Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CIPL Response to the EDPB Public Consultation on Draft Guidelines 02/2023 on the Technical Scope of Art. 5(3) of ePrivacy Directive

Centre for Information Policy Leadership (CIPL)

17 January 2024

CIPL Response to the EDPB Public Consultation on Draft Guidelines 02/2023

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on the European Data Protection Board's (EDPB) draft Guidelines 02/2023 on the technical scope of Art. 5(3) of the ePrivacy Directive. CIPL appreciates the EDPB's aim to provide more regulatory clarity and develop guidelines to ensure consistent application of data protection and privacy principles throughout the EU. We do, however, have a number of concerns with the current draft of the Guidelines. Below, CIPL outlines these concerns in more detail and provides recommendations for further clarification.

In the context of EDPB Draft Guidelines 02/2023, CIPL strongly suggests to:

- Provide further clarification on the applicability of the Guidelines, particularly regarding the coordination and cooperation between competent ePrivacy Directive authorities that are not members of the EDPB.
- Ensure that the Guidelines and specifically the proposed novel interpretation of concepts such as *gaining access*, *stored information* and *terminal equipment* continue to align with the existing text and legislative intent of the ePD.
- Differentiate sufficiently between technologies, their applications, and the feasibility of the proposed scope and provide concrete examples of how organisations can feasibly implement use cases identified in the proposed Guidelines.
- Provide guidance on how the existing exemptions under the ePD would apply to scenarios that are potentially brought into scope by the Guidelines.
- Align guidance with broader policy and legal context, considering user experience and consent fatigue concerns and giving due regard to privacy-enhancing technologies.

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

I. COMPETENCE OF THE EDPB

CIPL would like to respectfully point out that the national data protection authorities (and EDPB members) are not the sole competent authorities under the ePD in all Member States.[2] Even though the Guidelines, in their current form, have the potential to expand the scope of the ePD extensively through the suggested revised interpretation of certain terminology (see below in more detail), they do not provide any clarity regarding competence issues and how the Guidelines would be applied in practice by a variety of regulators. In the absence of information on any consultation process including all competent authorities, this raises questions about whether the Guidelines will apply only to those Member States whose competent ePrivacy regulator is also a national member of the EDPB or only in relation to personal data processing in the scope of the ePD, for instance.

To avoid a fragmented approach that would lead to legal uncertainty in an already complex piece of legislation, the final text should clarify the application of these guidelines in relation to different national competent authorities. This is all the more relevant given that the guidelines also put forward interpretations regarding the definitions of Electronic Communications Networks (ECN) and the public/private character of ECN, which should be aligned with BEREC's and NRA's interpretations under the European Electronic Communications Code.

II. THE NOTION OF "GAINING ACCESS", "STORED INFORMATION" AND "TERMINAL EQUIPMENT"

1. "Gaining Access"

The Guidelines confirm that ePD applies where the entity *takes active steps towards gaining access* to the information stored in the terminal equipment.[3] "Taking active steps" implies a conscious action by the entity seeking access, similar to entering premises in the analogue world to obtain an object stored there. This view is also in line with, for instance, the interpretation by the German DSK,[4] which provided guidance on the German ePD implementing law in December 2022. The DSK indicates that "access" requires a targeting browser transmission and can specifically not be end-user-activated, for instance.[5] Transmissions happening automatically or due to the settings of the terminal equipment (such as the browser settings) were explicitly excluded from the scope of ePD and, as per the example above, the implementing law by the DSK.[6] On the other hand, where information was actively sought from the end-user, for instance, by deploying a script, eDP would apply.

---

[2] According to the European Commission, several Member States have dedicated other regulators than the data protection authority regarding the ePrivacy Directive, namely Belgium, Denmark and Hungary. Some Member States share the ePrivacy Directives competence together with data protection authority and another sectorial regulator, namely Austria, Bulgaria, Cyprus, Czech Republic, Germany, Greece, Finland, France, Croatia, Ireland, Latvia, Malta, the Netherlands, Poland, Portugal, Sweden, Slovenia and Slovakia; available at: https://digital-strategy.ec.europa.eu/en/library/list-personal-data-protection-competent-authorities.

[3] EDPB Draft Guidelines 02/2023, p. 8.

[4] The Conference of the Independent Data Protection Authorities of Germany – Datenschutzkonferenz.

[5] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. December 2021, para (21), p. 9.

[6] Examples specifically provided were IP addresses, URLs, user agent strings, and language settings.

The proposed EDPB guidelines include in the scope of "gaining access" situations when:

- accessing entity wishes to gain access to information stored in the terminal equipment and actively takes steps towards that end;
- when accessing entity distributes software on the terminal of the user that then proactively calls an API endpoint over the network;
- ***but also*** in cases where protocols are in use "that imply the proactive *sending of information by the terminal equipment*, which may be processed by the receiving entity".

This last point could potentially include cases where information is sent automatically following an established communication protocol, which forms the basis of internet communication (e.g., an IP address). The EDPB's interpretation risks categorising the mere act of reading a URL received by a device as "access" even where there was no active querying for the information.

Similarly, IP addresses are routinely transmitted as part of Internet communication protocols. The Guidelines propose a broad interpretation suggesting that any developer or implementer of a communication protocol might be considered as the instructing party, thus bringing the collection or receipt of IP addresses within the ePD scope—even where these were not stored on a user's device (see also below). Essentially, routine webpage access by individuals could disproportionately fall under Article 5(3).[7]

Such extensive interpretation would leave little if any communication over the internet outside the scope of the ePD since all internet communications require the transmission of certain information as defined by the relevant communication protocol (data related to an email that was once (temporarily) stored on the sender's device, for instance). This broad reading, divorced from an actual **act** of *gaining access* directly linked to the entity intending to benefit from it, is misaligned with Recital 24 ePD, which seeks to protect users' terminal equipment from active intrusion that occurs without their knowledge that seriously intrudes upon their privacy. It is not evident to what extent the proposed new interpretation and expansion of the scope of the ePD beyond its legislative intent serves the aim of protecting privacy. Given the protection provided by the GDPR, it remains unclear where further protection is provided in instances of no (pixels) or minimal or ephemeral storage of data (see above) on the user device or third-party storage. Substantially revising the scope of the legislation is not in the power of the EDPB, however.

Additionally, the draft Guidelines do not sufficiently acknowledge the technical advances of Privacy Enhancing Technologies (PETs) over the past years.[8] For instance, on-device processing, one of the measures falling within the umbrella of privacy-enhancing technologies, can ensure that processing stays under the control of the end-user, which would be in line with the aim of the ePD.[9] Thus, PETs should be explicitly considered and further incentivised in the context of any guidance concerning technical measures to protect user privacy.

---

[7] It should be noted that IP addresses are not 'read' on user devices, and their transient nature limits their utility as trackers. Article 5(3) states specifically that the directive should not obstruct technical storage or access solely for the purpose of transmitting communication over an electronic communications network.

[8] Please see the recent CIPL Paper Privacy Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf.

2. "Stored Information"

Similarly, the EDPB's notion of what constitutes "stored information" in the sense of Article 5(3) of the ePD seems to expand the scope unreasonably. The wording of Article 5(3) ePD explicitly refers to "the gaining of access to information **already stored**". The proposed guidance appears to remove any restrictions on volume, medium, timing or even who stored the "information" and where. The guidelines specifically aim to include such ephemeral storage as RAM or CPU cache, expanding the scope not only to the use of *storage* capabilities of terminal equipment but also to the use of the *processing* capabilities of terminal equipment. These activities do not constitute *storage* within the meaning of the ePD, however, but instead stretch the interpretation of the clear wording of "already stored" of Article 5(3) beyond what seems linguistically possible and beyond the legislative intent. It also remains unclear how storage is affected in the context of terminal equipment powered by cloud-based technologies (e.g., devices without significant RAM/CPU that rely on cloud-based systems).

Furthermore, while the Guidelines clarify that storage and access are not cumulatively required for Art. 5(3) ePD to apply, they do not sufficiently delineate the distinct roles and responsibilities of the entity 'gaining access' as opposed to the entity 'storing information'. Consequently, both entities might be subjected to compliance with an array of transparency and consent obligations, adding to the complexity.

Considering the limited exceptions provided under ePD, this overly broad reading of "already stored" may ultimately result in any interaction with an end-user device that does not fall into one of the exceptions being subject to consent. Without further clarifications, this would, without a doubt, significantly impact how consent and user exceptions are managed, leading to further complexities for the user and technical challenges for organisations.

3. "Terminal Equipment"

Further clarification is also required with respect to the notion of "terminal equipment". The Guidelines' references to terminal equipment at present, particularly in relation to IoT devices, are not always consistent. As an example:

- Paragraph 15 suggests that a device functioning purely as a communication relay, without altering information, should not qualify as terminal equipment under Article 5(3) of ePD. According to paragraph 16, however, terminal equipment can potentially comprise multiple hardware components, which would then *collectively* constitute terminal equipment, such as smartphones, laptops, connected cars, connected TVs, and smart glasses.
- Paragraph 60 discusses a scenario with IoT devices connected through a relay device like a smartphone or a dedicated hub. Here, the data transmission to the relay might not fall under Article 5(3) ePD, where it does not use a public network. But when the relay transmits information to a remote server, this is deemed as being stored by a terminal, thus invoking Article 5(3) ePD.
- Paragraph 60 thus implies the smartphone can be the terminal, paragraph 15 excludes relay devices, and paragraph 16 suggests they may collectively be considered "the terminal equipment." Given these differing assertions, the Guidelines lack sufficient clarity on what precisely constitutes terminal equipment

- The guidelines also do not provide information on how consent requirements are to be met when the instructing entity and receiving entity are different or where multiple users/subscribers use the same terminal equipment (e.g. in a public library).

III. FURTHER OBSERVATIONS

Overall, CIPL would like to observe that the proposed Guidelines fail to sufficiently differentiate between the different technologies, their application or the feasibility of the proposed expanded scope. CIPL also misses a more in-depth view of the effect of the proposed expanded interpretation under the draft Guidelines on the individual and consideration of technical advances and the broader digital ecosystem.

1. Technical Applicability

The Guideline should provide concrete examples of how organisations can practically implement and operationalise the expanded interpretation of Art. 5(3) ePD in their day-to-day practices.

In the case of URL tracking, for example, URL tags that are at most stored on a user's terminal equipment "through the caching mechanism of the client-side software" cannot be managed technically in the same way as cookies or even pixels.[10] Rejecting cookies via a banner may also prevent pixel-dropping but is not applicable in the same way as URL tracking. URL tracking typically involves appending identifiers to URLs to track user interactions uniquely, enabling businesses to analyse content engagement. Simply rejecting cookies via a banner will not have the same effect. There is a broad spectrum of applicable cases for tracking technologies which present different levels of risk to the fundamental rights of a user and may form part of the expected user experience. The EDPB should provide a clear and pragmatic explanation of how these nuanced technical distinctions are to be managed and operationalised under the Guidelines.

Online identifiers are utilised for purposes such as enhancing service performance and quality, optimising user experience, and combating fraudulent activities or known CSAM material. It is imperative that any interpretation of Article 5(3) of the ePD is approached with a comprehensive understanding of the evolved nature of the services it encompasses. Such interpretations should more adequately reflect the technical necessities integral to both current and future digital services.

2. Exemptions

Despite the expanded scope of the application, the draft Guidelines remain silent on how existing exemptions might apply to scenarios that are pulled into scope (e.g., with respect to ephemeral information that is generated/stored by default in the terminal equipment, such as RAM or CPU cache). As an example, tracking based on IP addresses, which is specifically highlighted in the draft Guidelines, can be necessary for legal compliance. IP addresses are used to ensure that particular content is shown only to the user in a licensed territory or filter content that is deemed illegal or

[10] This, apart from the instances where URLs are not actively accessed but sent by the terminal equipment as part of routine protocols or browser settings.

inappropriate in a specific territory, for instance. There is also no indication that additional exemptions might be considered.

3. Broader Digital Strategy Context

Finally, CIPL would like to highlight that any guidance should be provided in a broader policy and legal context. The ePrivacy Directive and its provisions have been drafted over two decades ago. The original drafting of the ePD occurred in an era considerably different from our current digital landscape, particularly concerning information society services and electronic communication services. Despite efforts by European policymakers to revisit ePD, these efforts have remained stagnant since 2019.

The expansive interpretation of "access to terminal equipment" provisions would inevitably make even more digital interactions by individuals subject to their consent. Furthermore, since the ePD applies to personal and non-personal data, the expanded scope of the draft Guidelines could potentially bring additional activities within the scope of the consent requirement, including non-personalised content. This extended scope could ultimately lead to a scenario where obtaining consent becomes a prerequisite for loading a majority of web pages, including those featuring non-personalized content. However, broadening the interpretation of an essentially outdated Directive cannot replace the legislative process.

Meanwhile, the European Commission has acknowledged 'consent fatigue' as a significant concern in the context of the ongoing Cookie Pledge initiative.[11] The initiative aims to streamline cookie management and personalised advertising choices for consumers, with the premise of providing better information to consumers rather than an excessive and overwhelming flood of consent requests and information notices. By contrast, the current draft guidelines would increase the complexity for users and organisations alike and potentially add numerous additional consent requests without an evident increase in the protection of user rights.

The responsibility for scrutinising data processing practices should not be placed exclusively on the individual but should be with organisations. Merely increasing the number of consent requests does not inherently empower data subjects in relation to their fundamental rights. Instead, the emphasis should be on fostering organisational accountability measures, incentivising meaningful information notices and responsible data use.[12]

---

[11] European Commission, Cookie Pledge Initiative, available at https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/cookie-pledge_en.

[12] Centre for Information Policy Leadership, *What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework* available at https://www.informationpolicycentre.com/organizational-accountability.html; CIPL White Paper - *Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions* available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_in_data_protection_enforcement_-_how_regulators_consider_accountability_in_their_enforcement_decisions__6_oct_2021__3_.pdf.