Statement on the ePrivacy Directive revision process

Brussels, 22 December 2016

We are writing to express our concerns with the overall policy approach reflected in a leaked draft of the proposal for a revision of the ePrivacy Directive. As a group of trade associations[i] representing large segments of the digital economy in Europe, we urge the European Commission to take the concerns outlined below into consideration before adopting its definitive proposal.

We would like to reiterate that the General Data Protection Regulation (GDPR) already provides for a high level of protection of users' personal data and addresses the vast majority of the issues that the proposed ePrivacy Regulation seeks to cover. Furthermore, ensuring coherence between these two legal instruments is essential.

We believe that the policy approach in the draft proposal risks undermining the balance of the digital ecosystem, is disproportionate and is likely to be ineffective:

- **Scope**: Broad definitions underpinning the draft proposal will extend its scope to a disproportionate array of applications and services, including Machine-to-Machine communications which, by their nature, should not be subject to rights and obligations aimed at protecting end-users. This would risk putting an excessive burden on developers and might stifle innovation. The scope should be restricted to "interpersonal communication services".
- **Harmonisation, definitions and enforcement:** Whilst we welcome the choice of a Regulation as a legal instrument in principle, we are concerned that instead of simply referencing the relevant provisions of GDPR, the draft proposal replicates – and even redefines or qualifies – them, which would inevitably open the door for divergent interpretation and legal uncertainty. We strongly encourage the Commission to maintain only references to the GDPR and not to create an analogous duplicate framework subject to different interpretations.
- **Confidentiality of communications:** By restricting the legal bases which allow the processing of electronic communications, the proposal would require relying exclusively on user consent, despite the wealth of evidence demonstrating the ineffectiveness of the consent-only approach currently in force.
- **Communications metadata:** We welcome the attempt to provide more exceptions for the processing of communications metadata beyond consent. However, rather than proposing a restrictive 'white list' approach, the proposal should provide the needed flexibility for digital industries to flourish. The legal grounds for data processing should therefore be aligned with those of the GDPR.
- **Privacy by design:** Though titled "privacy by design," this provision bears little in common with the privacy by design provisions in the GDPR, which speak to general good data protection practices. The future ePrivacy instrument should not restrict the possibility of services to lawfully interact with user devices by imposing a duty on manufacturers and developers to erect technological barriers.

- **Online advertising and cookies:** The draft proposal would risk significantly disrupting the current advertising-funded model of the digital ecosystem, on which the vast majority of content and services in Europe and beyond rely. The draft provisions would also impede – if not make impossible – the funding of digital media and applications in Europe. While we welcome the addition of an exception to the consent requirement of the previous ePrivacy Directive, this does not reflect a harmonised approach. Lawful use of cookies and similar technologies should be aligned with legal grounds for processing of the GDPR – not only on the condition of prior consent.
- **Law enforcement access:** It is essential that the proposed regulation does not open the gates to law enforcement authorities to request users' personal data from an ever broader range of service providers. This would be in contradiction with DG HOME's ongoing effort to work collaboratively with industry to find practical solutions and achieve better cooperation between service providers and law enforcement agencies. Furthermore, it is fundamentally misplaced to use the ePrivacy Regulation, a legal instrument which is designed to protect privacy and ensure the confidentiality of communications, to facilitate law enforcement access to communications. This would not only undermine the credibility of the instrument, but is also in contradiction with the core principle of the draft Regulation.
- **Security of processing:** We welcome the proposed streamlining of security requirements and alignment with the GDPR. However, the remaining provisions on providing transparency of risks to end-users would set the threshold for notification far too low, given that network threat monitoring services see billions of security events every day. The introduction of any security requirements over and above those in the GDPR and the NIS Directive would not be evidence-based.
- **Unsolicited communications:** Transparency can help ensure the protection of individuals' rights without relying exclusively and excessively on consent, which leads to consent fatigue and fails to give users the necessary amount of control over their data.
- **Caller ID and call blocking:** While these provisions are intended to be targeted at traditional telecoms as opposed to OTT service providers, because many OTT communication services allow users to dial out to or in from, the public switched telephone network (PSTN), such services would nonetheless be covered, in contrast to the declared intention.
- **Redundant historical telecoms specific provisions:** Considering the evolution of technology and business models and practices, we question whether provisions on itemised billing, call line identification, directories, call forwarding (Articles 7, 8, 11 and 12, ePrivacy Directive) are still necessary today. These provisions relate to commercial practices and consumer protection rather than privacy or security concerns. If maintained, they should be covered by the telecoms regulatory framework.

The revision of the ePrivacy Directive is an opportunity to bring it more in line with the recently adopted General Data Protection Regulation, but should not be used to create new definitions and additional burdens. It is meant to protect the privacy of communications while ensuring a flourishing single market, not to prompt consent fatigue and stifle innovation. This is an opportunity to determine a workable and proportionate approach for a future-proof model.

[i] AmCham EU, CCIA, DIGITALEUROPE, EACA, EDiMA, EMOTA, EPC, EuroISPA, FEDMA, FENCA, IAB Europe, WFA