Friday, 17 May 2019

Re: Conditionality of access to ad-funded services on consent in the ePrivacy Regulation

We are writing to express our significant concern about the tentative positions reached by Member State delegations in WP TELE over the last few months on Article 8(1) of the ePrivacy Regulation ("**ePR**") and related Recitals 20-20(a) ePR. We, the undersigned, are associations who represent stakeholders in the online media and advertising sector. Our members include: (i) **publishers** who create content and services that are wholly or partially funded by the sale of advertising and made available to EU citizens at little or no cost; (ii) **advertisers** who ultimately fund content and services through their purchase of advertising inventory sold by publishers; and (iii) **agencies and technology companies** who act as intermediaries and service providers to publishers and advertisers to facilitate the effective and efficient sale, purchase and measurement of advertising online.

We are alarmed by the prospect of the ePR effectively making it illegal for publishers and other online services to make access to their services conditional on consent for the storage and/or access of information on a user's device that is necessary for online advertising that wholly or partially funds their services. We strongly believe that providers offering a free service should be allowed to determine the conditions under which this service can be accessed.

As currently drafted, the ePR (like its predecessor, the ePrivacy Directive ("ePD")) will require consent for virtually *all* storage and/or access to information on a device that occurs in the course of online advertising under Article 8(1) ePR. With the notable exception of storing and/or accessing information on a user's device for the purposes of security and fraud prevention, other exceptions of Article 8(1) ePR are either not applicable or, in the case of the audience measurement exception, scoped too narrowly for real life use cases. Moreover, to address the often-cited argument that online advertising is possible without storing and/or accessing information on a user's device, we would like to submit that any such advertising would bring in significantly less revenue for publishers and other ad-funded services.[1]

While Article 8(1) ePR maintains the consent-centricity of its predecessor Article 5(3) ePD, neither the European Commission's proposal of the ePR, the European Parliament's position on the ePR, nor the Council of the EU's current draft of the ePR, include Recital 25 ePD's critical clarification that access to content may be made conditional on consent for cookies (et al.). We are highly appreciative of Member State delegations' recognition that "[i]n some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service [...] that is wholly or mainly funded by advertising [and has in addition been provided with] information about the purposes [...] of cookies and similar techniques and has accepted such use."[2]

However, we feel that such language is not strong enough, not only on the basis of strategic considerations for the Council of the EU's trilogue negotiations with the European Parliament, which has taken the strict position of asking for a prohibition against services making access to their services conditional on consent,

[1] We have attached to this letter in Annex II for your consideration an overview of the various purposes for which our industry processes personal data (subject to GDPR), and for which it stores and/or accesses information, such as pseudonymous cookie or device identifiers, from users' devices (subject to ePrivacy rules).

[2] Recital 20, Revised ePrivacy Text Romanian Presidency of the Council of the EU (Document 7099/19, 13 March 2019).

but also in light of non-exhaustive suggestions introduced by the Austrian Presidency in Recital 20 ePR that state that making access to a service conditional on the user agreeing to the storing and/or accessing of information on their device for advertising purposes is likely to be limited to situations where "the end-user is able to choose between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes on the other hand."[3]

The rigorous application of the GDPR by supervisory authorities makes it clear that industry needs strong, unambiguous legal presumptions in favour of online services being allowed to make access to their ad-funded content conditional on consent to storing and/or accessing information on users' devices for advertising purposes. Real life experience shows that Article 7(4) GDPR, which in itself is the outcome of a compromise in trilogues between the European Parliament's strict position in favour of an outright prohibition and the Council of the EU's equally strong position that there should be no prohibition, is being interpreted by supervisory authorities as though the European Parliament's prohibition made it into law anyway. For example, the EDPB's opinion states that "[...] consent cannot be considered as freely given if a controller argues that a choice exists between its service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by a different controller on the other hand,"[4] even though the GDPR merely lays out some practices to consider when determining whether consent is freely given without generally prohibiting them. Most recently, the Dutch supervisory authority also issued a warning to Dutch publishers stating that so-called cookie walls are prohibited under GDPR.

We are strongly opposed to the adoption of a General Approach unless it features strong, unequivocal support for the right of publishers and other ad-funded online services to make access to their content and services conditional on consent for storing and/or accessing information on user devices for advertising purposes. We have attached for your consideration **proposed amendments** to Recitals 20-20a of the Council's ePR text that would make us feel more comfortable with the proposed ePR.

In addition, we are concerned about the latest language introduced by the Romanian Presidency in Recital 20a ePR that encourages browsers and other software enabling access to the Internet to act as gatekeepers.[5] When browsers and other software act as gatekeepers, they undermine the ability of publishers and other online services to have a direct dialog with users about privacy and choice on their services. This is particularly concerning to us, as many developers of such browsers and other software are also competitors of the very same publishers and online services vis-a-vis whom they act as gatekeepers.

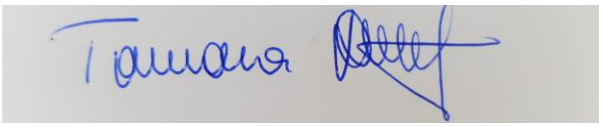
We kindly request a joint meeting with you at your earliest convenience to discuss these matters in person.

Kind regards,

[3] Recital 20, Revised ePrivacy Text Romanian Presidency of the Council of the EU (Document 7099/19, 13 March 2019).

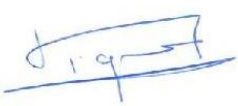
[4] EDPB Guidelines on consent under Regulation 2016/679 (Document WP259 rev.01, Revised and Adopted on 10 April 2018), p. 8.

[5] Recital 20a, Revised ePrivacy Text Romanian Presidency of the Council of the EU (Document 7099/19, 13 March 2019).



Tamara Daltroff, Director General, European Association of Communication Agencies

Townsend Feehan, Chief Executive Officer, Interactive Advertising Bureau Europe



Mathilde Fiquet, Director General, Federation of European Direct and Interactive Marketing

Angela Mills Wade, Executive Director, European Publishers Council

Conor Murray, Regulatory & Public Affairs Director, Association of TV & Radio Sales Houses

Wout van Wijk, Executive Director, News Media Europe

Annex I - Proposed AMENDMENTS to the Romanian Presidency ePR text

Recital 20

Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is ~~stored in~~ **processed by** or emitted by or **stored in** such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere, **including the privacy of one's communications,** of the end-users requiring protection under the Charter of Fundamental Rights of the European Union ~~and the European Convention for the Protection of Human Rights and Fundamental Freedoms~~. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users. Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and or for specific and transparent purposes.

The responsibility for obtaining consent for the storage of a cookie or similar identifier lies on the entity that makes use of processing and storage capabilities of terminal equipment or collects information from end-users' terminal equipment, such as an information society service provider or ad network provider. Such entities may request another party to obtain consent on their behalf. The end-user's consent to storage of a cookie or similar identifier may also entail consent for the subsequent readings of the cookie in the context of a revisit to the same website domain initially visited by the end-user. ~~Access to specific website content may still be made conditional on the consent to the storage of a cookie or similar identifier.~~

~~**Not all cookies are needed in relation to the purpose of the provision of the website service. Some are used to provide for additional benefits for the website operator.**~~ **Making access to the website content provided without direct monetary payment conditional to the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered disproportionate** ~~**in particular**~~ **inter alia if an information society service, requested by the end-user, is wholly or mainly financed by advertising, or if the end-user is able to choose between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes on the other hand. Conversely, in some cases, making access to website content conditional to consent to the use of such cookies may be considered to be disproportionate. This would normally be the case for websites providing certain services, such as those provided by public authorities, where the user could be seen as having few or no other options but to use the service, and thus having no real choice as to the usage of cookies.**

Recital 20a

End-users are ~~increasingly~~ often requested to provide consent to the storage and access to stored data in their terminal equipment, due to the ubiquitous use of tracking cookies and similar tracking technologies. As a result, end-users ~~are~~ may be overloaded with requests to provide consent, ~~leading to what has been can be referred to as 'consent fatigue'~~. This can lead to a situation where consent request information is no longer read and the protection offered by consent is undermined. Implementation of technical means in electronic communications software to provide specific and informed consent through transparent and user-friendly settings, can be useful to address this problem issue. Where available and technically feasible, an end user may therefore grant, through software settings, consent to a specific provider for the use of processing and storage capabilities of his or her terminal equipment for one or multiple specific purposes across one or more specific services of that provider. ~~Such consent can be given to several providers for specific purposes.~~For example, an end user can give consent to the use of ~~all or~~ certain types of cookies by whitelisting one or several providers for their specified purposes. ~~To that end, web browser and operating system providers p~~~~Providers of software are encouraged to include settings in their software which allows end-users, in a user friendly and transparent manner, to manage consent to the storage and access to stored data in their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment,~~ ~~such as whitelisting mechanisms. should To this end they are encouraged to ensure that end users can easily set up and amend such white lists and withdraw consent at any moment in a user-friendly and transparent manner.~~

Annex II - Purposes for processing of personal data (GDPR) and storing and/or accessing information on a user's device (ePR) for online advertising

Purposes <u>exempted</u> by Articles 8(1)(a) and (da) of the Council's latest draft ePR text
1. Basic technical delivery of ad files ● Use a user's IP address to deliver an ad over the internet ● Respond to a user's interaction with an ad by sending the user to a landing page ● NB: With this it is not possible to select an ad appropriate for the country or to choose the right language. An ad for a user in France could be Vietnamese for a store in Vietnam.
2. Security, fraud prevention, and debugging ● Ensure data are securely transmitted ● Prevent fraud or spam, including verifying that ads are not seen or clicked on by bots or other malicious actors ● Identify operational issues and correct them (debugging)

Purposes that are <u>partially exempted</u> by Article 8(1)(d) of the Council's latest draft ePR text
3. Ad measurement ● Measure whether and how ads were delivered to and interacted with by a user ● Provide reporting to advertisers about their ads including effectiveness and performance ● Provide reporting to publishers about the ads displayed on their property (*exempted*) ● Measure whether an ad is serving in a suitable editorial environment (brand-safe) context ● Determine the percentage of the ad that had the opportunity to be seen and the duration of that opportunity
4. Audience measurement ● Provide reporting to advertisers about the audience reached by their ads. ● Provide reporting to publishers about the audience that saw ads on their property (*exempted*). ● Provide reporting to publishers about the audience that viewed or interacted with content on their property (*exempted*).

Purposes that are <u>not exempted</u> by the Council's latest ePR text and <u>do not</u> rely on "tracking"[6]

5. Showing basic ads

- Use real-time information about the context in which the ad will be shown, including information about the content and the device, such as: device type and capabilities, user agent, URL, IP address
- Use non-precise geographic information to show geographically suitable ads
- Control the frequency of ads shown to a user
- Sequence the order in which ads are shown to a user
- Prevent an ad from serving in an unsuitable editorial environmental (brand-unsafe) context

Purposes that are not exempted by the Council's latest ePR text and do rely on "tracking"

6. Collecting data for personalised ads

- Collect information about a user, including a user's activity, visits to sites or apps, demographic information, or location, to create or edit a user profile for use in advertising

7. Showing personalised ads

- Select personalised ads based on a user profile or other historical user data (including a user's prior activity, visits to sites or apps, location, or demographic information)

[6] Tracking is defined by the World Wide Web Consortium (W3C) as the collection of data regarding a particular user's activity across multiple distinct contexts (such as different websites) and the retention, use, or sharing of data derived from that activity outside the context in which it occurred.