BCLP. Client Intelligent

Insights

EDPB EXPLAINS EU EPRIVACY COOKIE RULES APPLY TO EMERGING ONLINE TRACKING TOOLS

NEW RECIPES – SAME FLAVOUR?

Nov 30, 2023

SUMMARY

On 14 November 2023, the European Data Protection Board **(EDPB)** adopted guidelines on the technical scope of Article 5(3) of the ePrivacy Directive (Directive 2002/58/EC, as amended) **(ePD)**. This reflects the EDPB's intent to ensure that privacy laws keep pace with the rapidly evolving digital environment and helps fill a lacuna left by the stalled draft EU ePrivacy Regulation, intended to reform and update the ePD. The guidelines also anticipate an acceleration in new online tracking techniques being developed to address the withdrawal of support for third party cookies, which are at the core of the current AdTech ecosystem.

The EDPB is concerned to prevent new tracking technologies from circumventing the ePD's controls (or to prevent developers from considering themselves to fall outside of them). The guidelines specifically call out the following technologies as capable of (though not inevitably) coming within scope: (1) URL and pixel tracking; (2) local processing; (3) tracking based on IP address only; (4) IoT data reporting; (5) unique identifiers. The guidelines build on prior opinions covering the Cookie Consent Exemption and Device Fingerprinting issued by the precursor body to the EDPB.

COOKIE CONSENT

According to Article 5(3) of the ePD (the so-called "cookie consent" rule), *"the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user"* is only allowed on the basis of either: (i) prior, informed consent or (ii) technical necessity for specific purposes. The consent must be based on clear and comprehensive information provided to the user (or subscriber) about the purposes of the storage or access.

ANALYSIS OF THE KEY ELEMENTS

The following key elements are required in order to trigger the Article 5(3) transparency and consent rule.

- **Information:** first and foremost 'information' is not limited to 'personal data'; it covers any data stored on a user's device. This is because the ePD is a "privacy preserving legal instrument aiming to protect the confidentiality of communications and the integrity of devices" of natural persons and also legal persons. This will have increasing implications for IoT connected devices.

- **Terminal Equipment:** this can encompass a range of hardware, such as smartphones, laptops, connected cars, connected TVs or smart glasses. The guidelines emphasise that the device must be the 'endpoint' of a communication (and therefore the final interface with the user), rather than something intermediate, like a communication relay.

- **Electronic Communications Network:** this is described as any network system that allows transmission of electronic signals between its nodes, regardless of the equipment and protocols used. The network can be permanent or dynamic/intermittent. However, to fall within the ePD it needs to be publicly available to some extent, even if access is limited to a subset of the public, e.g. paying subscribers.

- **Gaining Access:** taking steps, such as sending specific instructions to the terminal equipment and then receiving back targeted information, is considered 'accessing' (this is how cookies work, in fact). Similarly, distributing software to a user's terminal device which has this effect is also caught by Article 5(3). The guidelines note that the party instructing the terminal to send the information does not necessarily need to be the same as the party receiving it (although query which party is then accessing the information – presumably just the latter?).

- **Stored Information and Storage:** storage is the placing of information on a physical electronic storage mechanism that is part of the user's or subscriber's terminal equipment. For the purposes of the ePD, the information can be stored by the user, or by a hardware manufacturer (e.g. MAC address), or it can include information resulting from sensors in the terminal equipment.

- When it comes to information stored by third parties on a terminal device, typically this does not occur as a result of a third party having direct access to a user's terminal device. Rather, it takes place through instructions initiated by the third party causing software on the device to generate (and store) specific information. The EDPB notes that there is no minimum or maximum period for such information to be stored (indicating that it can include transitory storage, such as caching).

USE CASES

The guidelines set out the EDPB's rationale and technical analysis for considering the ePD is likely to apply to many frequently-used online tracking technologies. Some of these are mentioned below.

The EDPB confirms that the use of **tracking pixels and URLs/links** is unlikely to escape the scope of Article 5(3). This is not unexpected, however the reasoning is more explicit than previously provided.

The position on **IP address tracking** is more nuanced, with the guidelines noting that only certain types would be caught. However, in view of the technical complexities (linked to the features of IPv4 and IPv6), the EDPB advises entities carrying out any IP address tracking to ensure compliance with the consent and notice requirements of Article 5(3) ePD, unless the accessing entities can ensure the specific IP address does not originate from the terminal equipment of the user.

IoT (internet of things) devices produce information continuously over time, typically through embedded sensors. Such information is then often made available to a remote server although the method of collection / transmission will vary in practice. Where IoT devices have a direct connection to a public communication network, e.g. through a network card or Wi-Fi, they are likely to be in scope of the ePD's Article 5(3). The ePD would apply because the instruction of the IoT device to send the stored data to the remote server amounts to 'a gaining of access'.

STEPS TO CONSIDER NOW

- **Review of current practices:** for website operators with significant EU (or UK) visitors, this would be a good time to review the range of tracking technologies in use. This should include IP address tracking, pixel and URL tracking as well as the more familiar "cookies". Adjustments may be needed to the privacy notice and consent-collecting mechanism in use. Organisations using marketing pixels in their customer email communications could similarly benefit from a check-up of their practices and notices provided.
- **IoT device manufacturers:** since the data being transmitted by an IoT device does not need to be 'personal data', the guidelines illustrate the breadth of the ePD's scope. This indicates that the EDPB and national regulators are looking for transparency around such data transmissions (characterised as 'access'). Where there is no clear, technical necessity for the 'access', an effective consent mechanism will also need to be engineered, placing demands upon designers and manufacturers.

The guidelines are subject to public consultation until 28 December 2023 meaning that adjustments may be made in a subsequent revision.

If you would like to discuss anything raised in this briefing, please contact Geraldine Scali or your usual BCLP contact.

Read the full guidelines >

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483