EDiMA

Proposed ePrivacy Regulation: Still many unresolved issues

Despite the progress achieved so far during Council discussions, there are still considerable unresolved issues that need further work and consideration to make sure companies understand their legal obligations and can comply with the law. EDiMA encourages Council negotiators to consider more ambitious changes and a restructuring of this file.

General observation: The provisions of the text are not aligned

A number of articles in the text are not harmonized and contain not only a different set of legal bases but legal bases that are worded differently. **Rules need to be clear, understandable and consistent** - particularly when they are associated with a 4% annual worldwide turnover sanction.

Here is a short case study of typical user activity that can present huge legal complexity for the service provider(s) involved. This should be avoided.

A user gives a voice command to a device (a phone, a watch, a car…etc.) asking it to send a message to person X – that device will need to process the content of his/her voice communication (Article 6(1) and (3)) – so that it "understands" the request; using software that uses the storage and processing capacity of their device (Article 8) and most likely connects to the internet (Article 10?), which will then send the message to person X processing both metadata and content data (Article 6) which will almost certainly be considered personal data under the GDPR. Finally, the messaging services will likely to store the message for the user (Article 7).

Article 6 - additional flexibility and clarity is needed

The text needs to clarify a number of elements still while providing the necessary flexibility to accommodate the technical reality of the services being used.

Electronic communications services have to process communication content and metadata to operate and deliver their services. Article 6 must allow processing that is necessary to provide the service (the same way as Article 8, so as to create essential consistency within the law).

'All party' consent is an impossible threshold to meet for any service that allows for interoperability with others. ePrivacy should rely on one consistent consent standard for metadata, content data as well as across the EU *acquis,* by simply requiring that the "user of the provider has given his/her consent" in Article 6(1). This would again ensure consistency within the Articles of ePrivacy, but also with the GDPR. An example of where 'all party consent will not work is in simple password reset procedures a relatively simple operation for any end users. Changing a password can be useful for security reasons or simply because the password has been forgotten by the end user. While from an end user experience perspective, the operation is quite simple and fast, it implies diverse communications between machines through public communication networks. The reset request is transferred from the website/App server to a third-party solution - usually cloud-based - that converts it into a text message sent to the end user's mobile. This simple operation includes interactions between multiple machines (servers, mobile) through public communication networks. Under the ePrivacy Regulation, such an operation will be subject to multiple consent between all the servers and devices involved, thus slowing down the resetting operation and impacting the end user experience.

Furthermore, processing of **communications content** (pursuant to Article 6(3)) for general training and improvement of machine learning (ML) algorithms and other innovative features that deploy

artificial intelligence (AI) remains prohibited without the explicit consent of all users. Given the nature of these technologies, consent may not always be realistic to enable the realisation of the full advantages of AI and ML, even when all the appropriate steps are taken to anonymise and minimise data collection and processing. This is particularly problematic as the proposal – unlike GDPR – does not provide any exception for anonymous data.

The lack of flexibility in the current Article 6.3 wording fails to correspond with EU objectives and Member State strategies for AI. Product improvements, whether or not they are based on AI, are also important for any business that wants to remain viable. Currently there is no clarity as to the legal basis under which these improvements be possible, if at all. Article 6(3) should still be amended to include additional processing grounds for content that (i) as a minimum allow further processing of communication content data; and, preferably (ii) that aligns all legal bases with that of the GDPR.

Article 7 - storing email for the user should be allowed

Article 7 requires that once a communication is delivered, the provider of the electronic communication service (though seemingly not the network) needs to delete or anonymise it. As the service provider is not considered a third party under the GDPR, Article 7 creates considerable legal uncertainty on the service providers' ability to preserve communication data to the detriment of users' expectations. It has been EDIMA's long held view that service providers should be allowed to store communication data for their users, until they delete it, even after receipt - in line with their obligations under the GDPR. The text should reflect this.

Article 8 - conflict with GDPR, lack of flexibility and software updates

As Article 8 applies to any use of the processing or storage capabilities of a device, not just of communications data, it has significant conflict with GDPR. It is still unclear where each will apply, and why different grounds for processing are being required for the same data. Clarity is needed on why the definition was changed from the ePrivacy Directive, what additional activity is captured, and why GDPR is deemed insufficient protection for that activity.

As currently drafted, Article 8 of the proposed ePrivacy Regulation fails to offer the flexibility needed to take due account of end-users' expectations when navigating online or using online services. For products such as "smart home" devices to improve their range of services and functionalities, they need to connect and interact with different networks and devices such as cloud computing servers, lights, medical devices, mobile phones or smart wearables.

An exception should be added to make communication data accessible to improve the performance, knowledge and quality of services, in a fair and transparent manner towards the end-users. This exception could, and should, be subject to prior impact assessment, balancing the technological interests requiring the access and use of the communications and/or information with the related risks with respect to the confidentiality and protection of the end-user. Such an exception would not only further align the ePrivacy Regulation with the GDPR's principle-based approach, but also reduce the increasing "consent fatigue". Without such or similar exceptions, it is unclear what legal grounds a provider could use to improve a service, if any".

It is also still unclear how software updates will get delivered to the terminal equipment of end-users when Article 8 is in force, particularly if they are not exclusively for security purposes. At the very least, corresponding recitals should be amended to clarify that current software-as-a-service (SaaS) business models – which provide updates beyond and unrelated to data collection - are not disrupted. It is also entirely unrealistic to require that an update does not in any way change settings. Sometimes these

very settings may be the source of some vulnerability. The legislation should require that any update "respects" the user privacy settings. This would reflect both the objective – i.e. don't use updates to change user privacy preferences – as well as the technical realities of how updates work.

Article 8 - concrete suggestions re: the text [based on 22.02.2019 text]:

(1) The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (...)

EDiMA recommendations in bold and strike through:

(daa) it is necessary to improve the performance, knowledge and quality of services as long as the improvement respects the confidentiality of the communication of the end user

(e) it is necessary for a software updates provided that:

> (i) such update ~~is necessary for security reasons and~~ **respects** ~~does not in any way change~~ the privacy settings chosen by the end-user, **and**
>
> (ii) the end-user is informed, **as appropriate** in advance ~~each time~~ **of** an update being installed. **This may not be possible due to limitations in the user interface or lack of a user interface, or other reasons.~~, and~~**
>
> ~~**(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates.**~~

Recital 21a

(...) Consent should not be necessary either when the purpose of using the processing storage capabilities of terminal equipment is to fix security vulnerabilities and other security bugs **or to otherwise update the software (for example, to make legally-required changes, render the software more accessible, add new features or improve performance)**, provided that such updates ~~do not in any way change~~ ~~the functionality of the hardware or software or~~ **respect** the privacy settings chosen by the end-user. ~~has the possibility to postpone or turn off the automatic installation of such updates. Software updates that do not exclusively have a security purpose, for example those intended to add new features to an application or improve its performance, should not fall under this exception.~~

Article 10 - Is it really needed?

Even though the removal of Article 10 has been maintained in the latest Presidency text, questions remain about how to address the technical limitations of browsers and all other software applications in the event that it is discussed further. Browsers can successfully block cookies and can see if a cookie does not belong to a website (first vs. third party), but they do not know the purpose of specific cookies. It also remains unclear how any version of Article 10, that is still very much drafted with browsers in mind, would work for all software that connects to the Internet. In addition, there has been no discussion or proposals – or assessment – of how this might work in the vastly different mobile ecosystem. The text gives no consideration as to how this will work for consumers, for mobile platforms or developers.

Article 11 - Requires more time and consideration

In particular, the following areas need to be resolved:

(a) **Data retention:** This issue requires more discussion and debate in light of the detailed case law (*Tele 2, Breyer*) on this topic since the ePrivacy Directive came into force.

(b) **Extension of scope:** The extended definition of ECS (adopted from the EECC), together with the extra public interest grounds laid down in Article 11[1], represents a material (yet unclear) extension of surveillance powers.

(c) **Interaction with other laws:** The relationship between Article 11 and the GDPR, the Law Enforcement Directive and e-evidence rules (currently under negotiations) needs clarification.

(c) **Encryption:** The European Parliament has shown a clear preference for ECS providers to use state-of-the-art technical measures, including end-to-end encryption of electronic communications data, to guarantee the confidentiality and integrity of communications. The inherent tension between this and an extension of surveillance needs to be further discussed and resolved before talks with Parliament can advance.

[1] When compared to the ePrivacy Directive – for example, in the 'general public interest' and for inspection and regulatory functions; interception powers are not limited to cases of terrorism or serious crime.