Ecommerce Europe response to Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

Introduction

Ecommerce Europe is the united voice of the European Digital Commerce sector, representing the interests of companies selling goods and services online to consumers in Europe. Our mission is to act at EU level by engaging with policymakers to create a better regulatory framework for all e-merchants. Ecommerce Europe is a platform where our members can stay informed, exchange best practices, and define common positions on EU legislation impacting the sector.

Our members always seek to ensure a high level of compliance with the existing legal framework, while also actively contributing to ongoing debates so that improvements can be made in the field of enforcement, interpretation, and harmonisation.

With this paper, we would like to share our concerns with regards to the EDPB public consultation on Art. 5(3) of the ePrivacy Directive. E-commerce players would be among those affected by the proposed changes in interpretation of the provision and we would therefore find it important provide our own feedback on the changes impacting this provision.

Preliminary views

While the EDPB is the principal body representing privacy regulators across the EU, they are not the sole regulator when it comes to the ePrivacy Directive. Taking this into account, an Opinion or Recommendation would be a much more suitable instrument than Guidelines. The risk in this instance is that the EDPB might exceed its mandate as regulated by Art. 70 of the GDPR. The uncertainty in this instance for companies would lead to questions such as: *is another authority, not privacy regulator, bound by such guidance?*

We also understand the necessity of this text given the outdated interpretation of the ePrivacy Directive. However, proceeding in this way without considering a “GDPR” approach is not leaving room to any risk-based approach / controller accountability. The proposed interpretation of Art 5(3) might result in a rigid approach that does not reflect the current technological landscape and does not consider companies’ challenges in implementing new technologies ensuring a by design approach. Guidance broadening the scope of a single provision may cause lack of harmonisation in interpreting the Directive overall. One example is that guidance is not helping companies as to how the concept of what is “essential” would apply in this expanded world. This may create more lack of coordination and harmonisation among Member States as there would be jurisdictions giving companies more flexibility than others when it comes to exceptions (it is already happening).

The Guidelines should be accompanied by a transition period. Implementing new requirements requires an adjustment of consent mechanisms and technologies, a process that demands time and resources. Recognising this, we recommend a reasonable transition period to facilitate the implementation of new Guidelines.

Detailed assessment of the Guidelines

To begin with, we find the interpretation adopted by the EDPB regarding what constitutes "**access to**" or "**storage of**" information to be too broad. Particularly concerning is:

(i) the notion that the party instructing the terminal to send the information and the party receiving the said information can be different – i.e., bringing into scope the passive receipt of information,

(ii) the bringing into scope the ephemeral and inevitable storage of information. This, when read together with the specific use cases highlighted in the Guidelines, results in a significant widening of the scope of applicability of Art.5(3). It could capture automatic, standard, consequential and/or inevitable transmission of information, including those initiated by the users/subscribers (or their terminal equipment), which occurs simply by the virtue of how certain technology operates or how the internet functions.

(iii) the interpretation would mean that the provisions would apply to all categories of storage. It is therefore necessary to have either some degree of flexibility or possibility of assessment.

While we understand that the main intent seems to broaden application of art 5(3). This provision is easy to apply when it comes to cookies as the concept of "gaining access" refers to access information already stored in the device. However, other tracking technologies like URLs would work differently. Simply put, day-to-day activities such as loading of a webpage by a user (even if there are no ads at all on such webpage) could come under the scope of Art.5(3). In addition, expansion might lead to misalignments with existing cookies' Guidelines already issued by some Member States (e.g., Germany – see DSK guidance on Telemedia[1]).

Moreover, the EDPB interpretation of the notion of "information" may infringe upon the tasks of the EDPB as it expands a requirement to include non-personal data. This further adds to the concern that these Guidelines would fuel the **legal uncertainty**: In certain cases, the EDPB's interpretation is inconsistent with the guidance issued by the national authorities[2]. Also, the effect of the Guidelines appears to be opposite to that previously contemplated by the proposed e-Privacy Regulation (which significantly extended the list of exceptions to the requirement to seek end-users' consent to the use of cookies, as mentioned above in relation to exemptions). In any event, businesses must consider any finalised Guidelines against the plethora of regulatory developments in this area with overlapping effect (e.g. DMA).

Furthermore, we must also underline the **unclear consent requirements**. While clearly extending the scope of applicability of Art. 5(3), the Guidelines do not clarify how the requirements of Art. 5(3) can be met in practice. For example, it does not provide information on how consent requirements will be fulfilled where the instructing entity and the entity receiving information from terminal equipment are not the same, or where multiple users/subscribers use the same terminal equipment. In this sense, the Guidelines raise more questions and offer little by way of suggesting potential solutions.

[1] https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf
[2] ibid

The inclusion of technologies or tools such as tracking pixels / beacons / JavaScript is quite problematic given that the usage of such technologies should be interpreted by considering the purpose as it could be "essential". The need of consent for other tracking technologies requires specific criteria and concrete examples for every type of use case, so we request that the Guidelines include compliant use cases and practical interpretation for all the different use cases representing common techniques, as well as in light of the emergence of (new) tracking methodologies beyond cookies (e.g., tracking pixels in emails or web or for the use of Local Processing, tracking based on IP only or Unique identifier). The Guidelines should include specific use cases to inform users when providing consent, stating clear transparency requirements for the first and second layer in the case of the cookies banner and with a practical approach in the rest of use cases.

While it is clear that ePrivacy Directive does not apply where using CGNAT (It groups a number of subscribers under the same public IP address, the interpretation of the Guidelines on IP addresses does not consider modern technologies ensuring anonymisation of IP addresses upon collection. We consider this to not be a pragmatic approach. If an IP address is collected and immediately anonymised before any other usage, then this should be considered in some way.

The Guidelines lack a **list of exemptions** despite the proposed expanded scope. There is no indication of any additional exemptions being introduced. Moreover, there is also no indication of how the existing exemptions would apply to scenarios that are now brought into scope in light of the new Guidelines (e.g., in respect of information that is generated/stored by default in the terminal equipment and are transient in nature, such as RAM or CPU cache). It is worth noting that, the previously proposed e-Privacy Regulation significantly extended the list of exceptions to the requirement to seek end-users' consent to the use of cookies (e.g., cookies for audience measurement, cookies necessary for security purposes or software updates, cookies that enable users to log into secure areas of a website, use a shopping card or use e-billing services). The proposed Guidelines have the opposite effect. We consider important that the list of approved exemptions to consent across Member States is harmonised, notably with regards to the use of analytics for aggregate and anonymous statistics.

Overall, the effect of the Guidelines is that it would **make consent fatigue worse**. The Guidelines are strictly applied, users/subscribers will receive consent request for each such transmission now in scope, resulting in them receiving an overwhelming number of consent requests, to a level they likely have never expected. This conflicts with the underlying objective of the EC's ongoing effort to develop Cookies Pledging Principles to reduce fatigue of the users. Furthermore, the ambiguity of the Guidelines (e.g., where it is unclear whether any exemptions would apply or who exactly needs to provide the information and request consent), organisations are likely to take a conservative approach and request consent in any case. This will exacerbate the issue, with even more consent being requested from users/subscribers.

Finally, we underline that the Guidelines are **not proportionate**. The broad interpretation of the EDPB seems disproportionate given the objective of the ePrivacy Directive. It arguably does not align with the spirit of Recital 24 of the ePrivacy Directive which suggests that the objective (or at least the requirement for users' consent under Art.5(3)) is to protect the users' terminal equipment from "active" intrusion that occurs "without their knowledge", that "seriously intrudes" upon their privacy).