Published on *The National Law Review* https://natlawreview.com

Why Every Company with Digital Activities Should Comment on the EDPB's New ePrivacy Guidelines

Article By:

Peter Craddock

So much for tackling consent fatigue. The short version: If unchanged, the new EDPB guidelines on what is known as the "cookie" rule would extend that rule to cover nearly every communication over the Internet and any use of software on a computer. Your business is probably more impacted than you might think, and it is important for you to take part in the public consultation that runs until 28 December 2023 – so reach out rapidly.

The ePrivacy Directive (2002/58/EC) is a misunderstood piece of legislation. While the public often links cookie banners to the General Data Protection Regulation (GDPR) of 2016, they actually stem from Article 5(3) of the ePrivacy Directive. This provision, as strengthened in 2009, requires EU Member States to ensure that "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user" is prohibited unless (i) the subscriber or user has consented to this storage/access, (ii) that storage/access is *"for the sole purpose of carrying out the transmission of a communication over an electronic communications network"* or (iii) that storage/access is "strictly necessary" for the provision of an *"information society service* [read: digital service] *explicitly requested by the subscriber or user"*.

In practice, therefore: no cookies or similar files can be placed on your device (for instance a computer or a smartphone) or accessed on your device if none of those three conditions is met (consent – which must meet the GDPR consent requirements; "strictly necessary" for a digital service;

or for the sole purpose of transmission of an electronic communication).

On 16 November 2023, the European Data Protection Board (EDPB) published its new Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive. The legal value of those guidelines is yet to be determined, given that the EDPB does not comprise all national authorities with the power to enforce the local implementation of that ePrivacy provision), and there are arguments to say that the EDPB did not have the authority to adopt "guidelines" on the topic (see a more detailed analysis here).

In these guidelines, the EDPB sets out a new interpretation of that provision: Article 5(3) of the ePrivacy Directive should apply not only to cookies and files stored on a device and (actively) accessed from a device but also to (i) any information that the device transmits automatically (such as the URL of a webpage being accessed or the public IP address of the Internet connection, sent automatically to make a connection possible with a website or application) as well as (ii) temporary information generated on that device and information stored ephemerally (i.e., not held on persistent storage, such as a hard drive). The consequence? Every bit of information that relates to a device, even indirectly (such as an IP address, tracking pixels, URLs visited, Internet-of-Things device reporting), is covered, regulating the simplest digital activities such as loading contextual advertising and running a script in Javascript to make a website seem more dynamic.

Is automatic receipt of information "access" to the terminal equipment sending that information?

The position in relation to Germany in particular reveals a fundamentally new approach regarding what constitutes "access".

In 2021, the German regulators collectively stated the following regarding the notion of "access" to a terminal equipment:

"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."" [machine translation]

One German regulator confirmed this again explicitly in 2022.

By way of comparison, in the new guidelines, the EDPB states that in its view, "access" can be both (i) a situation where *"the accessing entity […] proactively send[s] specific instructions to the terminal equipment in order to receive back the targeted information"* and (ii) a case where an *"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 second point may seem innocent and harmless, but it is leaned upon heavily by the EDPB to conclude that the fact that information is sent automatically following a communication protocol (e.g., an IP address) shows that there is an *"entity instructing the sending of information"*.

Beyond being linguistically problematic ("access" has an active connotation), this position makes any communication over the Internet "access" by the recipient, because **Internet communications all require the transmission of certain information as defined by the relevant communication protocol**.

To take an illustration perhaps not anticipated by the EDPB, e-mails could, following that logic, be passive "access". After all, the recipient is "accessing" the e-mail content and the sender's e-mail headers, such as the name that he or she configured for that e-mail account, i.e., information that was stored even temporarily on the sender's device during the drafting and sending of the e-mail and that is sent automatically because the developers of the relevant communication protocol (IMAP and POP being the main ones for sending e-mails) decided that this information would be sent for all e-mails. As a result, any further use of the content of e-mails would be subject to Article 5(3) of the ePrivacy Directive, following the EDPB's approach – which in turn means that the recipient would have to prove (i) the consent of the sender to the use of the e-mail or (ii) the fact that such use of that e-mail is strictly necessary to the provision of a digital

service that the sender explicitly requested. In practice, e-mail retention would overnight become illegal.

Why did the EDPB create this idea that the designer of a protocol is giving "instructions" to a device that mean that information will be "accessed" on the device? Likely because this was the only way for the EDPB to extend the scope of Article 5(3) of the ePrivacy Directive to cover IP addresses, which are frequently used in support of delivery of content and ads (whether personalised or not) and in support of analytics (for instance, monitoring usage of a website or app).

However, the end should not justify the means, and the means here create a significant broadening of the ePrivacy Directive's scope in a manner that does not appear to have ever been the intent of the EU legislator.

Is the transmission of information stored ephemerally really a form of access of information "already stored"?

The EDPB's position regarding information generated on a device and not stored in persistent storage such as a hard drive likely stems from the fact that the ePrivacy Regulation (if ever adopted) would foresee that it applies not only to the use of the storage capabilities of terminal equipment but also to the use of the processing capabilities of terminal equipment.

The technologies that the EDPB lists as being covered by Article 5(3) of the ePrivacy Directive (RAM and CPU cache) are inherently at best ephemeral "storage": information is temporarily "stored" in them purely because that information is actively being used by the device (RAM) or because it is frequently used and the computer decides on its own to store that information in a place that is even more rapidly available (CPU cache).

The EDPB's approach is problematic, first because the actual legal text talks about "the gaining of access to information **already** stored" (which introduces a notion of time – an instantaneous calculation could hardly be seen as "already" stored) and only uses examples of actual storage (such as cookies), without providing any illustrations that are more ephemeral.

Second, because – due to the central role of RAM and CPU cache in the way computers work – it means that no interaction with a computer is permitted unless you can show that there is (i) consent, (ii) strict necessity for provision of an explicitly requested digital service or (iii) necessity for the sole purpose of transmission of a communication. While many such interactions will fall within the “service” scenario, most companies will probably want to prepare an “information processing notice” (along the same lines as a cookie notice) for their software and websites, just to be on the safe side, in case a complainant or regulator challenges the applicability of the “service” exception. In other words, what may have been part of an initiative to combat consent fatigue may end up worsening it dramatically.

Why then should your company take part in the public consultation?

Irrespective of your sector and activities, if you have any digital activities, they will be impacted by these guidelines. Even if you only have one website, there may be elements on that website that could be challenged (e.g., an ad banner, even if it is contextual advertising or a “sign up for a newsletter” popup that appears to an individual who has not yet seen it on his or her device). If you use IP addresses for anti-fraud checks, if you use URL parameters to track how many people read your newsletters, this will be covered. Even the developer of the “phone” core application on your smartphone needs to pay attention, as the phone number of the recipient of a call could be considered to be “stored” on the sender’s phone (temporarily) and “accessed” by the recipient as a result of the communication protocol – so any further use by the recipient beyond the communication (e.g., lists of past calls) could be regulated under Article 5(3) ePrivacy Directive following the EDPB’s approach.

That broadening of the scope can severely **impact your company’s ability to deploy or use digital services and tools if you cannot rely on (i) GDPR-compliant consent or (ii) a strict necessity to provide a digital service explicitly requested by the user**.

This may seem to be a significant overreach and twisting of the words of the ePrivacy Directive – and to limit the risk for your business, it may be worthwhile responding to the public consultation (which runs until 28

December 2023).

Past consultations have shown that the EDPB usually sticks to its position. One notable exception was its adoption of a slightly more pragmatic approach in (only some parts of) its recommendations on “supplementary measures” for data transfers, but more often the changes appear to lead to a slight hardening of the EDPB’s position (see e.g., the recent administrative fines guidelines, which were barely modified and in fact were modified to propose even higher fines).

It therefore appears unlikely that the EDPB will suddenly restrict the scope of these guidelines or to clarify why the legislator might have intended for both ephemeral processing and passive “access” to be covered, but it may see fit to at least clarify its legal reasoning – which may come in handy in case of (likely) litigation in relation to the enforcement of the positions it sets out.

From that perspective, it may remain useful to submit comments on the guidelines.

National Law Review, Volumess XIII, Number 327