TO THE EUROPEAN DATA PROTECTION BOARD

Subject Feedback on Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, public consultation reference 2/2023

Comment

The applicability of the ePrivacy Directive Article 5(3) is an important subject, and it is good that the EDPB adopts guidelines concerning it. I especially welcome the guidance to interpret the four criteria of applying the ePrivacy Directive Article 5(3) as explained in the section 2 of the Guideline.

However, I wish to address the following issues to be taken into consideration in the Guidelines:

1) The ePrivacy Directive Article 5(3) should only be interpreted as the legislator intended in 2009 when the directive was amended.
2) The emergence of new tracking methods is "a critical data protection concern" as stated by the EDPB, and should thus be mitigated as such (i.e., through the GDPR) instead of applying the confidentiality of the electronic communications.
3) The ePrivacy Directive Article 5(3) is technology neutral.
4) Instead of instructing, what "can be subject to the applicability of Article 5(3) ePD", the EDPB should instruct what *most likely will* be subject to the applicability, and the EDPB should explain how each of the listed use cases fulfil all required criteria.
5) Too broad interpretation of "gaining of access" should be avoided to minimize unexpected applicability.
6) The ePrivacy Directive Article 5(3) is an exception from the Article 5(1), and it should be interpreted as such.

Reasoning

The ePrivacy Directive Article 5(3) should be interpreted as the legislator intended

The legislator amended the ePrivacy Directive 5(3) in 2009, when the original wording referring to the right to refuse processing was changed to refer to the consent as defined in the Data Protection Directive. The legislature has passed a law which needs to be enforced as such by the supervisory authorities using executive powers, and the law is interpreted by independent courts of law. According to the preambles of directive 2009/136/EC, the legislator intended to increase end-users' choice on certain information they send and receive, not to prevent service providers' ability to single out end-users – which was stipulated in the Data Protection Directive and later in the GDPR.

The EDPB has referred to the "tendency to circumvent the legal obligations provided by Article 5(3)" with technological development, which implicitly aims to broaden the scope of applicability of the Article 5(3). When it comes to the technical development which enables service providers to make more accurate conclusions of the end-users without triggering the wording of the ePrivacy Directive Article 5(3), there is nothing the EDPB can do about it. The tracking technologies have developed to function outside of the scope of accessing terminal device data because the legislator has chosen to request consent for storing and accessing certain data, not to use consent as the only legal basis for tracking.

The EDPB has found that new tracking methods cause a critical data protection concern. Instead of arguing for the broader interpretation of the existing legislation, the EDPB should consider advising the Commission on any issue related to the protection of personal data in the Union as per the GDPR Article 70(1)(b). If the legislative initiative by the Commission results in amending the law with a broad interpretation of processing requiring consent, the EDPB has better chances of enforcing it broadly.

Data Protection issues should be regulated by the GDPR, not by the ePrivacy Directive

In the Guideline, the EDPB has identified new tracking methods as a "data protection concern" but the solution focuses on the interpretation of accessing and storing

data on a terminal device. The ePrivacy Directive Article 5 only stipulates the confidentiality of communications whereas the General Data Protection Regulation stipulates any kind of directly or indirectly identifiable information processed for any purpose. It would make more sense to approach tracking through the GDPR than through the ePrivacy Directive.

The ePrivacy Directive 5(3) makes no difference between purposes of accessing or storing data on a terminal device if it does not fall within the exemptions of the Article 5(3). However, behavioural tracking on a website of a pharmacy without accessing device-specific information is more sensitive than providing non-essential functional cookies on a generic website. The difference between the *purposes* of processing the data on a terminal device can only be solved through the GDPR which also is the only guidance to recognise if the pharmacy-related tracking falls under the special categories of personal data.

The broad applicability of the ePrivacy Directive Article 5(3) broadens the use of the legal basis consent as defined in the GDPR at the expense of the other legal bases. A controller is entitled to base the processing on any legal basis when the criteria are met, and it is not desirable that a consent requirement as per the ePrivacy Directive differs from the GDPR. The CJEU has already ruled that IP address can be processed based on legitimate interests,[1] which means that the IP address can be *accessed* without consent and thus possibly used for various purposes. Unlike the section 3.3 of the Guideline expects, tracking based on accessing IP only can thus be subject to the consent requirement only as per the GDPR if the requirements for other bases are not met (or other applicable legislation), not by the ePrivacy Directive Article 5(3).

[1] C-582/14, Patrick Breyer v. Bundesrepublik Deutschland. German Federal institutions maintained websites which processed the IP address with the aim of preventing attacks and making it possible to prosecute 'pirates' – neither of which was for the sole purpose of carrying out the transmission or strictly necessary in order to provide service explicitly requested by Mr Breyer. The CJEU has also ruled in the joined cases C-26/22 and C-64/22 that a wide range of interests is, in principle, capable of being regarded as legitimate, and the EDPB should thus enable the controllers to refer to the legitimate interests as a legal basis instead of a consent in various cases.

The consent requirement of cookie data and similar data does not mean that all processing of cookie-related data would be subject to the same consent requirement but the consent is only required for *accessing* and *storing* data on the terminal device.[2] No matter how strict the ePrivacy Directive Article 5(3) is interpreted, there will always be tracking which is designed not to access data on a terminal device. Tracking requires that somebody is able draw conclusions of a user such as that index *i* in the list of users is the same as the index *j* thus generating indirectly identifiable personal data. The GDPR could provide a whole set of measures to mitigate the adverse effects of tracking such as necessity requirement in legal bases, balance in legitimate interests, accountability, data minimisation, etc. which the ePrivacy Directive does not have.

Even though it is not explicitly stated, the EDPB seems to argue that 1) all tracking means accessing the data on a terminal device, and 2) all tracking is thus subject to the consent requirement of the ePrivacy Directive Article 5(3). However, the Guideline only establishes that *there are* tracking methods which access the data on the terminal device, and there is thus some tracking which is subject to the ePrivacy Directive Article 5(3). When someone tries to contest the Guideline at the courts of law, all they have to do is to provide a counterexample which debunks the idea of the Guideline. Instead, it seems a better court strategy for the EDPB and the supervisory authorities to argue that

1) there are tracking methods which access the data on the terminal device subject to the ePrivacy Directive Article 5(3),

2) tracking, even without accessing the data on the terminal device, means that an individual is singled out constituting indirectly identifiable personal data as per the GDPR,

3) the processing of indirectly identifiable personal data needs a valid legal basis such as consent, contract, or legitimate interests,

[2] For example, there can be other bases for processing when the end-user withdraws their consent but cookie data is used for the establishment of legal claims, when the conclusions based on cookie data form an indirectly identifiable browsing pattern which is retained after the consent is withdrawn and cookies deleted from the terminal device, or when the EDPB makes comments of public consultation available to the public even though it is not based on solely for carrying out the transmission of a PDF file from the computer nor explicitly requested by a commenter.

4) when the legal basis is not consent, the processing must be *necessary* for fulfilling the said legal basis as required in the GDPR Article 6(1)(b)-(f),
5) tracking as such is (presumably, perhaps the EDPB could adopt guidelines to assess its balance) not a legitimate interest but tracking might be necessary for some other legitimate interest, and
6) a user is able to object processing based on the legitimate interests.

The ePrivacy Directive Article 5(3) is technology neural

The EDPB has analysed the four criteria to applying the ePrivacy Directive Article 5(3) and applied it to use cases which typically relate to World Wide Web. A guideline on the applicability of the article should also consider other Internet-related protocols since applying the article to a specific header or data type requires similar applicability to the other protocols as well. For example, strict consent requirements for HTTP headers may cause unanticipated affects to processing email metadata unless the Guidelines explain the differences by applying the 4 criteria.

The applicability of the ePrivacy Directive Article 5(3) has four criteria, and as analysed by the EDPB, none of which is the purpose of accessing or storing the information on the terminal device. The purpose of accessing or storing information is only relevant for the technical storage or access when the transmission is impossible without it, also known as "Criterion A" in the WP29's opinion.[3] This means that *accessing* the IP address for security features must be treated equally to tracking, and *accessing* the URL and pixel-related data for providing user-specific content must be treated equally to URL and pixel tracking. This emphasises the EDPB's task to determine if applying the GDPR would be more suitable solution to mitigate the harm caused by Internet tracking than it is to base it on the confidentiality of communications.

The broad applicability of the ePrivacy Directive 5(3) has already lead to different interpretations of necessity between the GDPR and the ePrivacy Directive. On one hand, the EDPB seems to interpret the term *necessary* of the GDPR Article 6(1)(b)

[3] The WP29 Opinion 04/2012 on Cookie Consent Exemption / WP 194.

in a way which does not include targeted advertising set out in the terms and conditions of a service. On the other hand, the EDPB seems to interpret *strictly necessary* of the ePrivacy Directive Article 5(3) as "beneficial for a specific purpose but technically not essential".[4] The wording *strictly necessary* indicates a higher level of necessity than *necessary*, which means that some of the exemptions identified by WP29 should fall within the scope of consent if the Article 5(3) is interpreted broadly. The EDPB should aim to harmonise and clarify legal wordings in its guidelines and to avoid any confusion.

The EDPB's instructions of what "can be subject to applicability" are unclear

The EDPB has described in the section 3 of the Guidelines what *can* be subject to the applicability of the ePrivacy Directive Article 5(3). It is possible to store any kind of information on a terminal device to be accessed later so technically any sort of information can be subject to the cookie consent requirement.[5] Instead, it would be more informative to explain the use cases by applying all 4 criteria of the ePrivacy Directive Article 5(3) and describe how all of them are most likely fulfilled. If even one of the criteria is not applicable, consent is not needed as per article, and there are most likely a huge number of technical solutions to provide the listed use cases.

In the paragraph 1 of the Guideline, the EDPB intends to establish a comprehensive list of the technical operations covered by the article, which means that the EDPB has a burden of proof beyond the "there is a case". The EDPB has found that both pixel tracking and tracking based on the IP address only would fall within the applicability of the Article 5(3) but little evidence is provided. Such tracking process could be provided without, at least reportedly, triggering the wording,[6] meaning

[4] The WP29 Opinion 04/2012 on Cookie Consent Exemption section 3.3 counts the user centric security cookies such as detection of failed login attempts in the scope of Criterion B even though the service would work without them. The WP29 has also stated that the safeguard is weak in practice.

[5] Some cookies contain IP address and hashed values of unique identifiers. In those cases, cookie consent is applied because of the used cookies, not because of the "tracking based on IP only" or "unique identifier" sections of the Guideline.

[6] E.g., An email written in HTML format contains the element , where id=123 is a unique parameter determined by prior to sending the email. When the recipient opens the message, their device or their email server sends a GET request to acquire the named resource (a JPEG image). It is possible that ID is provided to acquire the timestamp of GET request to know when the message was read or otherwise "track" the request's

that the use cases provided by the EDPB are not sufficient to stop malicious tracking but will harm service providers who require certain data for beneficial purposes within their legitimate interests.

The EDPB seems to have taken a strong stance against processing anything terminal device-related data without consent when the EDPB has described device fingerprinting as "abuse" of the application protocol including mechanisms to provide context data.[7] Taking into account that device fingerprinting has beneficial purposes even in the EDPB's opinion,[8] referring to "abuse" is an uncalled-for remark. An accessing entity has any right (to the extent permitted by the GDPR) to process device-specific data without consent when all 4 criteria of the ePrivacy Directive Article 5(3) are not present but the EDPB's characterisation might a service provider an erroneous impression. This emphasises the EDPB's obligation to clarify the technical examples by explain how each of them fulfils all required 4 criteria.

Too broad interpretation of "gaining of access" should be avoided

The EDPB has used active wordings[9] in the section 2.5 when describing the criterion of gaining access meaning that the Article 5(3) is applicable when the accessing entity actively pursues access to the information.[10] This would mean that it is not accessing in the sense of the ePrivacy Directive Article 5(3) if an end-user provides a service provider some information which is not determined or enforced by

user agent or other similar details. It is equally possible that the sender only wants to make that particular image available only to the recipient in question, or both. Either way, the sender could argue that no consent is needed because the identifier is never stored on the device but an email server, the timestamp of opening is based solely on user activity, the IP address used for the request is provided by the Internet Service Provider and router requesting a DHCP lease thus never originating from the terminal device, and that the sender has no power to decide what kind of attributes are provided with GET request (if any).

[7] The paragraph 42 of the Guideline refers to "the abuse of those mechanism" after referring to the HTTP header, caching mechanism and other functionalities.

[8] See e.g., Chapters 7.5 User centric security and 7.6 Adapting the user interface to the device in the Opinion 9/2014 of the WP29 / WP 224. The WP29 found that the use cases of user centric security and adapting the user interface might fall under the exception from requiring consent.

[9] Such as "actively takes steps towards…" and "accessing entity instructs the terminal equipment to proactively send…" in paragraph 31, "explicitly instructs…" in paragraph 32.

[10] This is also true for cookies. Even though they are passively added to every subsequent request to a server just like other headers by a browser, cookies are actively added either by Set-Cookie header in the HTTP reply of the server or using document.cookie in JavaScript.

the service provider. Nevertheless, the EDPB seems to accept more passive wordings as access in the section 3 of the Guideline.

The EDPB's use case examples of URL and IP-based tracking indicate that passive access to headers provided by the end-user could be sufficient of triggering the article.[11] If simply gaining access to HTTP request header is sufficient to trigger the wording of the Article 5(3), the EDPB should also elaborate its guidance on:

- How gaining of access to the same information when using firewalls would not be subject to the consent requirement.[12]
- If the SMTP headers or headers of other protocols would also fall under the consent requirement since the Article 5(3) is technology neutral, and how does it affect for example replying to an email or spam filtering them.[13]
- How an accessing entity is able to fulfil its obligation to respect user preferences as required by the WP29[14] if the mere access to said data requires a consent.
- If hashing an email address for unique identifier is within the scope of the Article 5(3) because it is "temporarily stored on a terminal device before being collected", why *all* Internet traffic does not require consent when all processed information is temporarily processed by a terminal device.

[11] Source and destination IP addresses are provided in every Internet Protocol Package. A server is unable to provide a reply (e.g., an HTML source of a webpage) without the source IP address. Receiving an IP address is sufficient for "tracking based on IP only".

[12] The WP29 Opinion 4/2012 on Cookie Consent Exemption (WP 194) requires for Criterion A to apply that it is not sufficient just to "regulate the transmission" and that the "transmission of the communication must not be possible without the use of the cookie [or other technologies where applicable]". The entire purpose of a firewall is to be a safety barrier between trusted and untrusted network (i.e., to regulate communications), and a network functions perfectly without one. We may assume that a firewall is a measure against someone who is not giving the consent and who does not "explicitly request" the use of a firewall. An exemption from the consent thus would not be applicable.

[13] Taking into account that From: Sender <email@domain.tld> is passively collected value in the email header which has not been actively provided by the user sending an email. Additionally, spam filtering is typically based on various header values such as DKIM or DK signatures. Replying to an email or filtering spam email requires the processing of email header data which has not been explicitly requested by the sender nor are they strictly necessary for the sender to deliver their message to the recipient.

[14] WP29 Opinion 04/2012 on Cookie Consent Exemption section 4.2 claims, yet does not establish, that an accessing entity would have an obligation to respect user's request parameter DNT=1. If consent is required for passively received data as a header, an accessing entity never becomes aware of the request inside of it and cannot fulfil it.

If the EDPB is unable to describe why the Article 5(3) would require consent for certain metadata in some situations but not others, the only conclusion is that either the Article 5(3) permits all processing purposes of the same data without consent or requires the consent for all.

The ePrivacy Directive Article 5(3) is an exception from the Article 5(1)

The ePrivacy Directive Article 5(3) itself is an exception from the Article 5(1) which establishes *the confidentiality of communications* between the parties on the Internet similarly as already established for postal mail.[15] On one hand, the confidentiality prevents third parties – namely the postal office workers and the electronic counterpart, the Internet Service Provider – from accessing or processing the contents and the metadata of communications when it is not necessary for the conveyance of a communication. On the other hand, the confidentiality means that the parties are allowed to impose their electronic messages and related metadata any way they find suitable.[16] The recipient of a letter has lawful access to the contents of the letter but also all analogical metadata – the stamp, the info on the envelope, the style of the handwriting, etc. Such rights are also granted to the recipient of an electronic mail unless otherwise stipulated.

Exceptions to general rules are construed narrowly which means that unclear cases should be follow the main rule. The cookie consent exemptions are interpreted narrowly, as instructed by the WP29, and the unclear cases fall outside of the exceptions. This also means that if the applicability of the ePrivacy Directive Article 5(3) should be excluded for unclear cases when the case does not strictly fall within the wording of the article. The article also sets a new obligation to service providers,

[15] Taking into account that the Internet is based on transferring data using Internet Protocol packets, comparison to postal world is justifiable. Each IP packet should be considered as "electronic mail" as defined in the ePrivacy Directive Article 2 regardless of if it is Simple Mail Transfer Protocol (everyday language e-mail), Hypertext Transfer Protocol, or something else. The server's inability to recognise packets to the same end-user is a fundamental use case for cookies – a GET request of a front-page returns different source code to the browser if the GET request to the same resource contains cookies which prove that the user has logged in.

[16] See e.g., the Finnish Act on Electronic Communications Services (917/2014) § 136 which explicitly states that the parties are entitled to process their messages and related metadata unless otherwise provided by the law.

or “accessing entities”, to request consent in certain situations, and unclear obligations are interpreted narrowly. The legislator did not intend to prevent electronic recipients from processing anything they could not do in postal world without a consent but to enforce the confidentiality of communications in all cases – regardless of if the communication is between a controller and a data subject, two controllers, two data subjects, or something else as per the GDPR. The EDPB’s guideline on technical scope of confidentiality of communications should be comparable to the postal secrecy, and the EDPB should apply the GDPR to mitigate the privacy concerns it has identified.