AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Clarity and consistency key for a strong ePrivacy Regulation

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3 trillion in 2020, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive Summary

The European Commission's ePrivacy Regulation seeks to further build trust and confidence in services for both the consumer and businesses. In the four years since the European Commission initially presented the ePrivacy Regulation the importance of metadata and electronic communications has been reinforced, especially in the context of the COVID-19 pandemic. The American Chamber of Commerce to the European Union (AmCham EU) commends the institutions for finding a way forward with regard to the ePrivacy Regulation and bringing it to trilogues, however we urge the co-legislators to rethink certain aspects of the regulation to avoid limiting the European data-driven economy.

AmCham EU's top-line recommendations to guide trilogue negotiations
Ensure clarity on scope and alignment with the GDPR whilst adopting a risk-based approach to the text
Permitted processing of data (articles 6 and 8) for software updates, security, compatible further processing and statistics is welcomed, and the legal basis of processing data should be closely aligned with the GDPR where possible
Privacy Settings: Additional lawful bases should be included in Article 8 to allow the use of storage capabilities on-device for limited processing activities and we recommend subsequent amendments to Recital 20 and 21. The deletion of Article 10 is supported however should not hinder introducing language that facilitates incentives

Introduction

It is now four years since the European Commission presented its proposal for an ePrivacy Regulation[1]. The trust and confidence of consumers and businesses in digital services is key for the success of the European Commission's Data Strategy[2]. The same goes for Europe's businesses as they develop innovative services in the space of Machine-to-Machine (M2M), Internet-of-Things (IoT) and Artificial Intelligence (AI). As has been highlighted by Commissioner Thierry Breton, the COVID-19 pandemic showed the importance of metadata and electronic communications for societal benefits, allowing governments to alert citizens about confinement rules. While we appreciate the amount of work put forth by the co-legislators, we believe that the proposal risks severely limiting the potential of a data-driven EU digital economy.

With this input, we touch upon the areas of the draft regulation that we encourage negotiating parties to consider ahead of forming trilogue compromise amendments. The below paper sets out three high-level points that we believe should guide negotiators during trilogues to ensure Europe is able to continue to protect the confidentiality of communication, while allowing for a competitive European data economy. These are 1) ensure clarity of scope, 2) permitted processing of data, 3) privacy settings.

1. Ensure clarity on scope and alignment with the GDPR (Article 2)

It is essential for trilogue negotiators to ensure greater clarity between the General Data Protection Regulation (GDPR)[3] and the proposed ePrivacy Regulation. Additionally, to ensure consistency between the two frameworks, the negotiators should adopt a risk based approach throughout the text. We remain concerned over the lack of distinction between the concept of data protection (regulating the processing of data related to individuals) and confidentiality (protection of communications from unauthorised access by third parties during transmission). We welcome the Council's attempts to clarify the relation between the proposed ePrivacy Regulation with the GDPR as highlighted in Recital 2a.

In addition, we are generally concerned about the extension of the scope of the draft regulation to legal persons, e.g. for B2B relations (see Council text in Recital 2a and Article 1a as well as broadly throughout the European Parliament text). We appreciate the Council's attempt in Recital 16c to exclude situations whereby legal persons allow natural persons, such as employees, to use a service and therefore designate any subsequent processing in accordance with the GDPR. However, it would be preferable to limit the scope of the draft regulation to only natural persons in alignment with the GDPR.

Of particular importance to AmCham EU is the distinction for data in transmission. It is essential to clearly define the scope of the draft ePrivacy Regulation by excluding electronic communications data processed after receipt by the end-user concerned. The problem arises from the inclusion of machine-to-machine (M2M) communication in the draft regulation. To ensure alignment with the GDPR, the concept of 'transmission' should be defined narrowly according to existing protocols and distinguish real-time communications from asynchronous communications. The draft regulation should also clearly state that the transmission phase ends with the electronic communication service provider and not the end-user. It should, for example, not depend on whether the user opened an email or not.

[1] Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

[2] Communication on a European Strategy for Data COM/2020/66 final

[3] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

The text would therefore benefit from an exclusion of M2M and IoT services from the scope. The inclusion causes concern in the case of self-provisioned services by an organisation that does not include processing of data of individuals (e.g. smart agriculture sensors).

AmCham EU's recommendations for ensuring clarity on the scope and alignment with the GDPR
We strongly support the European Parliament's clarification in Recital 15 that "*the transmission starts with the submission of the content for delivery and finishes with the receipt of the content of the electronic communication by the service provider of the intended recipient*". This would provide more clarity for the service provider, as per the jurisprudence of the Court of Justice of the EU. This language provides more clarity than the added suggestion by the Council in Article 2(2)(e) which limits it to receipt by the end-user.
Favour the Council's proposal in Recital 12 to exclude transmission of M2M or IoT services over a private or closed network.
Urge the co-legislators to address cases whereby an entity providing a service does not have a direct contractual relationship with the end-user. For example, when considering smart traffic management - such as smart traffic lights - road users' data may be processed, but there is no user interface providing the possibility to obtain consent. Such processing would be allowed under the GDPR yet the draft ePrivacy Regulation risks making such lawful and sensible processing activities unduly prohibited.

2. Permitted processing of data (Articles 6 and 8)

The ability for service providers to process electronic communications data and data collected from terminal equipment is one of the core components of the draft ePrivacy Regulation. AmCham EU has long advocated for closely aligning the legal basis for processing with those of the GDPR. The original European Commission proposal along with the amendments of the European Parliament remain highly restrictive and would lead to a situation in which user consent would be required for the overwhelming majority of use cases. We therefore welcome the additional grounds for processing provided in Article 6 and 8 related to software updates, security, compatible further processing and statistics.

AmCham EU's recommendations for the permitted processing of data
Ensuring security of services: We welcome the changes proposed by the European Parliament and Council to allow for processing for security purposes (see the Council text Article 6 (1)(b) and (c) as well as the European Parliament text Article 6(1)(b)). The same applies to Article 8 (1) (da) proposed by both the Council and the European Parliament.
Updates of software to manage vulnerabilities: it is positive that both parties have added grounds for processing to allow software updates to address vulnerabilities (see the European Parliament text Article 8(1)(i)-(iii), and Council text Article 8(1)(e) respectively). The European Parliament also extends this to hardware. We note that security updates may change or cancel certain settings or features that may be the cause of the identified vulnerability or breach. The legislation should not prevent that. Requirements should be limited to 'respecting' the previous settings, not prohibiting any changes to it.
Performance of contract: We support the Council introduction of a legal basis which would permit (among other purposes) the processing of electronic communications metadata, to the extent that such processing is necessary for the performance of an electronic communications services contract to which an end-user is a party (Article 6b(1)(b)). This provision allows for metadata processing that is necessary to provide agreed service features (other than mere transmission) in accordance with the terms of a contract. The introduction of such a legal basis will be pivotal to ensuring that end-users are able to continue to receive a product experience they've come to expect.

Allowing processing that is compatible with the initial purpose: We support the addition by the Council to allow compatible for further processing (CFP) of electronic communications metadata, in Article 6(c) and Article 8 (1)(g), as this ensures alignment with Article 6(4) of GDPR. It allows controllers to reuse personal data for a new purpose other than the purpose of the initial data collection, on the condition that the two purposes are compatible. Such compatibility must be assessed based on a number of strict criteria (context of data collection; nature of the data, in particular if sensitive data or criminal offence data are processed; possible consequences of the intended processing for data subjects; and existence of appropriate safeguards, e.g., encryption or pseudonymisation).
Allowing processing for vital interest: We support the Council introduction of a vital interest legal basis for the processing of electronic communications metadata. The introduction of this legal basis is important for protecting end-users and the wider public. This includes preventing and navigating emergency situations that have a high impact on public safety or health. The Council rightfully recognises the importance of processing in the vital interest for humanitarian purposes, including for monitoring epidemics or humanitarian emergencies, such as natural or man-made disasters.
Services requested by the user: We welcome that both parties have added language on the situation when processing is required to provide the service requested by the user (see Council text Article 6a (1)(a) and European Parliament text Article 6 (3a new)).
Web audience measurement: We welcome both institutions' introduction of web audience measurement by third parties among the exceptions listed under Article 8(1)(d). Measurement of audiences is a legitimate and necessary aim as it enables services providers to accurately understand the ways in which their services are being used, whether new features are working as intended, and to accurately assess end-user engagement. The purpose of audience measurement is to look for trends in an aggregated analysis, and not individual results. It is an essential activity for businesses, including SMEs, to grow their businesses across the EU Single Market. In addition, as not all measurement services are considered as 'processors', we welcome the reference to Article 26 GDPR by the Council

Our concerns remain on:
Consent of 'all' communication parties: both texts keeps the need to get consent of 'all' the communication parties to process metadata (see Council text Article 6a (3)(b) and Recital 15). It is a concept that does not work for services that allows for interoperability with another provider (such as email). We understand the Parliament tries to mitigate such unintended effects in Article 6 (3a) for situations that does "not adversely affect the fundamental rights and interests of another user or users". However, this notion could lead to legal uncertainty and would benefit from clarification.
Fundamental inconsistencies of the required consent standards across articles 6 and 8: We would propose to adopt a risk based approach in ePrivacy similar to GDPR. The difference does not only exist with the GDPR. There is a different requirement for metadata (Article 6b (1)(c)), two different standards for content data (Article 6a (1)(b)) as well as for terminal equipment (Article 8). In order to ensure a uniform standard and consistency with the GDPR, Article 6(1) should contain the same language as Article 8 (1)(b), namely that the 'end-user of the service has given his/her consent'.

3. Privacy settings (Article 8 and 10)

A more principle-based and tech-neutral approach would make the text more future-proof. Technology is evolving and the user expectations as well. More than ever trust is required and trust can help the further use of digital tools, services and digitisation in general.

The currently foreseen default-model of consent for processing electronic communications data (except in limited specified circumstances) and IoT will also apply to many privacy-enhancing/privacy-preserving technologies (PET/PPT)) in accordance with the obligation under Art 25 GDPR for data protection by design and by default. While these have a special legal ground in Article 25 GDPR this is not the case under the ePR. While it is positive that the Parliament's text acknowledges that such technologies can also be legitimate and useful (Recital 21 and 23), we recommend including additional lawful bases and safeguards in Article 8 to clarify and allow for limited processing activities and amendments to Recital 20 and 21. The ePR should not be a hurdle for this GDPR compliance and the further development of PET/PPT.

In addition, we support the deletion of Article 10 as proposed by the Council. We suggest also deleting Recital 20(a) and any corresponding parts to increase the lifespan of the legislation. 'Whitelists' will not be easily managed by consumers and do not remove the operational difficulties of a granular choice. The deletion of Article 10 should not hinder introducing language that facilitates incentives for further development of PPT through a privileged regime or a separate legal base that technologies under Art 25 GDPR do not require explicit consent.