SHOOSMITHS

The European Data Protection Board
Rue Wiertz 60,
B-1047
Brussels

1 Bow Churchyard
London
EC4M 9DQ
T 03700 864000
F 03700 864001

Delivered: By E-mail

Date 18 January 2024

Dear Sir

CALL FOR VIEWS: GUIDELINES 2/2023 ON TECHNICAL SCOPE OF ARTICLE 5(3) OF EPRIVACY DIRECTIVE (ePD) ADOPTED ON 16 NOVEMBER 2023

I am writing on behalf of our Privacy and Data team in response to your call for views in respect of the consultation on the Guidelines 2/2023 on the Technical Scope of Article 5(3) of ePrivacy Directive (**Guidelines**).

For ease of reference, the views below are separated into the relevant sections of the Guidelines. Capitalised terms have the meaning given to them in the Guidelines, unless otherwise stated.

Section 2.5 – Notion of 'gaining access'

Paragraph 31 of the Guidelines states that "*Whenever the accessing entity wishes to gain access to the information stored in the terminal equipment and actively takes steps towards that end, Article 5(3) ePD would apply"*. The Guidelines also clarify at paragraph 33 that "*one entity may have used protocols that imply the proactive sending of information by the terminal equipment which may be processed by the receiving entity."* This has the effect of also covering IP addresses and URLs (along with other types of information). In accessing the internet, many situations occur whereby information is transmitted automatically and passively by virtue of a user accessing a particular webpage. For example, the public IP address of the device and site-based tracking the URL of the called website. There is no direct instruction to access the Information and it is not targeted. The transmission is automatic by the very nature of how the internet works.

If this interpretation of 'gaining access' remains, it will have the impact of significantly broadening the scope of the application of the ePD to any situation which may reflect an interaction with a user's terminal equipment, including all past, present, active, passive, direct or indirect interactions.

Additionally, the linguistic nature of the verb 'access' suggests an active movement or action. The Guidelines however now extend the definition of the legislature's choice of an active word:

'access', to include passive actions. On reading Recital 24 ePD regarding spyware, "*devices can enter the user's terminal without their knowledge in order to gain access to the information, to store hidden information or to trace the activities of the user..".* The language of the recital speaks of active 'access' therefore it is logical this interpretation of 'access' should apply across the entire text of the ePD.

Further, should the transmission of IP addresses, URLs and other passive and automatic transmissions be considered 'access' under Article 5(3) ePD, failure to obtain the requisite consent would effectively render any interaction with a computer permissible only where the accessing party can rely on one of the two exemptions to the consent requirement, which is wholly impractical and not reflective of any current implementation of the ePD in practice. If consent is sought, the rise in the cookie-like consent requests a user would be required to click through on using every piece of software, app and webpage to allow it to function on a user's device, to ensure compliance, would be as unworkable as it sounds.

We invite the EDPB to revisit whether passive transmissions, and in particular IP addresses and URLs should be included within the scope of "gaining access" in Article 5(3) ePD.

Section 2.6 – Notions of 'Stored Information' and 'Storage'

Paragraph 34 of the Guidelines: "*Placing information on a physical electronic storage medium that is part of a user or subscriber's terminal equipment*" raises the question on the breadth of what is considered 'storage' within the Guidelines.

It is acknowledged that the Guidelines do not contain any upper or lower limits on the length of time that information must persist on a medium to be considered "stored", or on the type of medium for which "storage" takes place. The Guidelines also confirm RAM and CPU cache "*are not excluded from the scope of application*" (paragraph 3). This represents a significant broadening of the pre-established 'cookie rule' to information generated in a transient manner or purely for caching being caught by Article 5(3) ePD and therefore requiring consent. This position will present issues with the way that every user or subscriber interacts with the internet and the functionality of every website. For example, both RAM and cache are integral to the functioning of all websites and, unless one of the exemptions applies, failure to receive consent from users/subscribers will lead to websites suffering severe performance issues and rendering most unusable. The alternative would lead to those practical issues highlighted above.

Additionally Article 5(3) ePD states "*the gaining of access to information already stored*" which denotes some concept of time elapsing. In the case of information which is very briefly stored in RAM/cache, this requires further clarification.

We invite the EDPB to provide clarification on whether the placing of transient information which is necessary for the functionality of the media/communication is considered a form of access of information "already stored".

Section 2.3 Notion of "Terminal Equipment of a Subscriber or User"

The Guidelines note that Article 5(3) ePD applies to terminal equipment "*associated"* with a "*user*" or "*subscriber*", including where users or subscribers may own, rent or have been provided with terminal equipment, or where there are multiple users of the terminal equipment i.e. in the case of a connected car. It is however not addressed in the Guidelines how the

consent mechanism at Article 5(3) ePD is intended to work in cases of multiple users for a single terminal equipment. For example will the consent of a corporate subscriber, installing software of its employee users be sufficient or will each user be required to provide individual consent (which will be administratively complex to manage and maintain, particularly where GDPR also applies)?

Additionally, the examples within the Guidelines of what is considered terminal equipment regarding the internet of things (**IoT**) contain contradictions:

- paragraph 15 states "*Whenever a device is not an endpoint of a communication and only conveys information without performing any modifications to that information, it would not be considered as the terminal equipment in that context. Hence, if a device solely acts as a communication relay, it should not be considered a terminal equipment under Article 5(3) ePD*", suggesting the IoT device is the terminal equipment;
- paragraph 16 states "*A terminal equipment may be comprised of any number of individual pieces of hardware, which together form the terminal equipment*" suggesting the IoT device and the smartphone together is the terminal equipment;
- however paragraph 60 states "*In the case of IoT devices connected to the network via a relay device (a smartphone, a dedicated hub, etc.) with a purely point to point connection between the IoT device and the relay device, the transmission of data to the relay could fall outside of the Article 5(3) ePD as the communication does not take place on a public communication network. However, the information received by the relay device would be considered stored by a terminal and Article 5(3) ePD would apply as soon as this relay is instructed to send that information to a remote server*" suggesting a smartphone is the terminal equipment.

We invite the EDPB to clarify its interpretation of "terminal equipment".

Section 3 – Use Cases, the meaning of "abuse"

Paragraph 42 of the Guidelines refer to context data, caching mechanisms or other functionality and states that "*the abuse of those mechanisms (for example in the context of fingerprinting or tracking of resource identifiers) can lead to the application of Article 5(3) ePD."* The Guidelines do not expand upon what is meant by "abuse". From the context, it can be considered that any use of the information outside of the strict purpose of transmission between user and end-point receiver, would be considered "abuse" and therefore lead to the application of Article 5(3) ePD. As set out above, a number of identifiers contained within the information are inherent properties of the communication/transmission and are not actively stored nor extracted directly from a device. As above, this is a significant deviation from market practice and the fundamental way the internet works. If consent were requested in these situations, this would have a significantly detrimental impact on the usability and functionality of software/websites.

We invite further guidance from the EDPB on its definition of "abuse" in this context.

Yours faithfully

The Privacy & Data Team

Shoosmiths LLP