Renault Group

Renault Group comments on the EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

Executive Summary

The clarifications proposed by the EDPB are most welcomed and very useful. The guidelines provide a unique opportunity to clarify when the consent required by ePrivacy is applicable to data collected from vehicles.

However, little insights are provided regarding the notion of "public" network, even though it is a condition for the ePrivacy Directive application.

What criteria qualify the network used to access vehicle data as private or public?

Renault Group welcomes the publication of the EDPB draft guidelines on the technical scope of article 5(3) of the ePrivacy Directive.

Given its scope of application and the Directive is almost as important as the GDPR for some businesses, in a way that was not foreseen by the European legislator in 2009.

Even though the article 5(3) of the directive was originally meant to protect web users from spywares, web bugs, or hidden identifiers, Europeans Data Protection Authorities – DPAs - have extended its scope of application to a wide range of use cases, by virtue of a strict interpretation of the letter of the law.

While this position of the DPAs is fully understandable, it appears detrimental for some businesses since the work of the European legislator on ePrivacy regulation has completely stopped, even though this regulation could enhance the interplay between the GDPR and the principles of ePrivacy and allow the necessary evolutions that businesses and regulators have both called for.

In this context, it appears all the most important for companies to obtain legal certainty on the technical scope of application of the ePrivacy directive, to make sure that they apply its principle only when strictly required by the law.

In this respect, the clarifications proposed by the EDPB are most welcomed and very useful. The 4 criteria detailed by the EDPB in its guidelines allow business to conduct a step-by-step analysis in order to identify if the article 5(3) is applicable.

However, very little insights are provided regarding the notion of "public" network and services. As recalled in the guidelines, article 5(3) is applicable only when "the operations carried out are made in the context of the 'provision of **publicly** available electronic communications services in **public** communications networks'" (emphasized added).

Paragraph 25 only indicates that in order for the previous criteria to be fulfilled the communication service has to be public, and that "the fact that the network is made available to a limited subset of the public (for example, subscribers, whether paying or not, subject to eligibility conditions) does not make such a network private", without explaining why, on which legal basis and more importantly, without specifying the criteria that would qualify a network as "public". This part of the draft guidelines would deserve more clarity on how to, in practice, determine if an operation which meets the other criteria identified by the EDPB is actually performed in the context of the provision of publicly available electronic communications services in public communications networks, considering the previous statements already released on this topic by Data Protection Authorities.

Renault Group

For example, according to the EDPB[1]and to the French DPA[2], the internal network of a company is not considered as a public network but a private network, and therefore, any operation meeting the other criteria will not fall under the scope of article 5(3). This seems to indicate that, in some cases, the fact that the network is made available to a limited subset of the public (in this case the employees and the contractors of the company) does not make it public.

The French DPA[3], as well as the UK DPA[4] also indicates that the use of a virtual private network between a computer and the internal network of a company is considered to be private, even though the computer is connected to the Internet through a public communication service offered through a public communication network.

Lastly, the EDPS indicated in its Preliminary EDPS Opinion on the review of the ePrivacy Directive (Opinion 5/2016, page 12) the "*rising importance of the mixed (private/public) and private networks in everyday life*" justifies expanding in the future regulation the scope of the ePrivacy directive to cover those networks, meaning that they are, as of now, not covered by the ePrivacy Directive in force since 2009.

The draft guidelines subject to the present public consultation aim at removing "*ambiguities related to the application*" of the ePrivacy. As a consequence, it is a unique opportunity for DPAs to remedy the obvious lack of clarity on this subject and develop in further details the Criterion C of the guidelines to explain why the previous examples are considered as private and not public and provide practical guidance as to how to identify the nature (public or private) of a network.

To provide food for thoughts and secure our understanding of the DPAs interpretation, we have identified the following questions that remain unsolved after reading the guidelines and whose answers are necessary to provide legal certainty for the development of connected vehicles and many other connected products:

- Is an electronic communication service only accessible to companies from a specific sector, for example car manufacturers, considered as public?
- Does the use of a specific Access Point Name - APN - provided by a provider of telecommunication network and accessible only by a single company and connected to its core network qualify the data transmitted by the APN as being conveyed over a private network?
- Are connected vehicles connected to the core network of a car manufacturer by a virtual private network considered as exchanging data over a private network?
- Can the Transport Layer Security - TLS - connection between a connected vehicle and the core network of the car manufacturer be considered as a private network?
- Is it possible to identify the precise layer of the OSI model at which the Virtual Private Network - VPN - should operate in order to be able to consider that the VPN does indeed create a private network?
- Does the type of technology used by the VPN play a role in the determination of the nature of the network?

Those questions are critical for companies to understand to which legal obligation they must abide and have not been discussed by the previous EDPB guidelines[5] which consider that the use case they analyze implies

[1] See https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf paragraph 27

[2] See the seventh question of the cookies FAQ: https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/FAQ.

[3] See previous reference.

[4] See https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/#rules12.

[5] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, Guidelines 02/2021 on virtual voice assistants, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities

the use of a terminal in the sense of the ePrivacy directive, but without extending the analysis to the nature of the network used.

Hopefully the future ePrivacy regulation would allow the text to be clarified in the light of the new technologies that have been developed over the last 15 years, to rationalize its scope of application and refocus it on the spirit of the text, i.e., to prevent third parties, who are not involved in the operation of supplying electronic communications, from intruding on users' terminals.

In the meantime, and while regulators continue to strictly apply the letter of law, companies deserve to obtain legal certainty on all the aspects which trigger the application of the directive.