POSITION ON THE REVIEW OF THE ePRIVACY DIRECTIVE

1 December 2016

Summary

The review of the ePrivacy Directive is a unique opportunity for "Better Regulation". The European Commission is therefore right to consider repealing outdated or unnecessary provisions of the ePD and moving provisions to other legal instruments. It is in the interest of all EU stakeholders to avoid the possible duplication of rules if we are to reap the benefits of the Digital Single Market. In line with this view, IAB Europe strongly believes that:

1. The adoption of the General Data Protection Regulation in combination with Directive 2013/40/EU on attacks against information systems makes aspects of the ePD, in particular, Article 5(3) ePD on cookies and similar technologies, redundant. The adoption of the GDPR is a substantial milestone, and compliance with its numerous provisions will require material time and resources from companies that do business in the EU. Businesses and industry organisations are working in good faith toward the deadline in May 2018 to comply with the GDPR. Proposing and ultimately requiring compliance with a redundant cookie provision unnecessarily focuses attention away from GDPR compliance efforts.
2. Should the Commission decide against repealing Article 5(3) ePD, improvements should be made to the article to align it with the legal bases found in Article 6 of the GDPR. The GDPR expresses the will of the legislator as to what the principles of data protection should be in the foreseeable future, including, and indeed explicitly, in the online context so any further rules should be avoided.
3. The future ePrivacy instrument should maintain the clarification that 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. Users remain free to choose not to use a service. Online services and third party agents should be permitted to communicate the value exchange of personal data collection for the purpose of serving interest-based advertising, in exchange for free content and services when presenting users with a consent choice.
4. The ePrivacy instrument must not interference with the fundamental rights and freedoms of online service, such as the right to property and the right to conduct a business. Online service should not be forced to make available a paid alternative of their offering that does not entail the collection of personal data for the provision of interest-based advertising and analytics.
5. The Commission should encourage effective self- and co-regulatory alternatives to legislation. The online advertising ecosystem has already set up the flexible and adaptive multi-stakeholder OBA Self-Regulatory Programme – with the support of the Commission – to provide users with transparency, choice and control over targeted online ads. IAB Europe encourages the Commission to formally acknowledge the ability of self-regulation to keep up with changes in technology and create effective rules that take changes into account.

It is crucial that the Commission analyses the future of the ePrivacy Directive in a critical and informed way, one that takes full account of the risks of unintended consequences and legal uncertainty that could undermine the vital task of creating a Digital Single Market for Europe. Our recommendations are explained in more detail in the accompanying paper.

For additional information, please contact [redacted] at IAB Europe ([redacted])

Table of Contents

POSITION ON THE REVIEW OF THE ePRIVACY DIRECTIVE 1
1 December 2016 1
Summary 1
A Chance for Better Regulation 3
Article 5(3) ePD – Device Confidentiality and Cookies 3
The Legal Context of Article 5(3) ePD from 2002-2018 4
The Legal Context of Article 5(3) ePD as of 2018 4
Illegal Storage and Access as a Crime 5
Major Update of Personal Data Protection Rules 5
Future Regulatory Consistency 5
A Future Article 5(3) ePD 5
Lawful of Storage and Access 5
Clarifying the Legitimacy of Making Access to a Service Conditional on the Informed Acceptance of Storage and/or Access 7
Refraining from Interfering with Fundamental Rights, e.g. by Dictating Business Models and Making Legal Business Models Practically Unworkable 8
Encouraging Effective Self-Regulation and Refraining from Dictating Compliance Technology 9

A Chance for Better Regulation

IAB Europe believes that the review of the ePrivacy Directive ("ePD") is a unique opportunity for "Better Regulation" and welcomes that the European Commission ("the Commission") considers "repealing outdated or unnecessary provisions of the ePD" and moving provisions to other legal instruments.[1] This paper focuses on Article 5(3) ePD on device confidentiality ("the cookie provision"), and shows that new legislation adopted since the ePD's last review in 2009 already comprehensively addresses the issues covered by the provision, making it redundant.

The paper further outlines how the cookie provision could be improved in the future to "complement and particularise" the rules of the GDPR in the online context, with a view toward simplifying and streamlining the existing rules, should the Commission decide against repealing Article 5(3) ePD.

It should be noted that the adoption of Regulation (EU) 2016/679 ("General Data Protection Regulation", "GDPR") expresses the will of the legislator as to what the principles of data protection should be in the foreseeable future, including, and indeed explicitly, in the online context. IAB Europe calls on the Commission to exercise restraint when considering to open the exact same issues up for legislative intervention again and to refrain from moving the goal posts once more, before the GDPR even becomes applicable. The focus should be on aligning the two instruments, also with respect to Article 5(3) ePD, and not the introduction of additional rules.

The adoption of the GDPR is a substantial milestone, and compliance with its numerous provisions will require material time and resources from companies that do business in the EU. Businesses and industry organisations are working in good faith toward the deadline in May 2018 to comply with the GDPR. Proposing and ultimately requiring compliance with a redundant cookie provision unnecessarily focuses attention away from GDPR compliance efforts.

Article 5(3) ePD – Device Confidentiality and Cookies

Article 5(3) ePD stipulates that the storing of information, or the gaining of access to information already stored, is only allowed on the condition that the user has given their informed consent. Narrow exceptions are provided for situations where storage or access (a) have the sole purpose of carrying out a communication over the Internet; or (b) is strictly necessary for the provision of a service requested by the user.

The provision conflates two fundamentally different issues: surreptitious storage and/or access for illegitimate purposes, such as installing and using spyware, and the use of technologies, such as cookies, that store and/or access information for legitimate purposes.

The provision's first objective is to limit "spyware, web bugs, hidden identifiers and other similar devices" from entering a user's device "in order to gain access to information, to store hidden information or to trace the activities of the user" without their knowledge and therefore seriously intruding on the privacy of affected users (Rc. 24 ePD).

[1] REFIT Evaluation and Impact Assessment of Directive 2002/58/EC, available at http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_cnect_013_review_eprivacy_en.pdf

At the same time, it is clearly stated that that information storage or access, "for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising" and that where cookies "are intended for a legitimate purpose […] their use should be allowed" on the condition that the user is informed about the purposes of the information storage or access in accordance with information duties of general data protection law (Rc. 25 ePD). Lastly, it is explicitly stated that access to "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 Legal Context of Article 5(3) ePD from 2002-2018

When the ePD was first proposed in 2002 and reviewed in 2009, it was meant to complement Directive 95/46/EC ("Data Protection Directive", "DPD") in the electronic communications sector and online environment.

The DPD does not clearly apply to pseudonymous identifiers such as unique online identifiers, which allow personalising browsing experiences, but cannot (easily) be linked to an identified natural person. Some member states' implementations of the DPD treat pseudonymous identifiers as anonymous data, others provide for a specific legal framework for pseudonymous data that is separate from that of personal data, while some member states consider pseudonymous identifiers personal data. As such the legal protection offered across the EU concerning pseudonymous identifiers, such as cookie identifiers was everything but uniform.

The cookie provision sought to address this perceived gap in the protection of individuals in the online environment and give users information about the use of pseudonymous identifiers (be they cookie identifiers, device identifiers such as advertising ID, or device fingerprints) that can be used to collect information about the browsing behaviours of a user and to create profiles about them, e.g. to serve interest-based online advertising – and give users control about their use. First by granting users a right to refuse (2002) then by requiring that users consent (2009) to the collection of information through pseudonymous identifiers stored on their device. However, some member states' implementations of the DPD allow consent to be granted through an omission, such as not refusing the use of cookies, while others required a positive action. This has, in practice, led to very different practical implementations of Article 5(3) ePD across the EU and in some member states the switch from the right to refuse to requiring consent has not resulted in any change for the user in practice.

In addition, as the DPD does not apply to storage and access of non-personal information, there was a perceived need to have a provision that prohibits the accessing of a user's device without their knowledge as such. Indeed, the ePD is often purported to be the only EU legislation giving a user such comprehensive protections for their private sphere against surreptitious storage or access of information on their personal device.

The Legal Context of Article 5(3) ePD as of 2018

Since the last review of the ePD in 2009, the legal situation in the EU has changed significantly. Device confidentiality and data protection aspects of the provision are now covered in other EU instruments. From a legal protection point of view, the legal situation as of 2018 objectively obviates the need for Article 5(3) ePD bearing in mind its former spirit and purpose as a band-aid solution for addressing a perceived gap in the protection of individuals in the online environment.

Illegal Storage and Access as a Crime

Directive 2013/40/EU on attacks against information systems ("AAISD") introduces rules that cover device confidentiality that go significantly further than Art. 5(3) ePD. Not only does the directive outlaw the (a) access to devices (Art. 3 AAISD); (b) interference with devices (Art. 4 AAISD); and (c) interference with data on devices (Art. 5 AAISD) without authorisation (e.g. consent of the user) or another legal basis, it makes it a criminal offense. As such, illegal storage or access of information on a user's device is punishable by up to five years of imprisonment (Art. 9 AAISD) or "effective, proportionate and dissuasive sanctions" such as the judicial winding-up and closure of the legal entity liable (Art. 11 AAISD). As such, users are comprehensively protected by criminal law against the surreptitious storage or access of information on their devices, including spyware and other malicious software, hackers, etc.

Major Update of Personal Data Protection Rules

The new Regulation (EU) 2016/679 ("General Data Protection Regulation", "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 device identifiers, for which Article 5(3) ePD was created, are now 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 5(3) ePD was created, is now covered by the rules on profiling (Art. 4(4) GDPR, Rc. 24 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 means that for collection of a user's information through cookies or similar technologies 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). 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).

Future Regulatory Consistency

Considering the complete overlap of the substantive scope of application of the GDPR and Article 5(3) ePD, the policy goal of consistency between the two instruments, as established by Recital 173 GDPR, can only be achieved by – if not a complete repeal – amending Article 5(3) ePD in line with the GDPR.

A Future Article 5(3) ePD

Lawful of Storage and Access

In its current form, Article 5(3) ePD derogates from the GDPR by limiting available legal bases for processing personal data stored on a user's device to only one – the data subject's consent – compared to the six legal grounds of the GDPR. The remaining five legal bases of the GDPR are only available for processing personal data stored on a user's device in two very limited exceptions.

Consent is not a panacea: Industry has cautioned repeatedly against considering consent a "better legal ground" vis-à-vis other legitimate grounds for processing personal data. IAB Europe considers that good policy is based on facts, however, no data has been produced in support of the notion that data processing under the consent legal provides a higher degree of data protection. In its response to the public

consultation on the ePrivacy review the International Center for Law & Economics told the Commission that this is an empirical question that has been extensively researched:

> *"The 'Opt-in' is frequently portrayed as giving consumers greater privacy protection than 'opt-out,' and in fact, the opposite is true. 'Opt-in' provides no greater privacy protection than 'opt-out' but imposes significantly higher costs with dramatically different legal and economic implications."*[2]

Moreover, industry has long warned that by over-relying on consent, users would get accustomed to clicking without carefully considering the consequences of their action. As a result, consent has been losing its warning function for actually important decisions. IAB Europe invites the Commission to analyse the impact on society of consent-only policies to better understand the full implications of such policies.

IAB Europe welcomes the European Commission's intention to provide for additional exceptions to the consent requirement of Article 5(3) ePD. However, IAB Europe has concerns that a white-list approach would provide the necessary flexibility to meet real world requirements. Instead, IAB Europe recommends to align the ePD and GDPR by making storage or access lawful if it meets the criteria of the GDPR:

> *The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user shall only be allowed with the consent of the subscriber or user concerned or some other legitimate basis, laid down by law, in Regulation (EU) 2016/679 or in other Union or Member State law.*

All of the legitimate grounds for collecting and processing personal data under the GDPR provide data subjects with enhanced protection compared to the DPD, including notice, transparency and control over how their personal data is used. At the same time, unlike a rigid list of specific exemptions, the GDPR's principles-based approach allows a degree of flexibility for controllers to justify their 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. 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.

The importance of these alternative legal bases has been stressed by the Court of Justice of the European Union ("CJEU") 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 the relative definition of regulated personal data, but interpreted it broadly to include certain pseudonymous identifiers. Including pseudonymous identifiers that cannot be directly related to a natural person by the controller itself, but only by another entity. Moreover, the CJEU ruled that limiting the ability of a controller to rely on its legitimate interest for processing personal data – subject to an assessment that that interest prevails over the interests or fundamental rights of the user concerned – is incompatible with the legal provisions on the lawfulness of processing.

[2] Position Statement of the International Center for Law & Economics in the Matter of: The Public Consultation on the Evaluation and Review of the E-Privacy Directive, available at https://ec.europa.eu/eusurvey/files/c8992170-189b-43e2-ae04-993afaeec704

The Commission could consider to particularise the GDPR by clarifying under which conditions access to the legitimate interests legal ground is permissible in the online sector. IAB Europe supports strengthening user's rights by requiring that the collection of information for the purposes of interest-based advertising is only permissible under the legitimate interests of the controller legal ground under the condition that collected data is immediately pseudonymised. This would allow the Commission to level the playing field between B2C businesses who are able to obtain the user's consent more easily, and B2B businesses who are not in a position to obtain the user's consent very easily, or at all.

Allowing businesses to compete fairly in the online space encourages the development of privacy forward practices and technological solutions through innovation that ultimately benefit consumers.

Moreover, this would incentivize the pseudonymisation of personal data and use of pseudonymous data over identified personal data in line with the principle of data minimisation.

IAB Europe recommends that the Commission either repeals Article 5(3) ePD, or modifies it to be in line with other legislation covering the same matter. This could be achieved by simply making access or storage 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.

Clarifying the Legitimacy of Making Access to a Service Conditional on the Informed Acceptance of Storage and/or Access

In its current form, the ePD 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.

IAB Europe recommends that the future ePrivacy instrument maintains the clarification that 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 the Internet as we know it in jeopardy.

Advertising is the single largest revenue source for European digital media, making up more than 75 percent of revenues for journalistic content online and more than 50 percent of mobile application revenues.[3] The importance of digital revenues is only increasing, as revenues from print are declining. The Commission should understand that market realities today are that there is no advertising that does not rely on the collection and processing of data for one purpose or another, Data might be collected and processed before the fact for the purpose of delivering advertising programmatically (e.g. through automated real-time-bidding in milliseconds), and/or to delivery interest-based advertisements. On average, interest-based

[3] 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

advertising is more than 200 percent more valuable and effective compared to non-interest-based advertising.[4] Thus, interest-based advertising is a critically important source of revenue for publishers.

In addition, data might be collected and processed after the fact for the purpose of measuring and analysing the effectiveness of the advertisement. This is necessary for example, to ensure that a publisher receives payment for successfully displaying an advertisement to a user.

Moreover, data is collected and processed for purposes other than advertising for general web analytics and audience measurement. Web analytics provide aggregate insights into an online service's users, allowing the provider to understand and react to user demand, identify technical malfunctioning, and more. Audience measurement allows analysing web traffic beyond the individual site level to provide aggregate insight into the use of content and advertising at large. This provides market transparency, in the absence of which businesses would operate in the dark. Audience measurement is particularly important for small and medium sized enterprises who cannot rely on large audiences on their own individual site.

IAB Europe recommends that the future ePrivacy instrument clearly exempts analytics, including web analytics and audience measurement, from the requirements of the cookie provision.

Refraining from Interfering with Fundamental Rights, e.g. by Dictating Business Models and Making Legal Business Models Practically Unworkable

IAB Europe fundamentally opposes the view of the European Data Protection Supervisor ("EDPS") and the Article 29 Working Party ("WP29") that it should not be permitted to make access to a website conditional on the well-informed acceptance of a cookie or similar device. Users remain free to choose not to use a service. Online services and third party agents should be permitted to communicate the value exchange of personal data collection for the purpose of serving interest-based advertising, in exchange for free content and services when presenting users with the opportunity to make a consent choice.

Moreover, IAB Europe strongly disagrees with the view of the EDPS and WP29 that a user should have the right to refuse the terms and conditions under which an online service is made available to the public while still having access to that same service if these include the collection of personal data for the provision of interest-based advertising.

In addition, IAB Europe has tremendous concerns about the view of the EDPS and WP29 that an online service should be required to make available a paid alternative of their offering that does not entail the collection of personal data for the provision of interest-based advertising.

The above-mentioned views of the EDPS and WP29 discriminate against certain lawful business models, and are in complete disregard of both the economics of the online sector, as well as fundamental rights and freedoms guaranteed by the Charter of Fundamental Rights of the European Union ("CFREU"), especially, but not limited to, the right to property.

The right to property (Art. 17 CFREU) prohibits depriving anyone, including online services, of their right to use their property in the way they see fit – including deciding under which conditions services are offered to the public. Any regulation of the use of property is only permissible in very limited circumstances and subject to a rigorous necessity and proportionality test. IAB Europe takes the view that the regulation of the

[4] Howard Beales, The Value of Behavioral Targeting. 2009, available at http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf

use of property of private undertakings as proposed by the EDPS and WP29, and referenced above, are in breach of European fundamental rights.

Lastly, IAB Europe stresses that privacy and data protection laws should not be enlisted to achieve competition enforcement aims.

Encouraging Effective Self-Regulation and Refraining from Dictating Compliance Technology

IAB Europe cautions against legislatively interfering with the freedom of online services to choose the most appropriate way of complying with the law as set out in the GDPR. The practicalities of requesting and obtaining consent, for example, are best determined by the parties engaged in an interaction and/or transaction. Legislation in this field risks unnecessarily reducing the flexibility of the legal framework. This is especially important due to the fast-moving nature of the online environment, where a lack of flexibility due to rigid rules imposed through legislation can have a stifling effect on innovation, such as new privacy and user interface technology that benefits consumers, and raise costs for businesses and consumers.

Instead, the Commission should encourage effective self- and co-regulatory alternatives to legislation to the same effect. The online advertising ecosystem has already set up the flexible and adaptive multi-stakeholder OBA Self-Regulatory Programme[5] – with the support of the Commission – to provide users with transparency, choice and control over targeted online ads.

DG CNECT in particular, has been deeply involved in the set-up of the European Digital and Interactive Advertising Alliance (EDAA), the self-regulatory body of the European advertising industry. Self- and co-regulation can address sector-specific concerns more effectively. EDAA has proven in the past to be an efficient tool to address practicalities beyond base line compliance. According to the European Advertising Consumer Research Report 2015 up to 56% of respondents said that the option to manage their privacy preferences through this program increased their levels of trust in the advertised brand. Furthermore, up to 59% of respondents feel more favorably about online advertising thanks to the program.

IAB Europe believes that the flexibility and expertise of the EDAA and the stakeholders it includes, generally provides a better choice than regulation for addressing details such as the methods of providing transparency to users, or allowing users to express choice and exercise control, and do so quickly and meaningfully, but without unnecessarily stifling future innovation in privacy and user interface technology that benefits consumers. IAB Europe encourages the Commission to formally acknowledge the ability of self-regulation to keep up with changes in technology and to create effective rules that take these changes into account.

[5] European Digital Interactive Advertising Alliance (IAB Europe Framework for Online Behavioural Advertising), available at http://www.edaa.eu.