-centric business models as opposed to other business models where data processing is just ancillary to a main business.

The forthcoming review of the ePrivacy Directive will be a unique opportunity to enable the EU to regain leadership in the digital environment. If the GDPR becomes applicable two years after its formal adoption in the spring of 2016, as expected, this means that we have two years ahead of us, until Spring 2018, to undertake a fundamental review of the ePrivacy Directive.

Roberto Viola, Director General DG CONNECT has repeatedly stressed the need to look at data as a society challenge and Data Driven Innovation as a huge opportunity to be embraced and has called for the debate to be put at a higher level (up to Heads of State and Government). It is in this spirit that we need to address the review of the ePrivacy Directive.