khlaw.com
+32 (0) 2 645 5000

Keller and Heckman LLP
Stephanie Plaza
Avenue Louise 54
1050 Brussels
Belgium

Peter Craddock
+32 (0) 2 645 5074
craddock@khlaw.com

18 January 2024

European Data Protection Board
Rue Wiertz 60
1047 Brussels
Belgium

Re: Public consultation re Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

Dear Madam, dear Sir,

Since the publication of the proposed Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive (hereinafter the **Proposed Guidelines**), various organisations have been in discussion with our firm, voicing a wide range of concerns and questions regarding the Proposed Guidelines.

We write to you on behalf of some of those organisations, who wish to contribute to the public consultation regarding the Proposed Guidelines in a meaningful manner without drawing attention to their identity, notably to avoid being singled out.

In this context, we respectfully request that the European Data Protection Board (**EDPB**) and its members take the following comments and considerations into account, taking into account also the legislative context of the ePrivacy Directive (**ePD**) and the General Data Protection Regulation (**GDPR**).

I. Preliminary remark on the EDPB's authority to adopt such "guidelines"

While the organisations that have reached out to us acknowledge and appreciate the time and effort spent by the EDPB in examining the ePD and assessing how to clarify it, several have shared their concerns regarding the EDPB's very authority to adopt the Proposed Guidelines in their current format.

These concerns stem from the following legislative and factual context:

a) the EDPB's predecessor, the Article 29 Working Party, was entitled pursuant to Article 15(3) ePD to *"carry out the tasks laid down in Article 30 of [Directive 95/46/EC] with regard to matters covered by [the ePD], namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector"* – and that Article 30(3) of Directive 95/46/EC stated that *"[t]he Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community"* (which was the justification quoted in Opinion 04/2012 on Cookie Consent Exemption for the Article 29 Working Party's authority to adopt said Opinion);
b) in accordance with Article 94(2) GDPR, references to the Article 29 Working Party and to Directive 95/46/EC in the ePD now have to be read as references to the EDPB and to the GDPR, respectively;
c) the EDPB's powers under Article 70 GDPR are far broader than those of the Article 29 Working Party under Article 30 of Directive 95/46/EC, including not only the power to adopt opinions and recommendations but also the power to adopt e.g. guidelines;
d) one of those is the power for the EDPB to *"examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of [the GDPR] and issue guidelines, recommendations and best practices in order to encourage consistent application of this [the GDPR]"* (Art. 70(1)(e) GDPR);
e) however, none of the provisions of Article 70 GDPR appear to allow the EDPB to adopt guidelines or recommendations that relate to other legislation (the only power under Art. 70 GDPR going beyond the GDPR is the power to *"advise the Commission on any issue related to the protection of personal data in the Union"* – Art. 70(1)(b) GDPR), unlike Article 30(3) of Directive 95/46/EC;
f) nevertheless, the references in the Proposed Guidelines to Article 15(3) ePD and Article 70(1)(e) GDPR suggest that the EDPB views Article 15(3) ePD as an authorisation to apply all GDPR-related powers under Article 70 GDPR to the ePD, even if the text of a particular provision of Article 70 GDPR is explicitly limited in scope to only GDPR-related issues;

This apparent vision of the EDPB seems problematic, for various reasons:

a) the wording of Article 70 GDPR does not appear to allow it (nor do the very generic terms of Article 94(2) GDPR), despite being the newer legislation – had the EU legislator desired to allow the EDPB to adopt guidelines regarding the ePD, it would surely have included broader wording in Article 70 GDPR in order to avoid such contradictions;
b) Article 15(3) ePD was adopted at a time when the powers of the Article 29 Working Party were more limited, and the more restrictive scope of Article 70 GDPR must be considered as better reflecting the current will of the legislator;

c) finally, the EDPB's own members do not all have jurisdiction over enforcement of Article 5(3) ePD, and nothing in the GDPR or the ePD appear to suggest that the EDPB should be granted the power to change the way in which those authorities that *do* have jurisdiction over enforcement of Article 5(3) ePD interpret that provision. By way of additional explanation, from a linguistic perspective, "guidelines" appear to be intrinsically more binding upon authorities than "recommendations", which may explain why Opinion 04/2012 (a set of recommendations) was not challenged; should the EDPB be permitted to adopt "guidelines" on this matter, on the other hand, they would likely be expected to be binding upon authorities, despite the EDPB's membership not including all relevant authorities.

In summary, the adoption of guidelines in relation to Article 5(3) ePD raises important questions regarding the EDPB's authority in this field, as well as the consequences in terms of jurisdiction and enforcement.

As a result, the organisations who have asked us to submit a response on their behalf ask whether it would not be more appropriate for the EDPB to restrict the scope of the Proposed Guidelines to *only* the material and territorial scope of the GDPR (and in other words, only cases where there is actual processing of personal data regulated by the GDPR) or to otherwise solidify the EDPB's authority in this field, possibly by way of joint statements together with all competent regulators and by way of a transformation of the Proposed Guidelines into mere recommendations.

The remainder of their remarks are therefore to be taken not as a recognition of the EDPB's authority to adopt the Proposed Guidelines but as a request for clarification and adaptations, should the EDPB continue to consider that it has the necessary authority (without prejudice to any challenges to such authority).

II. Executive summary: unintended consequences and the threat to privacy-centric tools

By way of a summary of the comments below, the Proposed Guidelines present a marked development to the meaning of Article 5(3) ePD (in direct contradiction with positions of supervisory authorities as recent as March 2022 – i.e. a mere 18 months before the publication of the Proposed Guidelines), and their unamended adoption will have wide ranging and detrimental effects on the healthy operation of the Internet and key industries and practices that support it.

The Proposed Guidelines will not simply affect those engaged in activities that the EDPB may view (for whatever reason) as privacy-intrusive but will also affect those companies who have sought to develop genuinely privacy-centric tools for analysis and attribution by utilising information that is transmitted automatically as part of standard Internet operations and that is not "personal data" from their perspective (given that they have no lawful means of identifying or enabling the identification of the natural person using a particular device). In addition, they appear to create significant inconsistencies between the (reinterpreted) Article 5(3) ePD and various other provisions of the ePD, in a manner that does not appear to have arisen previously during the two decades that the ePD has existed in the EU legislative landscape.

The drafting of the Proposed Guidelines appears moreover at odds with the fact that the revision to the ePD has been under constant and painstaking negotiation since publication by the European Commission of a proposal for an ePrivacy Regulation in January 2017 and has always been viewed as a legislative matter. In effect, the Proposed Guidelines extend the scope of Article 5(3) ePD in a manner that negates all such legislative discussions, as if they had not ever been needed.

III. Broad interpretation of "gaining access" and "storage": far-reaching application and impact on any business with a digital presence, from the advertising industry to digital service providers

Organisations are concerned that the EDPB's interpretation of "gaining access to" information under Art. 5(3) ePD is so wide as to mean "merely inadvertent and inevitable receipt" for the most basic of Internet operations. In addition, they fear that the EDPB's interpretation of the concept of "storage" equally leads to covering any interaction with a device, a far broader scope than the common understanding of the term "storage".

A. Examples of digital activities likely covered by Art. 5(3) ePD based on Proposed Guidelines

From the Proposed Guidelines it appears that notably the following activities would fall under the scope of Art. 5(3) ePD:

- Aggregate counting of traffic across internet sources even when they (i) contain no identifier that relates to an individual and/or (ii) are not intended to be used in any subsequent tracking;

- Receipt of non-personal data used solely for the detection of fraudulent digital activity;

- Supporting any peripheral services beyond expressly loading content to the user that provides utility, safety or functionality beyond that content;

- Use of IP address data for use in anti-fraud bot verifications;

- Use of IP address data for business identification purposes;

- Recording the performance of advertising campaigns by using UTM *(Urchin Tracking Module)* parameters, such as the collection of "Ad" details (e.g. placement/creative, rather than anything with user identifiers);

- Recording the referrer (i.e. domain name) that led to a page view, to be able to identify organic search and social traffic;

- Recording the country of users based on IP addresses, to check that advertising is running in compliance with regulatory rules and to provide general non-user specific insights; and

- Recording of details extracted from the user agent such as the browser or platform, which are required to ensure sites are built to work with the technologies users are using.

All of the scenarios described above are based on information that is transmitted automatically as part of the way in which the Internet works (and more specifically the Transmission Control Protocol / Internet Protocol, or TCP/IP) – information that until the publication of the Proposed Guidelines appeared to be considered by authorities to be outside of the scope of Art. 5(3) ePD.

To illustrate, in Germany, the view expressed on 20 December 2021 at the level of all supervisory authorities through the **Datenschutzkonferenz**[1] was the following:

> *"An access requires a targeted transmission of browser information that is not initiated by the end user. If only information, such as browser or header information, is processed that is transmitted inevitably or due to (browser) settings of the end device when calling up a telemedia service, this is not to be considered "access to information already stored in the end device". Examples of this are:*
> *• the public IP address of the terminal device,*
> *• the address of the called website (URL),*
> *• the user agent string with browser and operating system version and*
> *• the set language.*
> *In contrast, it is already considered access to information on the end user's terminal equipment if the properties of a terminal are actively read - for example, by means of JavaScript code - and transmitted to a server for the creation of a fingerprint."* (machine translation)

This position was also included by the local supervisory authority for the **State of Baden-Württemberg** in later guidance in March 2022[2], stating explicitly that (machine translation) *"[the German implementation of the cookie rule] only covers "access" to information if this is targeted. Both IP address and user agent are information that the browser automatically sends when a website is called up, without the provider of the [digital] service being able to influence this".*

In other words, the position of the EDPB is inconsistent with very recent views in certain countries, creating legal uncertainty.

[1] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, 20 December 2021, *Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien,*available online at: https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

[2] Landesbeauftragten für den Datenschutz und die Informationsfreiheit – Baden-Württemberg, March 2022, *Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps*, available online at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/03/FAQ-Tracking-online.pdf

B. Available justification(s) under Art. 5(3) ePD for such digital activities

In addition to this issue of consistency, to date, no authority entrusted with enforcement of Art. 5(3) ePD appears to have (openly and successfully at least) defended that such digital activities require a justification under Art. 5(3) ePD, namely:

a) consent,
b) strict necessity for the provision of an information society service explicitly requested by the subscriber or user, or
c) use for the sole purpose of carrying out the transmission of a communication over an electronic communications network.

Additional consideration: no "legal obligation" or "legal authorisation" justification

It is first worth stressing that under Art. 5(3) ePD, there is no possibility for an organisation to claim that it is legally required or authorised to store information or gain access to information already stored on a user's terminal equipment.
This is unlike Art. 5(1) ePD, on the confidentiality of electronic communications, which specifically includes an exception to the prohibition of interception or surveillance of electronic communications "when legally authorised to do so" by Member State law (in accordance with the mechanism included in Art. 15(1) ePD), and also unlike Art. 6(1) GDPR.

With a more limited scope concerning only (as intended by the legislator) the actual (active) storage of information on a device as well as the actual (active) gaining of access to information on a device, the absence of a "legal obligation" or "legal authorisation" does not appear to raise any particular issues, as Art. 5(3) ePD then only concerns certain technologies and sufficient alternatives exist. However, in the context of an arguably excessively broad interpretation of the concepts of "storage" and "access", whereby any interaction with a computer or server is covered, the lack of such an exception creates greater difficulties.

Indeed, should Art. 5(3) ePD be extended to apply to the aforementioned digital activities, several of which are necessary for compliance with national or (distinct) EU law requirements in certain sectors, this creates a statutory conflict, as a result of which those other laws permitting or even requiring certain activities can suddenly be set aside for no other reason than a novel regulatory interpretation of the ePD.

As we will see hereunder, this raises particular issues in the context of IP-based validation.

Justification c) – communication transmission

Justification c) above does not appear to be available for the digital activities described above, as they involve precisely the reuse of information that was used solely for transmission of an electronic communication.

Justification b) – information society service

As regards justification b), there are practical and valid considerations in support of a broad concept of "strict necessity for provision of an information society service".
For instance, without fraud detection a service provider may be overburdened by e.g. fraudulent bot requests for a service and may be in a technical incapacity to provide the service to legitimate customers – and a given user's behaviour may in turn improve fraud detection for a subsequent user. Similarly, without the recording of performance of an ad campaign for an advertiser a publisher may not be able to attract advertisers – which in turn may signify that the publisher lacks the funding to make content, let alone make it available to the public.

However, inconsistencies in the approach of Art. 5(3) ePD regulators in relation to cookies, in combination with recent case law in the realm of separate legislation (the GDPR), create uncertainty as to whether regulators and supervisory authorities would accept its application.

First, the views developed for instance by **Traficom**[3] (Finland) and the **AEPD**[4] (Spain), which permit the use of cookies to manage the displaying of advertising without the need for consent, suggest a broad view of the notion of strict necessity for the provision of an information society service; the **CNIL**[5] (France) on the other hand has considered that cookies used for "capping" of advertising (i.e. to limit the number of times that a particular ad appears) require consent. This inconsistency means that in the absence of a pan-EU position, there is legal uncertainty associated with reliance on the "service" justification.

Next, recent GDPR-related case law suggests that the EDPB and (some of) its members have a narrow view of the notion of "necessity for performance of a contract" and likely therefore also of the similar notion under justification b), i.e. "strict necessity for the provision of an information society service".
Indeed, the reasoning developed by the EDPB in such GDPR-related matters suggests that the EDPB and (some of) its members consider that only the aspects that are related to the actual transmission of content or technical delivery of the service to the user are "necessary", ignoring all aspects that are in practice necessary in order to be in a position to offer such a service (for instance, financing, troubleshooting and service improvement). While the notion is different, conceptual similarities raise the spectre of a strict interpretation of the "service" justification by the EDPB and its members.

---

[3] Traficom, 8 June 2023, *Sanoma Media Limited*, pp. 39-40, available online: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Sanoma%20Media%20Finland%20Oy.pdf

[4] AEPD, July 2023, *Guía sobre el uso de las cookies*, p. 12, available online: https://www.aepd.es/documento/guia-cookies.pdf

[5] CNIL, 17 September 2020, *Délibération n° 2020-092 du portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs »*, p. 4, available online: https://www.cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf; see also CNIL, 29 December 2022, *Délibération de la formation restreinte n°SAN-2022-027 concernant les sociétés TIKTOK INFORMATION TECHNOLOGIES UK LIMITED et TIKTOK TECHNOLOGY LIMITED*, para. 55, available online: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046977994/

Therefore, to be a sufficiently certain and viable option for the aforementioned digital activities, strict necessity for the provision of an information society service explicitly requested by the user would require confirmation by the EDPB (if it chooses to continue adoption of the Proposed Guidelines with their current scope) as well as authorities in charge of enforcement of Article 5(3) ePD that:

- the service provider is free to define a service the way it sees fit, and
- the activities that underlie a service, from its conception all the way to actual provision of the service to a given user as well as the reuse of lessons from a given user's interaction in order to improve the service for a subsequent user, all can be deemed (subject to justification of course) to be covered by such concept of strict necessity.

In the absence of such confirmation, organisations will likely be fearful of taking such a position, in the light of the aforementioned inconsistencies from one Member State to another and in the light of the restrictive approach adopted by the EDPB and (some of) its members in GDPR-related cases.

Unfortunately, the EDPB has explicitly stated in the Proposed Guidelines that they *"do not intend to address the circumstances under which a processing operation may fall within the exemptions from the consent requirement provided for by the ePD"* (Proposed Guidelines, para. 4, page 5). In other words, the EDPB has elected to broaden the scope of Art. 5(3) ePD without bringing additional clarifications to the scope of the scenarios in which no consent is required.
This is the opposite approach to that taken in the context of the drafting and negotiation of the ePrivacy Regulation. In the proposed ePrivacy Regulation, the expansion of the scope of the equivalent of Art. 5(3) ePD has been accompanied by a multiplication of the scenarios not requiring consent – and each EU legislative body (Commission, Parliament and Council) has spent significant effort in reviewing the list of non-consent scenarios in its work on the ePrivacy Regulation, some of which would clearly cover the aforementioned digital activities[6].

In such a context, the EDPB's decision to provide a new interpretation of the scope of Art. 5(3) ePD, without any attempt to provide legal certainty regarding consent exemptions, appears to leave legal certainty for only one justification – justification a), i.e. consent.

C. Similar considerations regarding "storage"

With regard to the notion of "storage", the EDPB's Proposed Guidelines suggest that there is no upper or lower limit in the ePD with regard to (i) the length of time that information must remain on a storage medium in order to be considered stored, or (ii) the amount of information that must be stored. While the legislator is indeed not explicit in this regard, the EDPB's position appears to distort the meaning of the words deliberately chosen by the legislator - in particular when the EDPB suggests that any information "stored" in random access memory (RAM) or in the cache of the central processor unit (CPU) is covered by Article 5(3) ePD.

[6] See e.g. Council version of the ePrivacy Regulation as part of its mandate for negotiations with the European Parliament, which specifically includes consent exemptions for fraud prevention purposes, audience measurements etc., as well as a possibility to consider further use of information as compatible with the purpose of collection if certain conditions are met. Council of the European Union, document 2017/0003(COD), 10 February 2021, available online: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

At its most basic, "to store" means "to place or leave in a location (such as a warehouse, library, or computer memory) for preservation or later use or disposal" (Merriam-Webster). However, "to store" is not abstract - it is an action: someone is storing something. Identifying that "someone" is critical to understanding the scope of Article 5(3) ePD and, in particular, who then has any obligations.

In addition, the 'for preservation or later use' component of storage referred to in the definition above is critical to understanding the applicable thresholds. Information is stored for later retrieval. This is perfectly illustrated in the ePD by the legislator's choice to speak of access to information "already stored". This word "already" introduces a notion of time which, although it does not contain a precise threshold, implicitly excludes instantaneous calculations.

In other words, the storage of information does require control and intent, and a temporal notion; gaining access to information already stored equally requires a certain amount of time has lapsed, at least more than immediacy.

In this context, the EDPB's position on storage – which it interprets in a far broader manner in the Proposed Guidelines – would cause difficulties in various situations.
A useful example in this respect is caching, i.e. the temporary saving by a web browser of a copy of certain files or elements of a website, to enable the browser to load a page rapidly the second time. The caching is not crucial to the delivery of a service but makes it faster. However, if a webpage gets updated and an older cached copy remains on the user's device, a web browser loading the cached copy will in fact be displaying outdated content.
In that respect, the HTTP specification (i.e. one of the most fundamental specifications for websites) explicitly states the following[7]:
"Since origin servers do not always provide explicit expiration times, a cache MAY assign a heuristic expiration time when an explicit time is not specified, employing algorithms that use other field values (such as the Last-Modified time) to estimate a plausible expiration time."
Put differently, website content can be cached on a user's device, whether the website publisher requests caching or does not request it explicitly.
Yet because caching can prevent the viewing of up-to-date content, some organisations seek to ensure that when a user visits their (own or affiliated) website, the browser cache regarding that page's content is flushed (i.e. erased), so that only the new content is visible.
Such an approach is obviously covered by the EDPB's new "storage" interpretation – but should it be?
The "transmission" exemption could be argued not to apply, as caching and interacting with a cache is not part of the actual transmission of an electronic communication, despite precisely enabling it (by flushing the cache) or following it (the actual creation of the cache occurs upon the loading of the webpage).

[7] Internet Engineering Task Force (IETF), *RFC 9111 – HTTP Caching* standard, Section 4.2.2, available online: https://www.rfc-editor.org/rfc/rfc9111.html#heuristic.freshness

From a user's perspective, it is likely that the "service" exemption would be viewed as relevant: it seems a fair assumption that the user loading a webpage expects it to be up to date. Yet in the absence of a specific and explicit statement from the EDPB and relevant authorities from this perspective, such a position may be viewed as legally uncertain, as the existence of a cache does not prevent the provision of the service, nor is the creating of a cache a prerequisite for the provision of the service.
In other words, as with the "access" aspects, regulators are likely to require consent.

D. Consequences of consent

In practice, the Proposed Guidelines appear to lead to consent as a requirement for such digital activities, despite the relevant information being purely received automatically (and thus passively by the organisation in question) rather than actively and specifically retrieved from a user's device (on the initiative of the organisation in question) – and despite often being only ephemerally "stored" on that device. What can only be assumed to be an intent to cover fingerprinting and intrusive tracking techniques therefore leads to the covering of a broad range of technologies that are in many cases deployed for use cases far removed from such intrusive tracking.

However, a consent requirement for the aforementioned digital activities would have significant and negative consequences for both the whole digital sector and its users.

1. Rendering validation, a critical part of the digital ecosystem, ineffective

A significant consequence of such a consent requirement would be the fact that validation becomes entirely ineffective, because validation (a critical process in the digital ecosystem) cannot function if based on consent.

In this respect, it is first worth stressing that several regulated or sensitive sectors and even commercial agreements restrict the audiences to whom certain services or products may be advertised. For instance, in the financial sector, various professional investment services cannot be advertised to retail investors, and regional licences (e.g. Switzerland vs EU) also mean that adverts cannot breach geographic bounds; similarly, a video streaming service may only have the rights to display some films in certain countries, and cannot either show in other countries a trailer or advert featuring parts of those films.
In order to ensure that the advert itself is compliant with the regulatory requirements, therefore, an advertiser is in effect required to request the publisher to whose audience ads are shown to take measures, directly or through an intermediary, to ensure that only members of an audience within a certain segment (e.g. professional investors; people apparently living in countries X, Y and Z) are shown the ad.
IP addresses and similar indicators are in practice the best means of validating that the ad took place and was served to the right broad set of audiences.

Yet as indicated above, the position adopted by the EDPB and (some of) its members under the GDPR suggests that they might consider that the "service" justification does not cover the advertising portion of it (even though it may be financially necessary to the provision of the service). In such a case, they might consider that consent is required.

Requesting consent for ad validation, however, would severely affect the effectiveness of such ad validation, as in the event of refusal of consent a choice would have to be made either to by default validate all ads (with the result that they may be specifically shown to audiences that by law should not see them, which would cause the advertiser to be in non-compliance of the laws applicable to its activity) or not validate them by default (in which case the ads will be shown far less, with a snowball financial impact for both the publisher and the advertiser).

In addition, the inability to use (without consent) indicators such as IP addresses, HTTP referrers and URL-based information such as UTM codes would lead to the inability to identify genuine *vs* fraudulent traffic (as consent would in any event never be given by bad actors or bots).
This would very rapidly be seized upon by bad actors, with the result that legitimate advertising budgets would be spent on fraudulent advertising, a significant portion of which would benefit terrorist organisations, organised crime and even malevolent state-sponsored actors.
This would moreover undermine established industry controls preventing individuals and business from harming others in the advertising ecosystem. Corporate sabotage could be easily achieved. For instance:

- A company wishing to get ahead of a competitor could sabotage the competitor with relative impunity by using a bot farm to spam the competitor's ads – this would use up the entirety of the competitor's advertising budget in mere days;
- a bad faith advertising agency could set up a website in a matter of hours (e.g. using artificial intelligence tools such as Generative AI), put all of the advertising budget of its clients into one website, and it could drain their revenue before disappearing.

Today, such behaviour is not possible, or is at the very least significantly more difficult, thanks to the self-regulatory framework that the industry has been able to put in place through the deployment of validation techniques using the aforementioned indicators.

Beyond such obvious bad faith examples, validation and verification techniques are critical to ensure trust in commercial relationships in the online advertising ecosystem. By way of simplification, if an advert costs X EUR to be displayed on website Y, the advertiser needs to know how often the ad has actually been displayed on the website (to a legitimate audience – see above); without any technical information being readable (without consent), that number of impressions will be at best an approximation, and more likely a purely fictional number. In other words, those techniques allow trust by permitting the verification of the numbers put forward by the publisher of website Y or any other intermediary along the advertising chain.

The aforementioned digital activities are not just relevant to online advertising but also to the provision of online content. For instance, in the event where content is placed behind a paywall, the publisher may seek to prevent access not only to (human) users who do not have a subscription but also unauthorised bots – all the while maintaining access for search engines (e.g. Google's Googlebot), in order to allow the content to be easily found. Certain circumvention techniques deployed by malicious users or bots involve masquerading as Googlebot; the aforementioned activities enable the deployment of additional verifications to prevent such abuse. i

Similarly, in relation to network and information security, it is critical that organisations be allowed to use indicators suggesting that a device is part of a botnet in order to mitigate the risk and likely impact of an attack such as a distributed denial-of-service (DDoS) attack. There are concerns that regulators might not view this as strictly necessary to the provision of a service to the user, even though in such a case it is not a legitimate user and the organisation should therefore be entitled to deny provision of the service on that basis. In any event, consent would be nonsensical, as the bad actor would never give his or her consent.

Put differently, requiring consent for the use of such technologies would prevent proper validation – which in turn will only penalise good actors and bring no benefit whatsoever to (good) end-users.

2. Turbocharged consent banners

Beyond the issue of validation, consent for the aforementioned digital activities would have the perhaps unintended consequence of leading to more complicated consent mechanisms covering more data types.

While "cookie banners" are a widely adopted practice, expanding them to cover additional types of technologies may end up making them overcomplicated, in particular if regulators require consent to be given per technology or purpose without any bundling being possible or if regulators insist on the provision of technical explanations for each technology.

This is not a theoretical concern:

- Looking at current practices regarding Art. 5(3) ePD, regulators often request that at the latest in a second layer the cookie consent be split per category or even per individual cookie – in spite of the fact that Art. 5(3) ePD merely requests consent for non-necessary cookies. The reason for this interpretation appears to be that under (their interpretation of) the GDPR, regulators consider that e.g. analytics, social media plugins and advertising relate to distinct, (allegedly) non-necessary purposes, and that they therefore have to be de-coupled.
- Under the GDPR, in relation to direct marketing, some supervisory authorities have already stated that consent to direct marketing must specify the means of communication, and that any means not explicitly indicated are not covered by such consent[8].

Combining these two perspectives, it appears likely that some authorities will require the means of storage or access to be described at length, with identification of each individual technology used for "storage" or "access", and potentially even that in a second layer of the consent management page each specific element be identified and feature its own consent toggle or checkbox.

[8] See for instance Belgian Data Protection Authority, *Recommendation 01/2020 regarding the processing of personal data for direct marketing purposes*, 17 January 2020, para. 198, available in French and Dutch – machine translation: *"Moreover, the fact that consent was given to receive advertising or informative messages via e-mail does not mean that consent was also given to receive telephone calls. It is therefore necessary to ensure that unambiguous consent is obtained both on the content of the messages and on the means used for this purpose. Thus, if multiple means of communication can be used, consent requests should be split up, rather than making a single request."*

Such requirements from authorities might involve the need to share extensive and intricate technical details with users, which represents first the need for a time-consuming documentation process for organisations. Such practices may not significantly benefit user understanding, due to the complexity of the information involved (in particular when it is not simultaneously personal data).
In addition, the sharing of such information may present risks in and of itself to the security objectives of several of the aforementioned digital activities. For instance, providing detailed information about non-personal technical data might inadvertently disclose sensitive details on how the organisation combats fraud technically, potentially allowing fraudsters to exploit vulnerabilities and bypass certain security processes.

The only way to avoid such complexity – and the negative impact that this has on intelligibility – would be for the EDPB and all other relevant regulators to adopt a clear, unambiguous statement explicitly confirming that it is possible to bundle all such technologies together into one or more simple terms, without this affecting the validity of any consent given.

In addition, due to the fact that this interpretation by the EDPB marks a departure from previous guidance (as indicated above), all organisations will be faced with the question of whether such bundling of technologies for consent negates any consent given beforehand, at a time when only actual storage and access (e.g. the placing of cookies or HTML5 storage files on a device, and the reading thereof) were deemed to be part of the scope of Art. 5(3) ePD.

In summary, it is crucial for the EDPB to aid organisations in finding a balance between meeting regulatory requirements and safeguarding sensitive information for the sustainable operation of their services, ensuring that these regulatory demands contribute practical value to subscribers and end-users.

3. “Consent for everything” favours privacy intrusiveness and centralised solutions

An additional effect of regulatory requirements for consent for the aforementioned digital activities would be that privacy-friendly alternatives become less desirable.

Indeed, if consent is needed anyway both for (i) privacy-intrusive models using actively retrieved information and (ii) privacy-focussed non-personal data models using passively received information, there seems to be little incentive under the ePR to innovate to a privacy-centric or less intrusive approach. In other words, this may create a temptation for companies to ask for consent for “as much as possible” and to go for the most invasive technique.

Some organisations even fear that this might end up placing more commercial power into the hands of large online publishers and platforms, as users might end up opting to only give their consent to those select few publishers and platforms.

From that perspective, the Proposed Guidelines might miss what they assume to be the intended target of the EDPB, namely privacy-intrusive profiling and tracking of individual users as perpetuated by new technologies, and might instead restrict innovation, including that which could benefit individual users.

E. Additional concerns for telecommunications services

Beyond the concerns highlighted above in relation to digital activities in general, there are moreover concerns among organisations in the telecommunications sector that the EDPB's interpretation of Art. 5(3) ePD may lead that provision to apply also to all information that such organisations are led to process in the context of telecommunications, due to the EDPB's broad interpretation of the concepts of "access" and "storage".

By way of an illustration, the ePD requires telecommunication operators to erase or anonymise any traffic data "when it is no longer needed for the purpose of the transmission of a communication" (Art. 6(1) ePD), unless specific exceptions – one of which being the permission for telecommunication operators to use traffic data for the purposes of customer billing and interconnection payments (Art. 6(2) ePD). For phone calls, the phone number of the recipient is an example of traffic data used for billing purposes (as it e.g. helps to determine whether the number being called is a premium number requiring an additional charge, in which country the recipient is and thus whether any roaming charges may apply, etc.). Yet that phone number originates from the caller's phone: when a user wishes to call someone, he or she inputs the phone number of the recipient on his or her phone (i.e. terminal equipment), and that phone number is then automatically sent as part of the communication protocols applicable to phone communications.

Following the EDPB's broad interpretation, the phone number would therefore have been "stored" even temporarily on the terminal equipment and the telecom operator would then have "gained access" to it simply by virtue of the fact that this information is sent to the telecom operator as part of the communication protocol. In other words, following the EDPB's broad interpretation, Art. 5(3) ePD would apply.

This in turns raises questions as to the compatibility of such a scope of Art. 5(3) ePD, which requires consent unless one of two exemptions can be established, with Article 6(2) ePD, which explicitly permits the processing of traffic data (outside of the actual transmission of a telecommunication) for billing or interconnection purposes.

Consent does not appear to be a viable justification for billing or interconnection payments under Art. 5(3) ePD. Indeed, telecom operators cannot be expected to offer services for free in the event of refusal to give consent to the use of traffic data for billing purposes and interconnection payments.

Yet because each legal provision must be interpreted as having a purpose, Art. 6(2) ePD's existence suggests one of the following options:

a) "Storage" and "gaining access" must be interpreted more restrictively than the EDPB states in its Proposed Guidelines, or
b) Art. 6(2) ePD must be viewed as a legal justification in favour of a broad interpretation of "strict necessity" in Art. 5(3) ePD's "service" exception, given that interconnection payments and billing all relate to post-factum remuneration – directly and indirectly – of all parties in the communication chain (the telecom operator itself and all intermediaries), paving the way for an application of the "service" exception also to storage and access needed for other indirect forms of remuneration (e.g. online advertising), or

c) Art. 6(2) ePD must be regarded as an exception to Art. 5(3) ePD, despite the absence of a "legal obligation/authorisation" exception under Art. 5(3) ePD – in which case any (EU) law can deviate from Art. 5(3) ePD.

Clarity on the EDPB's position in that respect would be critical, in order to provide greater legal certainty to organisations active in the telecommunications sector regarding the legal justification for a large swath of their activities.

In addition to the use of traffic data for billing purposes and interconnection payments, data retention provides an additional illustration of inconsistencies. National rules in Member States on data retention obligations for telecom operators typically include a clear legal obligation for such operators to collect and store certain categories of information (including personal data depending on the nature of the subscriber), some of which may fall within the scope of Art. 5(3) ePD based on the EDPB's new interpretation. Article 15(1) ePD allows exceptions to notably Article 5 ePD (in full) *"when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system"*. However, if the national legislation does not refer to the full scope of Article 5 ePD (and therefore including 5(3)) and is instead limited to e.g. Article 5(1) and (2) ePD, there will be the question of whether telecom operators are permitted by EU law to comply with their own statutory obligations in terms of data retention. As above, in the absence of further clarifications, the EDPB's position in the Proposed Guidelines may be viewed as creating legal uncertainty.

The topic of fraud prevention was highlighted above in relation to digital activities in general and advertising in particular, yet it is also a topic of specific importance in relation to telecom services. Telecom operators frequently process traffic and technical data, working on the basis of both legal obligations and legitimate interests to combat network fraud. This dual approach, as illustrated by Art. 122(4) of the Belgian Act on Electronic Communications (**BAEC**), which partially transposes the ePD, demonstrates the intricate balance between legal requirements and complementary processing activities often based on the operators' and/or subscribers' legitimate interests. However, the broad definitions and strict interpretations included in the EDPB's Proposed Guidelines may hamper such critical processing, in particular as regards technical data that is crucial for fraud prevention. This potential restriction clashes with legislative efforts aimed specifically at fighting telecom fraud (see e.g. Art. 121/8, 122(4) and 125(7) BAEC), such as the fight against SMS-based phishing or "smishing".

Beyond the fight against fraud, telecom operators are also required to assess and continuously strengthen the security of their networks and services. Telecom operators has notably expressed concern that a broadened scope Art. 5(3) ePD and the strict interpretation of its consent exemptions would prevent operators from performing certain security verifications, such as preventively assessing whether a device is generating a high consumption and might be hacked.

The absence of any guidance on audience measurement and service improvement in relation to an expanded scope of Art. 5(3) ePD moreover prevents telecom operators from using such techniques to assess the working of devices such as Wi-Fi access points, given the practical difficulties in ensuring not only that a consent request can be intelligible (due to the technical nature of the information being analysed) but even that a consent request can ever be made available to the subscriber or user, let alone that such consent can be easily withdrawn or otherwise managed.

The Proposed Guidelines do include some considerations that have a very specific telecom component to them, such as the reference to private networks as a situation to which Art. 5(3) ePD would not apply. However, the current wording in that respect (in para. 25 of the Proposed Guidelines) is insufficiently clear, as it indicates that *"the fact that the network is made available to a limited subset of the public (for example, subscribers, whether paying or not, subject to eligibility conditions) does not make such a network private"*. It would be important for the EDPB to then clarify under which circumstances an organisation can be deemed to be using a private network, by way of certain illustrations.

Such clarifications are particularly important when looking at the broad range of services that telecom operators provide, as some might be deemed to be covered or not depending on the precise meaning of e.g. "private networks" (for instance, services whereby technical data related to user devices is used to optimise the use of a network and to address technology-specific issues might or might not be covered depending on the nature of the network).
In relation to the latter, it is important to stress that troubleshooting is a fundamental aspect of maintaining network functionality and ensuring a seamless user experience. Some of the information that enables troubleshooting may be a set of statistics, information regarding the state of a device, a report. Automatic detection of issues, such as poor network coverage in a customer's house or premises, may trigger automated guidance through mobile applications. Because of its practical importance and the benefits of troubleshooting, consent is not a viable option (and even if it was, such consent would not likely be considered freely given by regulators), while the "service" exemption would likely only apply if regulators admit that strict necessity for the provision of a service also covers customer support.
This reinforces the observation that clear guidelines on the consent exemptions under Art. 5(3) ePD are crucial to navigating the delicate balance between operational efficiency, user experience enhancement, and compliance with privacy and data protection rules.

Finally, in a similar manner to other industries such as the advertising industry (as described above), telecom operators implement, on top of strict statutory obligations, measures that increase the overall protection of the operator and users/subscribers.
For instance, telecom operators pour significant efforts into combating SIM card fraud and identity theft, on top of the statutory obligations to identify subscribers and users. While not necessarily mandated by strict statutory obligations, such practices have become industry standards for safeguarding users and maintaining the integrity of telecommunication services.

Depending on the state of legislation in each EU Member State, the telecom operator might resort to additional measures such as enhanced identity verification, real-time monitoring (to detect unusual or suspicious patterns of sim card activation, usage or changes to account details), multi-factor authentication, anti-sim swap fraud measures (e.g. putting in place a procedure and notification system to alert customers in case of SIM card swap requests), measures against simboxing etc. These efforts could be impacted by a broad and strict interpretation of Art. 5(3) ePD.

In other words, a broad interpretation of "storage" and "gaining access", without careful consideration for the exceptions to the consent requirement linked thereto, would not only raise concerns regarding digital advertising and content, but also regarding the very telecommunications services that enable them.

IV. Final considerations

Taking all of the above into account, the organisations that asked us to file these submissions on their behalf request the EDPB to take the following actions in relation to the Proposed Guidelines, with a view to their finalisation:

- Re-evaluating the EDPB's authority to adopt guidelines such as the Proposed Guidelines and (i) restricting the scope of the Proposed Guidelines to *only* the material and territorial scope of the GDPR or (ii) transforming the Proposed Guidelines into mere recommendations, ideally with also the support of all competent regulators;

- Restricting the scope of the notions of "access" and "storage" under Art. 5(3) ePD to active storage specifically directed by the entity to whom the obligations under that provision apply, and active access to terminal equipment on the initiative of such entity;
    - In this context, bringing the (thus adapted) Proposed Guidelines in line with established positions of regulators, with a view to re-creating legal certainty, notably as regards information automatically transmitted by virtue of general communication protocols such as TCP/IP;

- Providing guidance on how the consent exemptions would apply, based on the EDPB's (thus adapted) understanding of the notions of "access" and "storage";
    - Notably, in relation to the "service" consent exemption, confirming that:
        - the service provider is free to define a service the way it sees fit, and
        - the activities that underlie a service, from its conception all the way to actual provision of the service to a given user as well as the reuse of lessons from a given user's interaction in order to improve the service for a subsequent user, all can be deemed (subject to justification of course) to be covered by the concept of strict necessity that defines the scope of that "service" consent exemption;
    - In addition, confirming that such "service" exemption can also encompass any "access" or "storage" that is statutorily authorised or required for the activities of the relevant service provider, as well as any "access" or "storage" for validation or verification purposes;

- In relation to consent, confirming that organisations are permitted to bundle a broad range of technologies covered by Art. 5(3) ePD together into one or more simple terms in any consent request form, without this affecting the validity of any consent given;

- Also in relation to consent, confirming that any such bundling of technologies further to an expansion of the scope of Art. 5(3) ePD (compared to the most recent guidance of authorities) does not negate any consent given beforehand;

- Increasing legal certainty by anticipating and avoiding contradictions or inconsistencies with other statutorily required use of information, such as the other provisions of the ePrivacy Directive and obligations for electronic communication service providers.

* *
*

We thank you for taking the above into consideration and remain at your entire disposal to provide any additional clarifications you may require.

Yours sincerely,

Peter Craddock