Telecommunications and Cable Industry Note on the Draft e-Privacy Regulation

ETNO, the GSMA and Cable Europe, as the voice of Europe's leading telecom and cable operators, have been heavily invested in the debate surrounding the draft e-Privacy Regulation, since its publication in January 2017.

We have contributed constructively to the deliberative process given that confidentiality of communications lies at the heart of the services offered by telecom and cable operators. We consider the protection of privacy of our customers and their communications as integral, and not an obstacle, to allowing European telcos to use electronic communications metadata for added-value services improving customer experience and bringing societal benefits.

Since the General Data Protection Regulation (GDPR) has transformed Europe into a standard setter for fundamental rights protection in the digital economy, it is crucial that the ePrivacy Regulation has a clear articulation and alignment with the GDPR, confirm a level playing field for all players, and allow European industry to be competitive in the growing field of data analytics and lead in responsible Artificial Intelligence.

Council's recent failure to achieve an agreement on the proposal begs for a moment of reflection. Although the reasons for rejection may differ from one Member State to another, the draft regulation continues to raise deep concerns across countries and across sectors, nearly three years since its inception.

Therefore, ETNO, the GSMA and Cable Europe believe it is the right time to consider whether the proposal on the table is an appropriate basis for adequately complementing the GDPR framework, as well as enabling the European Commission's vision for digital leadership, a thriving data economy and trustworthy Artificial Intelligence.

We thereby call on the Commission to **support a revamped proposal** that effectively achieves the above-mentioned objectives. We are committed to cooperating with the Commission and the rotating Presidency of Council in attaining the best possible way forward for this crucial file.

To this end, we would like to recommend the following **guiding principles**:

- **Strong confidentiality principle**: The fundamental principle that private communications should be confidential is enshrined in national Constitutions and has been at the core of the telecommunications sector's business. We therefore believe that a clear legal safeguard for the privacy and confidentiality of people's communications remains necessary.

- **A clear regime for personal data:** While communications may contain both personal and non-personal data, and confidentiality should be ensured for the whole of the communication, the rules governing the lawful processing of user communication data should only cover personal information in line with the stated scope of the draft regulation [Art. 1(1): "This Regulation lays down rules regarding (…) the protection of natural persons with regard to the processing of personal data]. Adding further clarifications that non-personal and anonymised data (see Art. 7) are outside the scope of the regulation (except for the confidentiality principle) will guarantee legal certainty also for machine-to-machine and Internet of Things services.

- **<u>A flexible and risk-based approach to metadata processing that ensures an adequate level of protection</u>:** The processing of electronic communication metadata may or may not reveal sensitive personal information of the user, depending on the nature, scope, context and purposes of the processing operation at hand[1]. This is the case with processing of personal data in general, to which the GDPR applies a risk-based approach that grants data controllers a margin of appreciation of the safeguards and the mitigation measures to take following an assessment of the risks for individuals. Accountability is a key principle of the GDPR and ensures that the framework remain future-proof and do not hinder innovation.

  Article 6 GDPR establishes that personal data can be processed based on a set of legal grounds:

  - Individual's consent;
  - Necessity for the performance of a contract;
  - Necessity for compliance with a legal obligation;
  - Necessity for protecting the vital interests of individuals;
  - Necessity for the performance of a task carried out in the public interest;
  - Necessity for achieving 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 individual.

  In collecting and processing data according to these legal bases, a controller must comply with various principles and safeguards as per Article 5 (e.g., transparency, purpose limitation, storage limitation, accuracy, integrity, accountability). Furthermore, specific measures apply when a particular processing operation could entail a high risk to the rights and freedoms of individuals, such as the obligation to conduct a data protection impact assessment (Art. 35) and to consult the supervisory authority before initiating the processing if the risk cannot be adequately mitigated (Art. 36). Rules on transparency and information toward data subjects (Art. 12-14) and strong data subject rights (Art. 15-21) ensure that individuals can control how their personal data is used and shared in real life by companies beyond the moment of collection of the data.

  Such flexible approach, which warrants a high level of protection by basing on accountability and comprising a set of principled legal grounds for processing coupled with an appreciation of the safeguards according to the risk, is completely absent in the proposed e-Privacy Regulation. The draft rules allow for metadata processing only against user's consent and a few narrow purposes modeled around specific exceptions and use cases, rather than principle-based legal grounds that can meet these specific purposes as well as many others that may arise. This severely undercuts the ability of electronic communications providers to process metadata under the most suitable legal base according to the purpose, and to safeguard the data according to the level of risk for individuals. This very restrictive approach is not future-proof despite the fast-evolving nature of digital services.

  The idea that consent is the only and best way to ensure that individuals' rights are protected is questionable. While consent can be appropriate in many instances,

[1] See 'Legal memo with respect to the concept of metadata and its degree of sensitivity under future European e-privacy law', Timelex, January 2018.

overreliance on consent can lead to 'consent fatigue', thus rendering poor privacy outcomes for individuals. Asking users to continuously evaluate notices and provide consent shifts responsibility from service providers to users, which may undermine and potentially even weaken the notion of consent. A telecom provider is accountable for ensuring that its processing is being conducted in a lawful manner, and documenting and demonstrating that accountability, all against the backdrop of potential enforcement and significant fines.

This regulatory imbalance between the rules for metadata processed by electronic communications data providers, and those for similar personal data (e.g., GPS location data) processed by other players is unjustified, since metadata as such are not inherently sensitive and their potential to reveal delicate private information could be mitigated thanks to GDPR's safeguards and measures.

In light of the above, we recommend that, in addition to preserving the principle of 'compatible further processing' laid down in the Council text, the lawful grounds for processing metadata in the revised e-Privacy proposals be further aligned with those for personal data processing under Art. 6 GDPR, and explicitly provide that the GDPR's principles for processing, safeguards, and risk-mitigating measures cover metadata *mutatis mutandis*.

We recognise that the content of electronic communications may require stricter grounds for processing than the processing of technical metadata.

- **More certainty on the relationship between processing of metadata and processing based on end-users' terminal equipment**. The provision of innovative digital TV offerings (such as personalisation of content or targeted advertising) may involve the use of information from end users' terminal equipment (e.g. set-top-boxes) and may also involve the processing of metadata. That broadcasting data do not constitute electronic communication services.[2] The potential application of articles 6 and 8 to the provision of these services does not contribute to legal certainty and would be at odds with the European Electronic Communications Code.

- **More certainty for safeguarding the fulfillment of legal obligations**: The concerns raised by some Member States in Council that the draft e-Privacy rules may stifle the ability to handle communications data to safeguard specific law enforcement purposes is rooted in the proposal's tight approach to permitted data processing. The GDPR already provides solutions to tackle these concerns. The alignment of the lawful grounds for processing metadata with the GDPR, including compliance with a legal obligation would provide public authorities with more certainty that important public interests will not be hampered.

We firmly believe that an e-Privacy Regulation proposal amended along said guiding principles would meet the need for a consistent privacy framework that, together with GDPR, successfully protects the privacy of citizens, keeps up with fast-paced technological developments, and lets European industry use data responsibly as a key factor for innovation and competitiveness.

Our Associations would be delighted to engage constructively with the new European Commission's leadership towards achieving said goals, and to elaborate in more details on our suggested guiding principles.

[2] Recital 7, Directive (EU) 2018/1972