Submission to the public consultation on the Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive of the European Data Protection Board – Federazione Concessionarie Pubblicità (hereinafter "FCP")

***

FCP – Federazione Concessionarie Pubblicità, is the Association that, since 1951, brings together the best skills and experiences in the world of Italian advertising. FCP includes the most important companies and sales houses that operate in the field of the sale of advertising spaces on the main media: newspapers, magazines, television, radio, Internet, cinema, Gotv. FCP is delighted to provide feedback to the current debate around the European Data Protection Board ("**EDPB** or the **Board**") Guidelines 2/2023 on Technical Scope of Art. 5(3) of the ePrivacy Directive ("**Guidelines**").

1. Preliminary remarks.

During its twenty years of life, the ePrivacy Directive has proved to be able to face the challenges posed by the fast-paced technological environment and the rise of new forms of advertising. Nevertheless, it is unquestionable that there is a need for a review of the current regulatory framework, which is being addressed at the EU level with the upcoming ePrivacy Regulation. The ePrivacy Regulation will provide new rules for several current state-of-art technologies, such as metadata or other forms of communication, such as WhatsApp.

In such a fast-changing environment, the regulators' role becomes crucial in balancing the need to foster technological evolution as a business growth driver and protect EU citizens' personal sphere. Also, particular emphasis should be placed on preserving a level playing field, ensuring no direct or indirect discrimination occurs among players in the industry.

In light of the above, FCP believes that EU Authorities should be cautious in releasing their initiatives and guidelines, as interpretations can have far-reaching consequences, seeking to strike a balance between fairness and market dynamics. Such initiative and guidelines, if not well-calibrated, can give rise to detrimental unintended consequences and may introduce challenges, distortions or inequities into the digital industry.

2. FCP's position on the Guidelines.

As stated by the Board, the Guidelines focus on the applicability of Art. 5(3) of the ePrivacy Directive to emerging technical solutions to clarify certain aspects of such solutions in order to determine whether Art. 5(3) applies to them. In addition to that, the Guidelines focus on a non-exhaustive list of use cases, such as "*URL and pixel tracking*", "*Local processing* ", "*Tracking based on IP only*", "*Intermittent and mediated Internet of Things (IoT) reporting*", and "*Unique Identifier*".

While FCP welcomes the initiative of providing further guidance on the intricacies stemming from the Directive and aligning it with the current technological landscape, FCP would like to take the opportunity granted through this public consultation to submit some technic and economic considerations that need to be addressed.

The aim of this paper is to comment on whether the interpretation given by the Board on the technical scope of Art. 5(3) of the ePrivacy Directive (i) is consistent with the spirit of the Directive; (ii) may cause unintended consequences for the advertising market, and (iii) can disrupt the online advertising market.

3. The risks of broadening definitions.

The Guidelines provide an extended definition of the concepts of "*gaining access*" (to information), "*storage*" or "*stored*", respectively in paragraphs 26 to 33 and 34 to 39. It is FCP's concern that this broader interpretation may extend beyond the original intent of the EU legislator and that its potential ramifications may include unintended consequences affecting digital services providers and users alike.

A. Extension beyond the original intent of the EU Legislator.

- **Broader notion of "*gaining access*":** Paragraphs 29, 30 and 31 of the Guidelines clarify that (i) the storage and access (i) do not need to occur cumulatively, and (ii) do not need to be carried out by the same entity in order for Art. 5(3) to apply (see WP29 Opinion 9/2014). In the view of the Board, this implies that there are no restrictions on the origin of information on the terminal equipment for the notion of "access" to apply. Moreover, the Board believes that Article 5(3) would also apply when the accessing entity actively takes steps to gain access to information stored in the terminal equipment, which typically involves the accessing entity proactively sending specific instructions to the terminal equipment to receive back targeted information (the example given is for cookies, where the accessing entity instructs the terminal equipment to send information on each subsequent HTTP call proactively).

- In FCP's view, the interpretation of the notion of "*gaining of access*" **should exclude the passive receiving of information required for the transmission of communications**.

  The interpretation transposed in the Guidelines cannot have been the intent of the EU legislator, who specifically chose the term "*gaining access*". The word "*access*" inherently indicates an active movement, unlike the passive verb "*to receive*". The active nature of "*access*" is corroborated by the language of Recital 24 ePrivacy Directive, which only describes the act of "*entering the user's terminal without their knowledge*" ("*entering*" also implying active movement). The ePrivacy Directive never employs broader, passive wording to describe gaining access (for instance, it could have used the word "*receive*" or could have included an example about remote monitoring of server logs). In addition, Recital 24 ePrivacy Directive emphasizes that the information regulated for access and storage is "*part of the private sphere of users*", a concept that seems fundamentally incompatible with extending that scope to encompass information that has already left the private sphere of users due to its automatic transmission via the Transmission Control Protocol (hereinafter, "**TCP**").

  In an attempt to exemplify FCP's view, we can take the HTML functions as an example of the challenges posed by such an interpretation (from now on, we will refer to this as the "**HTML scenario**"). Following the interpretation given in the Guidelines, whenever a server places pixels on a webpage, even though these are only triggering actions without directly retrieving user information from the display of the browser, it would still constitute access to information. In fact, in the interpretation of the Board, the instructions exchanged between the server and the

webpage, would involve the server "*gaining access*", even though such access only refers to its own instructions without any active role played by the accessing entity nor access to the users' private sphere, due to the automatic transmission via the TCP.

- **Broader notion of "s*tored information*" and "s*torage*":** With regards to the concept of "*storage*", the Guidelines seems not to properly differentiate between merely technical operations that are tied to the inner functioning of the communication technology and storage activities deliberately undertaken by the operator managing such technology to collect the end user's information. A first consideration that should be taken into account is whether such a "*technical storage*", with no other purpose than letting the communication taking place, can legitimately be considered as falling within the broader scope of Art. 5(3). In the HTML scenario, for example, according to the interpretation of the Board, the server is not only gaining access to the information, but also storing such information. While it is reasonable to recognize that the activity of the HTML may involve storage in memory (as a technical consequence of the functioning of the protocol), the interpretation given by the Board of both "access" and "storage" would make such storage subject to Art. 5(3) and may raise concerns as to whether such an interpretation really reflects the original aim of the ePrivacy Directive.

- **Passive *vs* Active:** In FCP's view, the interpretation of the notion of "*gaining access*" and "*storage*" should exclude the passive receiving of information required for the transmission of communications. This narrow interpretation would better align with the ePrivacy Directive's first objective of protecting the private sphere of users, particularly in scenarios where there is an active action to gain access to the user's terminal. FCP firmly believes it is crucial to balance the protection of the private sphere of the users, which has to be guaranteed, and the practices of web interactions, ensuring that the regulatory framework remains effective and user-friendly to avoid the consequences described below.

B. The unintended consequences

- **Increase of consent fatigue for users:** The main conclusion that can be drawn from the Guidelines is that if a technology falls under the scope of Art 5(3), as interpreted above, then the company deploying that technology must obtain in advance, *opt-in* consent before accessing or storing the information, unless it can be demonstrated that the storage of, or access to, the information is strictly necessary for the purpose of "*carrying out or facilitating the transmission of a communication over an electronic communications network, or is strictly necessary in order to provide an information society service explicitly requested by the subscriber or use*". It is worth to say that this does not consistently happen in practice, and obtaining consent may also be difficult, depending on the context in which the technology is used. FCP stresses that the unintended consequences of this interpretation would bring to detrimental effects on both service providers and users. Considering users, the HTML scenario reveals that the majority of the users' activities on a web pages could be subject to the application of Art 5(3) since the consent could be necessary. From the user's perspective, the so-called "*consent fatigue*' issue emerges in a reality where users are already heavily stressed by cookie consent banners. Given this scenario, it would be arguable whether increasing the instances where transmission of information requires consent would equally increase the overall level of protection of the users and this approach may even weaken the role of consent

increasing the stress and the pressure on users and transforming the user consent into an instrument to block any kind of electronic communication and advertising (i.e. "adblocker"), without any reason effectively related to the protection of user's privacy.

- **Disruptive impact on the market, our survey:** In onder to provide a better understanding of the effects driven by the application of Art. 5(3) as interpreted by the Board in the Guidelines, FCP has done a preliminary analysis to evaluete the potential impact of consent requests within the scope of our Federation's member concessionaires. The results of this estimate appear to be drastically disruptive, with economic losses estimated for 2024 equal to 20 per cent of the aggregate turnover of the FCP's members compared to 2023. In FCP's view, this forcasted scenario appears very critical, in particular considering also that (please see the following study made by IAB Europe, https://iabeurope.eu/the-value-of-digital-advertising/):

  - digital advertising is undoubtedly the main revenue source for the industry, representing 81.5% of publisher revenues in the EU and 51.9% of the revenues for online video platforms;
  - in total, digital advertising adds 526 billion Euros to the EU economy each year;
  - thanks to digital advertising, 68% of Europeans have never paid to access websites, online news or core internet services like mail;
  - 69% of Europeans are willing for their browsing data to be shared for advertising in order to access digital content such as news articles and online videos for free;
  - 80% of internet users prefer free sites with ads to paying for content.

- **Open web disruptive consequences: potential consolidation of market concentration in favor of big-techs and/or rise of paywalls:** Advertising relies heavily on data collection, primarily to provide users with personalized recommendations and content, ensuring that the advertisements presented are more likely to align with their interests while sustaining the availability of the services they use free of charge. While the aforementioned data suggests a marked inclination of users to share their browsing data so as to continue using online services for free, FCP considers it reasonable to assume that the strict enforcement of Art.5(3) as interpreted in these Guidelines, and the consequent significant decline in the industry revenue our survey reports, is highly likely to result in equally open-web disruptive phenomena, namely:

  1. **Big-tech and Walled-garden benefits**: the diminished capacity arising from the financial constraints imposed by reduced revenue streams limits investments in content creation, innovation, and service improvement. The consequent reduced overall quality of the service brings with it the further consolidation of market concentration in favor of so-called "*big-techs*", whose vast resources and *walled garden* structures may only benefit from the weakening of the player of the open web. In order to better understand how strong the position of these giants already is in Italy, according to the study of the Politecnico di Milano (please see https://www.osservatori.net/it/home), in 2022 the advertising market in Italy reached a total value of € 9.4 billion with a further increase in the internet media share compared to what was observed in the previous year. This trend, which has been progressing for years now, is also confirmed by the Politecnico di Milano forecast for the 2023 advertising market closing, according to which a total market of € 9.8 billion is expected with a share of the digital component equal to 49%. In the given context, the steadily growing trend of "*big-techs*" is clear

and it represents the 81% of the total Digital market and the 40% of the total advertising market in Italy (source: Politecnico di Milano at the latest edition of the Internet Media Observatory). The outcome of such scenario leads to a loss of resources and to a decrease of the potential of the open web and can improve the supremacy of the big tech giants (i.e. "walled garden").

2. **Rise of paywalls**: to avoid the scenario above, service providers may find themselves obliged to adopt alternative revenue models, potentially leading to limitations on free access and the introduction of paid subscriptions and/or paywalls. This scenario limits the potential and capabilities of the open web just as well, providing end users with higher costs to exploit the same services, and does not exclude the walled garden effect, which may take place just as well.

3. **Risks for the open web**: Ultimately, a significant decline in the industry revenue not only jeopardises the stability of the sector but also carries the risk of diminishing the so-called open web, impacting both users and service providers alike. In fact, this scenario may lead to disruptive consequences, such as a decrease in the quality of the services offered to end users and in the bolstering of the supremacy of the so-called "*big tech*".

4. Interpretative and technical comments regarding paragraph 3.3 "Tracking based on IP only" of the Guidelines

Given and considered all the foregoing, a final point that FCP considers worthy of being addressed concerns paragraph 3.3 of the Guidelines, which (in emphasizing the tracking of the user by advertising solutions that rely on the collection of IP address only) states "*advertising solutions that only rely on the collection of one component, namely the IP address, in order to track the navigation of the user, in some cases across multiple domains*". While the meaning of "*tracking*" is not explicitly defined in the ePrivacy Directive, its literal meaning is generally understood to encompass the collection, storage, and analysis of user data to create a profile of their online behavior. FCP, on the other hand, would like to point out the existence of advertising solutions that involve the realtime processing of the IP address, without subsequent archiving/storage of the same, or collection, which in no way offers the possibility to track and profile users. These solutions represent an essential tool offered to publishers and their advertising sales houses to maintain free access to content on websites, mobile apps, and for CTV, representing a form of economic support for the exercise of the business model. The interest in delivering general digital advertising messages is to be considered legitimate also as it is instrumental to guarantee the exercise of the freedom of enterprise, a fundamental right recognized by Article 16 of the Charter of Fundamental Rights of the European Union. Where the relevant operators adopt advertising solutions that are technically capable of excluding user profiling, IP archiving/storage, and, above all, user tracking, Article 5(3) ePrivacy Directive should not be considered applicable, regardless of whether or not it is possible to ensure that the IP originates from the user/subscriber terminal or not, as they can reach their objective to deliver advertising while matching the ePrivacy Directive's first objective to protect the private sphere of users. However, if it remains confirmed - as stated in this passage of the Guidelines - that the use of any advertising solution that makes an instant reading of the IP address still falls within the scope of application of Article 5(3) ePrivacy Directive, the direct consequence will be to reaffirm the concept that consent will have the typical and direct purpose of an adblocker as portraited above.

Moreover, recital 24 of the ePrivacy Directive suggests that the objective of the Directive is quite different, where it recites "*The terminal equipment of users of electronic communications networks and any information stored in such equipment form part of the private sphere of the user, which must be protected under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, invisible bugs ("web bugs"), hidden identifiers and other similar devices may be introduced into the user's terminal without their knowledge in order to have access to information, store hidden information or track the user's activities and may constitute a serious intrusion into the privacy of such user. The use of such devices should be permitted only for legitimate purposes and the user concerned should be aware of it".*

Putting on the same level different situations such as the introduction of spyware, web bugs, and hidden identifiers with others in which there is an instant reading, for example, to an IP address (which is also an essential element for the technical functioning of the communication itself) for the sending of a general advertising message, without any tracking purpose of the user, in FCP's view does not appear in any way reasonable remaining arguable whether such a broad approach was in the legislator's intentions, as the wording used appears to indicate otherwise. If such association between spyware and reading the IP address were to be confirmed in the Guidelines, the consequence would be to create the belief that users' terminals must be protected from the delivery of any advertising message, even if general/contextual (and therefore non-profiled) and in general from any type of electronic communication since the IP does represent the fundamental basis of the TCP/IP protocol.

The paradox that would arise, therefore, is that general, non-profiled advertising (a) in the context of devices connected to the Internet, would be subject to the prior consent of the user, further exacerbating the consent-fatigue phenomenon and (b) in the world of traditional media (i.e. excluded from the scope of ePrivacy Directive), could, on the other hand, continue to be delivered without any consent requirement. In fact, general advertising would (1) represent a risk for the privacy of users in the context of electronic communications, (2) be completely irrelevant with respect to the privacy of users outside the context of electronic communications.

It is also relevant to stress how the IP address is essential for any type of electronic communication. In the context of the TCP/IP protocol, the source and destination IP addresses are always present (source = IP of the user's client; destination = IP of the Ad Server). Reading the IP address is functional to electronic communication without assuming or including any tracking activity (regardless of the type of IP address considered: IPv4 or IPv6). In the context of any advertising solution that makes an instant reading of the IP address, the trigger that activates the entire chain is given by an Ad Server component (Software Development Kit, "*SDK*" or direct browser call) that is called by the user's client at the time of content viewing. In the absence of consent, any advertising solution that makes an instant reading of the IP address can respect the choice of the user delivering advertising without any tracking or profiling activity. Storing of the IP address or subsequent tracking activities are not involved. This dynamic could therefore lead to the exclusion, as far as FCP is concerned, of the applicability of paragraph 3.3 "*Tracking based on IP only*" (unless real-time management, without the storing of any data, is included in the concept of tracking). The fact that the IP address must be verified to originate from the user's device assumes the technical and legal possibility of being able to access this information in advance (therefore, access would still be necessary regardless of any expression of user consent). Even imagining that it could be possible to proceed in this way, it is an information currently in the possession only of internet providers that is not intercepted or manageable by the typical tools of digital advertising (such as Ad Servers or SSPs), nor

it should be as it will become unproportionate with respect to the goals set for ourselves of respecting the privacy of users.

5. Conclusions.

Considering all the above, while the Board's efforts to enhance protection and align regulations with contemporary trends in technology are commendable, FCP believes that the current interpretation of Art. 5(3) enshrined in the Guidelines may produce the opposite effect. What appears to be more striking is that the potential introduction of economic losses for digital service providers as highlighted above, can decrease the potential of the so called "open web", improve the supremacy of the big tech giants and, at the same time, is not counterbalanced by an enhancement of the user's protection under the current EU data protection framework (it should be noted that the ePrivacy Directive entered into effect in most of the EU Member States at a time in which comprehensive regulatory instruments - above all, Regulation 679/2016 (GDPR) – were not still effective). On the opposite, FCP reinforces that the "*consent fatigue*" phenomenon will likely affect the users' experience, exacerbated by additional burdens, and it turns the user consent into an instrument to block any kind of electronic communication and advertising (i.e. "adblocker"), without any reason effectively related to the protection of user's privacy. The final (and rather worrying) outcome, therefore, is represented by the potential increase of the market concentration in favor of the "tech giants" and the potential decrease of the potential of the Publishers and the Sales Houses of the open web.

FCP's conclusions emphasize the importance of achieving a delicate balance between regulation and economic initiatives. Guidelines and the interpretations therein should adapt to the dynamic digital landscape and consider the practical implications for service providers. Reaching this balance is fundamental to prevent any economic repercussions and to reinforce the user security in an effective and sustainable manner for all the stakeholders involved.