POSITION ON THE PROPOSAL FOR AN ePRIVACY REGULATION

28 March 2017

Summary

- The ePrivacy Regulation doubles down on the approach that has irritated internet users with ubiquitous consent banners and other forms of consent requests over the past five years. By failing to revise this consent approach in favour of the principles-based approach of the GDPR, the ePrivacy Regulation will trigger even more irritating consent pop ups than the ePrivacy Directive.
- IAB Europe recommends to amend Article 8(1) ePR to fully align it with the principles-based approach of the GDPR on lawful processing, including processing necessary for a legitimate interest where the fundamental rights of a data subject are not overriding. Currently rules of Article 8(1) deviate from the rules of the GDPR by imposing a rigid set of consent-centered specific exceptions. While IAB Europe does not consider it necessary to change principles adopted as recently as those of the GDPR, any changes should respect the flexibility and diversity of legal processing under the GDPR.
- IAB Europe recommends that the ePrivacy Regulation maintains the clarification found in the current ePrivacy Directive that access to an online service may be made conditional on the well-informed consent of the user to data processing for advertising purposes not strictly technically necessary for provision of that service but which are necessary for the monetisation model chosen by that service.
- IAB Europe warns strongly against mandating browsers to provide the option to block processing at a technical level. The effect in most cases would be that services could not function properly without users changing their browser settings, resulting in more user irritation as websites would prompt users to change their browser settings.
- IAB Europe welcomes the intention of the European Commission to address the "overload of consent requests for internet users" by allowing users to express their consent on a *general* basis. However, it is doubtful that this would reduce the amount of notices users receive as they are mandatory under the GDPR. In addition, users would still face *specific* consent requests, such as consent banners or consent walls, where they do not consent on a general basis.

For additional information, please contact Matthias Matthiesen, Senior Manager – Privacy & Public Policy at IAB Europe (matthiesen@iabeurope.eu, +32 (0) 2256 7507)

Foreword

Data-driven advertising is the single largest revenue source for European digital media, making up more than 75 per cent of the online revenues for publisher's journalistic content and more than 50 per cent of mobile application revenues.[1] The importance of digital revenues is only increasing, as revenues from legacy print formats and app purchases are declining. The proposed ePrivacy Regulation ("ePR") in its current form threatens to derail European digital media outlets by significantly undermining their ability to generate enough revenue to create and provide free online content and services.

[1] IHS TECHNOLOGY, Paving the way: how on line advertising enables the digital economy of the future, available at http://www.iabeurope.eu/wp-content/uploads/2016/01/IAB_IHS_Euro_Ad_Macro_FINALpdf.pdf.

As the name suggests, data-driven advertising relies on the processing of data, including personal data, such as pseudonymous online identifiers, i.e. randomly generated numerical values not connected to names or contact information, subject to the ePrivacy Regulation's cookie rules and the General Data Protection Regulation ("GDPR"). Data might be collected and used, for example, to deliver advertising, which – in some cases – involves advertisers bidding or the opportunity to show ads in real time to deliver interest-based advertisements. Interest-based advertisements generate 200 per cent more revenue on average compared to generic or contextual advertisements.[2] In addition, data may be collected and processed for measuring and analysing the effectiveness of advertisements, as well as for reporting, and billing purposes. This is necessary, for example, to ensure that a publisher receives payment for successfully displaying an advertisement to a user.

The adoption of the GDPR is a substantial milestone, establishing the principles of data protection for the foreseeable future, including, and indeed explicitly, in the digital advertising context. Compliance with its provisions will require material time and resources from companies that do business in and with the EU. Businesses and industry organisations with support from data protection authorities and the European Commission are working in good faith toward purposefully applying the GDPR as of May 2018. The prospect of hard-won compromise rules of the GDPR being altered by the ePrivacy Regulation has created significant legal uncertainty and has raised concerns that investments already undertaken and efforts already underway to achieve GDPR-compliance could be undermined. Indeed, in combination with the GDPR the uncompromising rules of the proposed ePrivacy Regulation might severely harm the ability of digital advertising to play its crucial role in funding free content and services in the EU.

IAB Europe calls on Members of the European Parliament to bear in mind the context of the transition to the GDPR in which the discussions around the ePrivacy Regulation takes place, and urges them to understand the interplay and focus on aligning the two instruments rather than introducing divergent rules on the same issues.

IAB Europe further expresses concern regarding the indicative timeline for the legislative process for the ePrivacy Regulation and its indicative date of application. Rather than pursuing an expedited adoption of the draft ePrivacy Regulation, legislators should take the necessary time to thoroughly assess and consider any new draft rules. Moreover, the ePrivacy Regulation should provide for a reasonable transition period to ensure that businesses have time to assess new rules and make the necessary changes to their privacy policies, products and services.

Aligning the "Cookie Provision" with the General Data Protection Regulation

A major problem with the ePrivacy Directive is the amount of consent banners and other consent notices a user is confronted with on a day to day basis. Contrary to what the European Commission claims, the new ePrivacy Regulation does not address this issue but doubles down on the approach that originated the problem. The ePrivacy Regulation would trigger even more irritating consent pop ups than did the ePrivacy Directive. A simple solution to this issue would be to align the cookie provision with the GDPR, which already addresses the same issues the cookie provision purports to addressed in a more nuanced manner.

The GDPR unambiguously applies to pseudonymous data, which is now clearly defined as a subset personal data (Rc. 26 GDPR). Online identifiers, including cookie identifiers, and other identifiers, the ePrivacy Regulation purports to regulate with the so-called cookie provision (Art. 8(1) ePR), are explicitly called out in the definition of personal data (Art. 4(1) GDPR, Rec. 30 GDPR). In addition, online "tracking", another reason for which Article 8(1) has been proposed, is

[2] Howard Baeles, The Value of Behvioral Targeting, available at http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

covered by the rules on profiling and transparency (Art. 4(4) GDPR, Art. 13 GDPR, Art. 22 GDPR, Rc. 24 GDPR, Rc. 60 GDPR, Rc 71 GDPR). Thus, the collection of personal information through cookies and similar technologies, including for "tracking" and profiling purposes, are "subject to the rules of [the GDPR] governing the processing of personal data such as the legal grounds for processing or data protection principles" (Rc. 72 GDPR).

This assessment is reflected in the European Commission's impact assessment, which notes that the GDPR's new definition of personal data "clarifies that online identifiers are personal data" and that the GDPR "further complements the level of information to be provided to the data subjects under Article 12, Article 13 and Article 14. The obligation to inform users about processing of personal data is therefore covered by the GDPR."[3]

This means that for collection of a user's information through cookies or other techniques to be lawful under the GDPR, users must be provided with comprehensive information about, amongst others, the purposes of the processing in an easily accessible and easy to understand manner (Art. 12 GDPR, Rc. 39 GDPR) as well as granted the full suite of data protection rights. In this context, the GDPR especially stresses the importance of transparency in the online advertising sector (Rc. 58 GDPR). Moreover, under the GDPR, the collection of information through cookies or similar identifiers, for any purpose, is only lawful "on the basis of the consent of the [user] concerned or some other legitimate basis, laid down by law" (Rc. 40 GDPR).

The importance of alternative legal bases has also been stressed repeatedly by the Court of Justice of the European Union ("CJEU"), e.g. in its recent ruling in Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*. *Breyer* concerned the question whether a pseudonymous identifier, a dynamic IP address, is personal data and, if yes, whether a controller's ability to process personal data under its legitimate interest of protecting its service against cyber-attacks could be limited. In its ruling, the CJEU confirmed that pseudonymous identifiers can be personal data and that it is not compatible with the principles of data protection law to reduce the scope for processing where it is necessary for the pursuit of a legitimate interest – provided that the fundamental rights and freedoms of the user do not override that interest.

In its current form, Article 8(1) ePR derogates from the GDPR by limiting the scope for processing personal data stored on a user's device for the pursuit of a legitimate interest (and other legal grounds). Lawful processing under Article 8(1) is limited to only one legal basis – the data subject's consent – compared to the six legal grounds of the GDPR. All legal bases[4] for collecting and processing personal data under the GDPR provide data subjects with enhanced protection compared to Directive 95/46/EC and the current ePrivacy Directive, including enhanced notice, increased transparency and greater control over how their personal data is used.

IAB Europe recommends amending Article 8(1) ePR to fully align it with the GDPR's rules on lawful processing. This could be achieved by simply making "[t]he use of processing and storage capabilities of terminal equipment and the collection of information from end-user's terminal equipment" lawful only to the extent that it takes place on the basis of the consent of the user concerned, or some other legitimate basis, laid down by Union or member state law, in accordance with the GDPR. Moreover, transparency obligations and data protection rights of the GDPR could be extended to apply to the subject matter covered by Article 8(1) ePR to ensure further alignment between the two instruments.

[3] European Commission, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, SWD(2017) 5 final, p. 102 available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41242.

[4] *See* Article 6 GDPR on the lawfulness of processing, establishing the following six legal grounds for process personal data: (a) the consent of the data subject; (b) processing is necessary for the performance of a contract; (c) processing is necessary for compliance with a legal obligation; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights of the data subject.

Unlike a rigid list of specific exemptions as proposed by the ePrivacy Regulation, the GDPR's principles-based approach allows for the needed flexibility to justify data processing in situations where relying on the consent of the user is not possible, feasible, or preferable. For example, where the processing serves the purpose of security, such as protecting a service against cyber-attacks, or the purpose of preventing other malicious behaviour, such as fraud and other legitimate interests. As it is unlikely that the legislator will be able to perfectly anticipate all potential future situations in which consent would not be the appropriate legal ground for processing, this approach would also mitigate unintended consequences and improve legal certainty in the long term. Indeed, in guidance to businesses on consent under the GDPR the UK's data protection authority, the Information Commissioner's Office, states that "[c]onsent is one lawful basis for processing, but there are alternatives. If consent is difficult, you should consider using an alternative basis."[5] Under the draft ePrivacy Regulation that would not be an option.

Particularising the General Data Protection Regulation in the "Cookie Provision"

Maintaining helpful clarifications around consent of the existing ePrivacy Directive

The existing ePrivacy Directive clarifies that storage or access of information on a device for online advertising purposes is in principle legitimate. Furthermore, the ePD clarifies that "[a]ccess to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose." The GDPR states that when assessing whether consent is freely given, and therefore valid, "utmost account shall be taken of whether, *inter alia,* the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for performance of that contract" (Art. 7 GDPR). This requires that the legality of making access to a service conditional on the well-informed consent of a user is scrutinised taking into consideration all the relevant factors to that situation and ensures that free interest-based advertising-funded services are, in principle, legal.

While IAB Europe believes that the cookie provision should reflect the lawful grounds for processing of the GDPR beyond only consent, IAB Europe also recommends that the future ePrivacy Regulation maintains the clarification that where processing is based on consent, access to an online service may be made conditional on the well-informed consent of the user to data processing that is not strictly technically necessary for provision of that service. Failing to do so would put advertising funded services on the Internet as we know it in jeopardy, result in a steep decrease of the quantity or quality of free services, and/or result in the erection of paywalls for previously free services. Moreover, IAB Europe recommends that it is clarified that first parties can obtain consent on behalf of third parties.

Particularising exceptions to the general consent requirement

As described above, all lawful grounds for processing personal data provide ample protection of users, including control and transparency about the processing of their personal data, while giving the law the necessary flexibility to stand the test of time. IAB Europe does not consider it necessary to change principles adopted as recently as those of the GDPR and if there were changes they should at minimum respect the flexibility and diversity of legal processing under the GDPR.

[5] ICO, draft GDPR consent guidance, available at http://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

New derogations from the ePrivacy Regulation's general consent requirement with adequate safeguards "could lead to the emergence of innovative, privacy friendly business models and technical solutions" and "stimulate the R&D in privacy preserving technologies" such as anonymisation and pseudonymisation techniques according to the European Commission's impact assessment on the ePrivacy Regulation.[6] The impact assessment also recognises that the general consent requirements has strong negative effects on industry, such as limiting "innovative business models relying on a large availability of data, such as free online personalised services."[7] Moreover, the impact assessment considers "a negative effect on the capacity of online providers to collect big data" and that "[t]his effect is likely to be felt more by small players or newcomers than by big established players."[8] Indeed, the impact assessment warns that the general consent requirement would damage Europe's ability "to grasp the benefits of the data economy."[9] However, all these negative effects, it continues, could be balanced by "crucial elements of flexibility, such as additional exceptions and derogations with adequate safeguards"[10], including for legitimate business practices such as personalised advertising.

If Members of the European Parliament consider that further particularisation of the principles of the GDPR are necessary, IAB Europe recommends that rather than deviating from the GDPR, the ePrivacy Regulation could clarify under which conditions the legitimate interests legal ground may be used in the online sector. Next to ensuring that users are provided with all relevant information and applicable rights under the GDPR, privacy protection could be strengthened without reducing the flexibilities of the principles-based approach of the GDPR by requiring that the collection of information necessary for a legitimate interest is only permissible if additional privacy safeguards not always required under the GDPR are met, such as conducting a privacy impact assessment about the processing, putting in place encryption or pseudonymisation measures where possible and appropriate, lower retention time periods, and other safeguards – the details of which could be established by an implementing act of the European Commission, or a decision by the European Data Protection Board.

Software Privacy Settings

Consent through appropriate settings of a software application is not a complete solution

The ePrivacy Regulation enables users to express their consent through the appropriate settings of a software application. Under the GDPR, valid consent must be *specific*, but the ePrivacy Regulation would allow a user to give consent on a *general* basis. It is critical that the law permits businesses to obtain specific consent from users in line with the GDPR where they do not choose to grant consent on a general basis.

IAB Europe has continually warned that a consent-only approach would result in consent fatigue and supports efforts to reduce user irritation. However, allowing users give a *general* consent to all data processing on the Internet to reduce consent requests is not a complete solution as it would effectively suggest users opt out of their fundamental right to data protection because dealing with consent is burdensome. Instead, IAB Europe recommends that Members of the European Parliament consider allowing the processing of data under legal grounds other than consent, consistent with the GDPR, effectively allowing businesses to take responsibility for guaranteeing that the personal data of their users is protected – rather than making users responsible. Where processing is based on consent, however, it is important that legislation does

[6] Ibid, SWD(2017)3 Part 1/3, pp. 40-41.
[7] European Commission, ePrivacy Regulation Impact Assessment, SWD(2017)3 Part 1/3, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41243, p. 40.
[8] Ibid, SWD(2017)3 Part 1/3, p. 39.
[9] Ibid, SWD(2017)3 Part 1/3, p. 40.
[10] Ibid, SWD(2017)3 Part 1/3, pp. 39-40.

not dictate which technologies to use as to not unnecessarily inhibit innovation around providing information and requesting consent in the most appropriate fashion.

Concerns about requiring software applications to block device interactions at a technical level

IAB Europe also has severe concerns about mandating browsers and other software enabling access to the Internet to provide the option to *prevent* use of processing and storage capabilities of terminal equipment and the collection of information from end-user's terminal equipment. This would make it impossible for a service to collect or display information lawfully as a technical matter. Browsers and other software are not able to distinguish between technologies that are necessary for a service to function and technologies that are not strictly necessary, processing that is lawful and unlawful, exempted or non-exempted. As a result, services would not function properly or require users to change their browser settings in order to use a service adding more irritation without added value.

Conclusion

Given the enormous interplay between the ePrivacy Regulation and GDPR, AB Europe urges Members of the European Parliament to align the two documents, rather than create a divergent set of rules that threaten to upend implementation of the GDPR. The GDPR was the result of hard fought compromise that should not be undermined by the ePrivacy Regulation.

IAB Europe asks Members of the European Parliament to:

(1) amend the cookie provision (Art. 8 ePR) to align with the GDPR's legal bases for processing, including to pursue a legitimate interest provided that the rights and interests of the user are not overriding.
(2) clarify that access to digital content and services may be made conditional on the well-informed consent of the user;
(3) do not limit the ability of businesses to obtain specific consent in line with the GDPR in cases where general consent is not given; and
(4) avoid requiring browsers to block device interactions at the technical level.

Failure to align the ePrivacy Regulation with the GDPR in these ways is likely to result in a substantial increase in irritating consent pop ups, or requests to change browser settings, severely harm the ability of digital media outlets to generate enough revenue through online advertising to provide free content, news and other services, and undermine the ability of third party business services providers to deliver expert solutions on which first party consumer services rely to generate advertising revenues or to improve their offerings.