Comments on recent Council Presidency text on ePrivacy

This document includes views of the American Chamber of Commerce to the EU (AmCham EU) on the recent text proposal published by the Romanian Council Presidency on 22 February 2019[1]. It draws on the 2017 AmCham EU position paper[2].

Key messages

1. **We welcome attempts by the Presidency to introduce more flexibility into the Commission proposal on confidentiality of electronic communications ('The e-Privacy Regulation'). However, based on the current text, it remains unclear what business operations have to comply with what law (GDPR vs. e-Privacy).**
2. **Alignment with the GDPR does not go far enough. The e-Privacy Regulation continues to focus on regulating processing rather than interference, without foreseeing all necessary legal bases to allow the functioning of devices, services and features that rely on processing of communication data.**
3. **More flexibility is needed on permitted processing of communication content and metadata. Any 'all-party' consent requirement would outlaw email and any other interoperable communication services.**
4. **As it stands, there are different consent standards respectively for metadata, content data and for terminal equipment information. The language around consent requirements should be consistent and simply refer to 'end-user of the service has given his/her consent'.**
5. **The Regulation should adopt a technology-neutral approach. Legislators should consider the impact of suggested restrictions on third-party processing beyond cookies and browsers, given that they would apply to all types of software.**
6. **On-going discussions on 'e-evidence'[3] should be taken into account and be referenced both in Article 11 and Recital 26.**

[1] Document 6771/19: https://data.consilium.europa.eu/doc/document/ST-6771-2019-INIT/en/pdf

[2] http://www.amchameu.eu/position-papers/position-paper-amcham-eu-position-paper-proposal-regulation-e-privacy

[3] AmCham EU position on the Commission proposals here: http://www.amchameu.eu/position-papers/proposal-cross-border-access-e-evidence

AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
amchameu.eu • European Transparency Register: 5265780509-97

More information:
Maika Fohrenbach
mfo@amchameu.eu

Recommendations

Contents

Alignment with the GDPR

The lack of clarity between the GDPR and the proposed e-Privacy Regulation stems from the fact that the latter continues to confuse the concept of data protection (regulating the processing of data related to individuals) with confidentiality (protection of communications from unauthorised access by third parties during transmission). These rights are intentionally separated in the EU Charter of Fundamental Rights (Articles 7 and 8) and that same differentiation should be reflected in both legal instruments: the GDPR should provide for data protection, while the e-Privacy Regulation should protect the confidentiality of communications.

- We note and welcome the Presidency's attempts to clarify the relation between the e-Privacy proposal with the GDPR as highlighted in **Recital 2a**;

- However, uncertainty continues to arise from the fact that the e-Privacy Regulation, in addition to confidentiality of communication data, also covers processing of communication data (see our comments on article 6, 8 and 10).

Data in transmission

In the light of the comments included in the previous section (overlap with the GDPR), the concept of 'transmission' should be defined narrowly according to existing protocols and distinguish real-time communications from asynchronous communications. It should also be noted that including data in transmission in the scope is problematic in the context of machine-to-machine communications (M2M), as noted in the following section. Therefore, the text should clearly state that the transmission phase ends with the provider of the electronic communication service provider and not the end-user.

- The changes to **Article 5 paragraph 1 and Recital 15** are helpful as they clarify that the objective of proposal is the prohibition of 'any interference' instead of the prohibition of 'processing' electronic communication data.

- We welcome the attempts included in the **Recital 15** to clarify the scope of the proposal by stating that the prohibition of interference should only apply until receipt. It adds that: 'receipt implies that the end-user gains control over, and has the possibility to interact with, the individual electronic communications content, for example by recording, storing, printing or otherwise processing such data'.

AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
amchameu.eu • European Transparency Register: 5265780509-97

More information:
Maika Föhrenbach
mfo@amchameu.eu

- However, as per the above, the recital should make it clear that the prohibition should apply until receipt of the content of the electronic communication 'by the electronic communication service provider'. The application of a law should not depend on whether the user opened an email or not and should be predictable and foreseeable for the service provider, as per the jurisprudence of the Court of Justice of the EU.

Machine-to-machine communication

Computing in the Internet of Things (IoT) context is increasingly moving closer to the sensor in phenomena known as 'edge computing' and 'fog computing'. The rationale of these technologies is to decrease bandwidth, overcome unreliable connectivity, reduce latency and improve security and privacy. In this context, the processing typically takes place during transmission and hence would be covered by the Regulation as currently drafted.

- First of all, uncertainty stems from the fact that the e-Privacy Regulation clearly includes transmission services for machine-to machine (M2M) services, as per the definition of 'electronic communication services' foreseen in the Electronic Communications Code (**Recital 12**).

  The inclusion of processing during transmission in the scope reduces the number of legal bases available for such processing when compared to what is foreseen under the GDPR for personal data (e.g. legitimate interest, performance of contract or public interest) and/or unregulated processing of non-personal data.

- Furthermore, the presidency text insists even more - compared to the Commission proposal - on the applicability to both legal and natural persons (**Recital 2a, Article 1a**). Legal persons benefit from a range of protections and should be excluded from the scope in the same way they are excluded from the GDPR.

- The broad scope is particularly problematic in use cases where the M2M service is self-provisioned by an organisation but does not include processing of data of individuals (e.g. smart agriculture sensors). If none of the additional legal bases foreseen in the GDPR for processing data are relevant (which is more than likely as no personal data is involved), it is unclear how consent would be used as there is no obvious end-user in a self-provisioned service.

  Recital 19b clarifies that consent can be obtained by the end-user at the time of the conclusion of a contract. However, it further states that if a natural person makes use of the service, such as an employee, consent needs to be obtained from the individual concerned. The suggested consent requirement for employees in recital 19b seems to be at odds with the GDPR, as the latter is sceptical whether consent in this context can be valid.

  We need a more practical answer to the following situations:

  - When the end-user is a company (i.e. when communication and usage of terminal equipment is carried out for non-private business reasons);
  - When the end-user is an employee (i.e. in case of private communication/usage of terminal equipment).

  Furthermore, the text also needs to tackle cases where the entity providing the service does not have a direct contractual relationship with the end-user. One example is smart traffic management - such as smart traffic lights - where road users' data may be processed but there is no user interface providing the possibility to obtain consent. This would not be an issue under GDPR as either public interest or legitimate interest would be valid legal bases to process the data.

  We regret that **Recital 21**, which relates to cases where consent is not required, does not address all these situations.

AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
amchameu.eu • European Transparency Register: 5265780509-97

More information:
Maika Föhrenbach
mfo@amchameu.eu

Ancillary services

We welcome attempts to clarify that **ancillary services** are only covered by the Regulation if they represent interpersonal communications services as per the Electronic Communication Code (**Recital 11a**). The Code already contains a definition of what interpersonal communications services are, therefore we welcome that the second part of Recital 11a which re-defined 'interpersonal communications services' has been deleted.

However, we remain concerned about the broad scope of the Regulation and wonder why there is a need for such a catch-all clause. It does not seem proportionate to the risk of processing such communication data.

Deletion of communication data

Storage and erasure of data should be context-based to reflect different users' expectations for different types of services. We question whether a one-size-fits-all approach is in line with user expectations. Instead of the proposed **Recital 15a** and **Article 7**, we suggest the following language to achieve this objective:

Article 7 - 'Without prejudice to Article 6, the provider of the electronic communications service shall erase electronic communications content or process such data in accordance with Regulation (EU) 2016/679'.

Article 7 paragraph 1 states that after receipt, data can be processed by the end-users or a third-party entrusted by them in accordance to the GDPR. It is important to note that service providers are not considered a third-party in the GDPR.

Security

We welcome that the exception to permitted processing for ensuring network and information security (**Recital 8**) has been maintained. Furthermore, it is positive that the exceptions in articles 6 and 8 now also consider the need to fight fraud and abusive use of a service (e.g. child pornography). We welcome following provisions:

- **Recital 8**: maintains that information society service providers that process electronic communication data for purposes of network and information security are not covered by this Regulation;
- **Recital 16**: covers security, including availability, authenticity and integrity or confidentiality of electronic communication services;
- **Article 6 paragraph 1 b), c) and d), 2 a):** if it is necessary, to maintain and restore the security of electronic communications networks and services; if it is necessary, to detect and prevent security risks on terminal equipment; if it is necessary to enable detection and deletion of material constituting child pornography (together with 1a);
- **Article 8 paragraph 1 (da):** 'it is necessary to maintain or restore the security of information society services, prevent fraud or detect technical faults for the duration necessary for that purpose';
- **Article 8 paragraph 1 (e) (i):** software updates which are necessary for security reasons.

  We also note here 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.

We would like to raise one contradiction: the Presidency suggests excluding security-related processing from the scope (Recital 8), however, it also suggests language for security under articles 8 and 6. A general exception for security measures, including fraud and abusive content, would provide more legal certainty.

AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
amchameu.eu • European Transparency Register: 5265780509-97

More information:
Maika Föhrenbach
mfo@amchameu.eu

Consent for permitted processing

First of all, we would like to emphasise the need to provide more flexibility and move away from an overreliance on consent, especially given the broad potential scope of the Regulation (see previous sections). In particular:

- We are concerned about the fundamental inconsistencies of the required consent standards across articles 6 and 8. The difference does not only exist with the GDPR. There is a different requirement for metadata (Article 6(2)), two different standards for content data (Article 6(3)) as well as for terminal equipment (Article 8). In order to ensure only one standard and ensure consistency with the GDPR, Article 6(1) should contain the same language as Article 8, namely that the 'end-user of the service has given his/her consent'.

- We welcome that the Presidency deleted the reference to consent of **'all'** the communication parties in **Recital 15**, a concept that does not work for any service that allows for interoperability with another provider (such as email).

  However, we are very concerned to note that this is not reflected in **Article 6** (see paragraph 3 (b)). As per the above, all party consent requirements – especially given the lack of alternatives in the current text – would *de facto* outlaw emails or other interoperable services.

- We also note that **Article 6** does not recognise that processing is required to provide the service requested by the user, and not just for transmission. Thus, the same language as is currently proposed in **Article 8 paragraph 1 (c)** should be included in Article 6(1).

- We also take note of the discussions related to child safety, terrorism and other issues which can be potentially impacted by the Regulation. Under the GDPR, companies can deal with these questions through the other available legal bases, such as legitimate interest and legal obligation. These legal bases should be considered here as well. We should not underestimate how legitimate interest can allow for dealing with unpredictable future challenges and changes.

- The suggested consent requirement for employees in **Recital 19b** seems to be at odds with the GDPR, as the latter is sceptical as to whether consent in this context can be valid. A 'one-off' consent for businesses subscribing to electronic communication services is not mentioned in this recital, as a definition and a legal description of the improvements for legal persons is missing. On the contrary, the recital makes it very clear that companies are now completely dependent on the consent of their employees for any electronic communication service or software/app update in relation to work phones, tablets or connected machines.

Emergency calls, incoming call blocking and publicly available directories

We continue to believe that provisions in **Articles 13 and 14** are historic elements that are no longer relevant in today's context. They relate to commercial practices and consumer protection rather than privacy or security. If they remain relevant, they would be better addressed under the telecoms regulatory framework.

In particular, we are concerned that the reference to 'publicly available' has been deleted in **Article 13 paragraph 1**, and **Article 15 in paragraphs 1, 2 and 3**.

Terminal equipment data

We welcome the suggested change of the title in **Article 8**. We would like to reiterate our call for a principle-based and technology-neutral legislation. While we appreciate more flexibility, **Articles 8 and 10** will have a broader impact than just on cookies and browsers. This needs to be taken into account when defining the wording. With that in mind we welcome additional exceptions which have been added in Article 8 related to software updates, emergency communication and statistics. In particular:

- Website analytics are critical to understand how a website is performing and to upgrade the users' experience by improving features and tools. As companies often outsource this service by contracting external parties, prohibiting web audience management by third parties would create asymmetry and affect the level-playing field now in place. We therefore welcome the the introduction of web audience measurement by third parties among the exceptions listed under **Article 8 paragraph 1 (d)**. In our amendment proposals, we have suggested the following solution:

  Article 8 (1) (d) - 'It is necessary for measurement, including reach measurement of the use of information society service for the purpose of calculating remuneration'.

  Furthermore, we take note of the fact that not all measurement services are considered as 'processors'. Therefore, reference to Article 26 of the GDPR should also be added to the text.

- The change made in **Article 8 paragraph 1 (c)** to enable the use of device information for reasons other than 'information society services' is welcome. This change should be operated throughout Article 8 to acknowledge the fact that other services – including communication services – rely on the use of storage and processing capacity of a device. In addition, we welcome the deletion of **Recitals 23 and 24** to ensure a technology-neutral legislation.

- We welcome changes that recognise the importance of the advertisement-funded business model. Indeed, monetisation is a necessary component for any commercial service and should be recognised as such.

- Finally, whilst we welcome the deletion of **Article 10**, we suggest also deleting **Recital 20(a)** 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. We therefore encourage the legislators to adopt a more principle-based and less prescriptive approach in order to avoid solutions that work today but might become ineffective in several years as the technology will evolve.

Direct marketing communications

A new provision in **Article 16 paragraph 2 (a)** allows Member States to set a time limit for using customers' contact details for direct marketing. Furthermore, **Article 16 paragraph 3 (a)** allows Member States to require certain prefix or code for direct marketing calls.

We are concerned that these provisions may cause fragmentation of the Digital Single Market and will be contrary to the choice and nature of this Regulation that intendeds to avoid divergent implementation at a national level and ensure legal certainty across Europe.

Law enforcement access

AmCham EU regrets the broad and substantial caveats included in **Article 11**. In addition to the flexibility granted in the Commission's proposal for Member States to restrict the obligations and rights included in the Regulation, the Presidency text allows for the possibility of imposing data retention on providers in **Article 11 paragraph 2**. This contradicts the EU's objective of harmonisation and the goal of the on-going discussions on the e-evidence package. Clear safeguards and procedures are required for law enforcement for electronic evidence.

Furthermore, if **Article 11 paragraph 2** should at all stay in the text, it should very clearly reference the e-evidence framework as the legislation outlining the obligation on service providers. The same is true for the corresponding **Recital 26**.