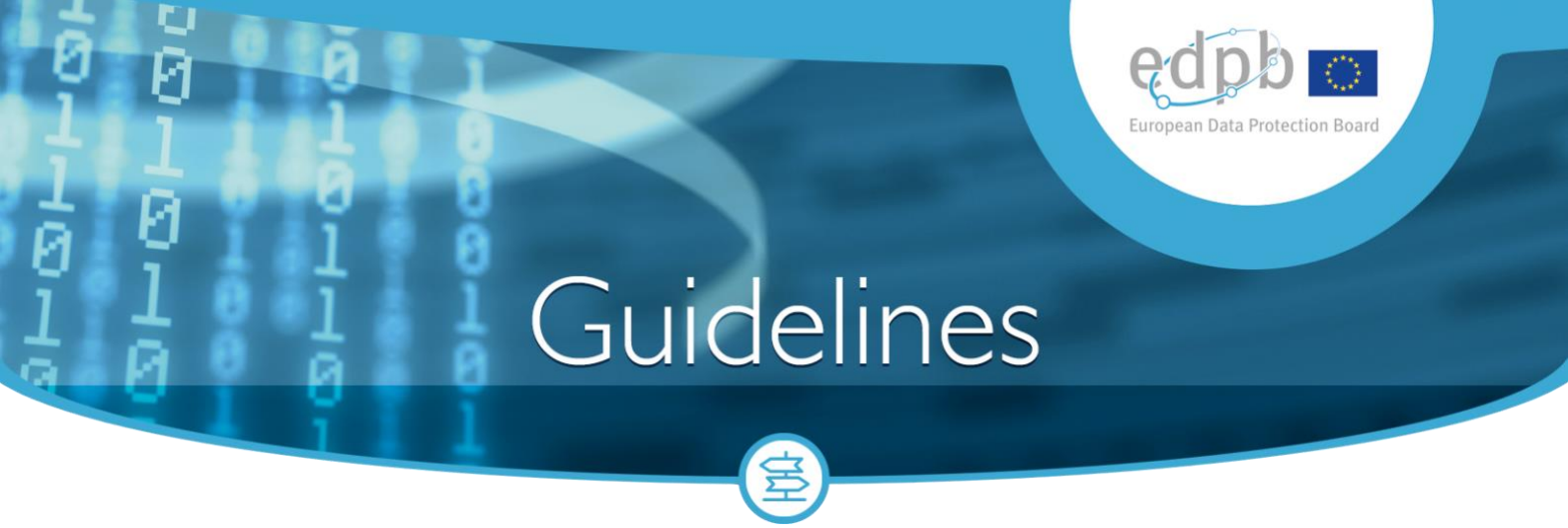

Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

Version 2.0

Adopted on 7 October 2024

[
Nicholas Vollmer: Hier geht es um das Schreiben von Cookies und den lesenden Zugriff auf Daten vom Endgerät.

Die deutsche Datenschutz-Konferenz bezieht sich einen Monat später (am 20.11.2024) darauf.

Siehe auch im Kapitel 9.6.4 im PrivazyPlan® zur Pflicht [TDDDG_025].
]

Version History

Version 1.0	14 November 2023	Adoption of the Guidelines for public consultation
Version 2.0	7 October 2024	Adoption of the Guidelines after public consultation

Executive summary

In these Guidelines, the EDPB addresses the applicability of Article 5(3) of the ePrivacy Directive to different technical solutions. These Guidelines expand upon the Opinion 9/2014 of the Article 29 Working Party on the application of ePrivacy Directive to device fingerprinting and aim to provide a clear understanding of the technical operations covered by Article 5(3) of the ePrivacy Directive.

The emergence of new tracking methods to both replace existing tracking tools (for example, cookies, due to discontinued support for third-party cookies by some browser vendors) and create new business models has become a critical data protection concern. While the applicability of Article 5(3) of the ePrivacy Directive is well established and implemented for some tracking technologies such as cookies, there is a need to address ambiguities related to the application of the said provision to emerging tracking tools.

The Guidelines identify three key elements for the applicability of Article 5(3) of the ePrivacy Directive (section 2.1), namely 'information', 'terminal equipment of a subscriber or user' and 'gaining access and 'storage of information and stored information'. The Guidelines further provide a detailed analysis of each element (section 2.2-2.6).

In section 3, that analysis is applied to a non-exhaustive list of use cases representing common techniques, namely:

- URL and pixel tracking
- Local processing
- Tracking based on IP only
- Intermittent and mediated Internet of Things (IoT) reporting
- Unique Identifier

Table of contents

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter, 'GDPR'),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 15(3) of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC (hereinafter, 'ePrivacy Directive' or 'ePD'),

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES:

1 INTRODUCTION

1. According to Article 5(3) ePD, *'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 consent or necessity for specific purposes set out in that Article. As reminded in Recital 24 of the ePD[2], the goal of that provision is to protect the users' terminal equipment, as they are part of the private sphere of the users. It results from the wording of the Article, that Article 5(3) ePD does not exclusively apply to cookies, but also to 'similar technologies'. However, there is currently no comprehensive list of the technical operations covered by Article 5(3) ePD.

2. Article 29 Working Party (hereinafter, 'WP29') Opinion 9/2014 on the application of ePrivacy Directive to device fingerprinting (hereinafter, 'WP29 Opinion 9/2014') has already clarified that fingerprinting falls within the technical scope of Article 5(3) ePD[3], but due to the new advances in technologies further guidance is needed with respect to the tracking techniques currently observed. The technical landscape has been evolving during the last decade, with the increasing use of identifiers embedded in operating systems, as well as the creation of new tools allowing the storage of information in terminal equipment.

[1] References to 'Member States' made throughout this document should be understood as references to 'EEA Member States'.

[2] 'Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.'

[3] WP29 Opinion 9/2014, p. 11.

3. The ambiguities regarding the scope of application of Article 5(3) ePD have created incentives to implement alternative solutions for tracking internet users and lead to a tendency to circumvent the legal obligations provided by Article 5(3) ePD. All such situations raise concerns and require a supplementary analysis in order to complement the previous guidance from the EDPB.

4. The aim of these Guidelines is to conduct a technical analysis on the scope of application of Article 5(3) ePD, namely to clarify what is technically covered by the phrase '*to store information or to gain access to information stored in the terminal equipment of a subscriber or user*'. These Guidelines do not address the circumstances under which a processing operation may fall within the exemptions from the consent requirement provided for by the ePD[4], as these circumstances should be analysed on a case-by-case basis accounting for the relevant member state transposition(s), and guidance issued by national Competent Authorities.

5. A non-exhaustive list of specific use-cases will be analysed in the final part of these Guidelines.

2 ANALYSIS

2.1 Key elements for the applicability of Article 5(3) ePD

6. Article 5(3) ePD applies if:

   a. **CRITERION A:** the operations carried out relate to '*information*'. It should be noted that the term used is not 'personal data', but 'information'.

   b. **CRITERION B:** the operations carried out involve a '*terminal equipment*' of a subscriber or user (B.1), which imply the need to assess the notion *of a 'public communications network*' (B.2).

   c. **CRITERION C** the operations carried out indeed constitute '*storage*' (C.1) or a '*gaining of access*' (C.2). Those two notions can be studied independently, as reminded in WP29 Opinion 9/2014: *'Use of the words "stored or accessed" indicates that the storage and access do not need to occur within the same communication and do not need to be performed by the same party'*[5].

   For the sake of readability, the entity gaining access to information stored in the user's terminal equipment will be hereafter referred to as an 'accessing entity'.

2.2 Notion of 'information' - Criterion A

7. As expressed in CRITERION A, this section details what is covered by the notion of 'information'. The choice of the term 'information', encompassing a broader category than the mere notion of personal data, is related to the scope of the ePrivacy Directive.

8. The goal of Article 5(3) ePD is to protect the private sphere of the users, as stated in its Recital 24: '*Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European*

[4] As stated in Article 5(3) ePD: '*This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'*

[5] WP29 Opinion 9/2014, p. 8.

Convention for the Protection of Human Rights and Fundamental Freedoms'. It is also protected by Article 7 of the EU Charter of Fundamental Rights.

9. In fact, scenarios that do intrude into this private sphere even without involving any personal data are explicitly covered by the wording of Article 5(3) and Recital 24 ePD, for example the storage of viruses on the user's terminal equipment. This shows that the definition of the term 'information' should not be limited to the property of being related to an identified or identifiable natural person.

10. This has been confirmed by the Court of Justice of the EU: '*That protection applies to any information stored in such terminal equipment, regardless of whether or not it is personal data, and is intended, in particular, as is clear from that recital, to protect users from the risk that hidden identifiers and other similar devices enter those users' terminal equipment without their knowledge*'[6].

11. The questions on whether the origin of this information and the reasons why it is stored in the terminal equipment should be considered when assessing the applicability of Article 5(3) ePD have been previously clarified. For example, in the WP29 Opinion 9/2014: '*It is not correct to interpret this as meaning that the third-party does not require consent to access this information simply because he did not store it. The consent requirement also applies when a read-only value is accessed (e.g. requesting the MAC address of a network interface via the OS API)*' [7].

12. In conclusion, the notion of information includes both non-personal data and personal data, regardless of how this data was stored and by whom, i.e. whether by an external entity (also including other entities than the one having access), by the user, by a manufacturer, or any other scenario.

2.3 Notion of 'terminal equipment of a subscriber or user' – Criterion B.1

13. This section builds on the definition used in Directive 2008/63/EC and as referenced in Article 2 Directive (EU) 2018/1972, where 'terminal equipment' is defined as: '*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal equipment and the interface of the network*'[8].

14. Recital 24 ePD provides a clear understanding of the role of the terminal equipment for the protection offered by Article 5(3) ePD. The ePD protects users' privacy not only in relation to the confidentiality of their information but also by safeguarding the integrity of the user's terminal equipment. This understanding will guide the interpretation of the notion of the terminal equipment throughout these Guidelines.

15. Article 3 ePD states that for the ePD to apply the processing of personal data has to be carried out in connection with the provision of publicly available electronic communications services in public communications networks. This entails that a device should be usable in connection with such service and that, in order to be qualified as a terminal equipment, it should be connected or connectable[9] to the interface of a public communications network. The EDPB notes that the amendments made

[6] Judgement of the Court of Justice of 1 October 2019, Planet 49, Case C-673/17, ECLI:EU:C:2019:801, paragraph 70.
[7] WP29 Opinion 9/2014, p. 8.
[8] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version), Article 1(1).
[9] That is, having the technical capabilities to be connected to the network even if that connection is not currently in place.

in 2009[10] in the text of Article 5(3) ePD extended the protection of terminal equipment by deleting the reference to the 'use of electronic communications network' as a means to store information or to gain access to information stored in the terminal equipment. Therefore, as long as a device has a network interface that makes it eligible for connection (even if such connection is not in place), Article 5(3) ePD applies to every entity that would store and gain access to information already stored in the terminal equipment whatever the means of access to the terminal equipment is, and whether connected or disconnected from a network

16. Equipment that are part of the public electronic communications network itself would not be considered terminal equipment under Article 5(3) ePD[11].

17. A terminal equipment may be comprised of any number of individual pieces of hardware, which together form the terminal equipment. This may or may not take the form of a physically enclosed device hosting all the display, processing, storage and peripheral hardware (for example, smartphones, laptops, network-attached storage device, connected cars or connected TVs, smart glasses).

18. The ePD acknowledges that the protection of the confidentiality of the information stored on a user's terminal equipment and integrity of the user's terminal equipment is not limited to the protection of the private sphere of natural persons but also concerns the right to respect for their correspondence or the legitimate interests of legal persons[12]. As such, a terminal equipment that allows for this correspondence and the legitimate interests of the legal persons to be carried out is protected under Article 5(3) ePD.

19. The user or subscriber may own or rent or otherwise be provided with the terminal equipment. Multiple users or subscribers may share the same terminal equipment.

20. This protection is guaranteed by the ePD to the terminal equipment associated to the user or subscriber, and it is not dependant on whether the user set up the means of access (for example if they initiated the electronic communication) or even on whether the user is aware of the said means of access).

2.4 Notion of 'public communications network' – Criterion B.2

21. As the situation regulated by the ePD is the one related to '*the provision of publicly available electronic communications services in public communications networks in the Community*'[13], and the definition of a terminal equipment specifically mentions the notion of a '*public communications network*', it is crucial to clarify this notion to identify the context in which Article 5(3) ePD applies.

[10] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), OJ L 337, 18.12.2009, Article 2(5) and Recital 65.

[11] To identify the limits of the network in different contexts, refer to the BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies (BoR (20) 46)

[12] Indeed, as reminded in Art. 2(13) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, the user can be a natural or a legal person.

[13] Article 3 ePD.

22. The notion of electronic communications network is not defined within the ePD itself. That concept was referred to originally in Directive 2002/21/EC (the Framework Directive) on a common regulatory framework for electronic communications networks and services[14], subsequently replaced by Article 2(1) of Directive 2018/1972 (the European Electronic Communications Code). It now reads:

> *"electronic communications network" means transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.*[15]

23. This definition is neutral with respect to the transmission technologies. An electronic communications network, according to this definition, is any network system that allows transmission of electronic signals between its nodes, regardless of the equipment and protocols used.

24. The notion of electronic communications network under Directive 2018/1972 does not depend on the public or private nature of the infrastructure, nor on the way the network is deployed or managed ('*whether or not based on a permanent infrastructure or centralised administration capacity*'[16].) As a result, the definition of electronic communications network, under Article 2 of Directive 2018/1972, is broad enough to cover any type of infrastructure. It includes networks managed or not by an operator, networks co-managed by a group of operators, or even ad-hoc networks in which a terminal equipment may dynamically join or leave a mesh of other terminal equipment using short range transmission protocols.

25. This definition of network does not give any limitation with regards to the number of terminal equipment present in the network at any time. Some networking schemes rely on nodes relaying information in an ad-hoc manner to nodes presently connected[17] and can at some point in time have as little as two peers communicating. Such cases would be within the general scope of the ePD directive, as long as the network protocol allows for further inclusion of peers.

26. The public availability of the communication network is necessary for the device to be considered a terminal equipment and in consequence for the applicability of Article 5(3) ePD. It should be noted that the fact that the network is made available to a limited subset of the public (for example, subscribers, whether paying or not, subject to eligibility conditions) does not make such a network private[18].

2.5 Notion of 'gaining access' – Criterion C.1

[14] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)
[15] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), Text with EEA relevance, Article 2(1).
[16] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), Text with EEA relevance, Article 2(1).
[17] For example, in the context of delay-tolerant networking scheme that implement 'store and forward techniques' such as the Briar open source project.
[18] For further analysis on the identification of public communication networks, refer to the BEREC Guidelines on the Implementation of the Open Internet Regulation (BoR (20) 112)

27. To correctly frame the notion of 'gaining access', it is important to consider the scope of the ePD, stated in its Article 1: '*to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community*'.

28. In a nutshell, the ePD is a privacy preserving legal instrument aiming to protect the confidentiality of communications and the integrity of devices. In Recital 24 ePD, it is clarified that, in the case of natural persons, the user's terminal equipment is part of their private sphere and that accessing information stored on it without their knowledge may seriously intrude upon their privacy.

29. Legal persons are also safeguarded by the ePD[19]. In consequence, the notion of 'gaining access' under Article 5(3) ePD, has to be interpreted in a way that safeguards those rights against violation by third parties.

30. Storing information or gaining access can be independent operations, and performed by independent entities. Storing of information and access to information already stored do not need to be both present for Article 5(3) ePD to apply.

31. As noted in the WP29 Opinion 9/2014: '*Use of the words "stored or accessed" indicates that the storage and access do not need to occur within the same communication and do not need to be performed by the same party. Information that is stored by one party (including information stored by the user or device manufacturer) which is later accessed by another party is therefore within the scope of Art. 5(3)*'[20]. Consequently, there are no restrictions placed on the origin of information on the terminal equipment for the notion of access to apply.

32. Whenever an entity takes steps towards gaining access to information stored in the terminal equipment, Article 5(3) ePD would apply. Usually this entails the accessing entity to proactively send specific instructions to the terminal equipment in order to receive back the targeted information. For example, this is the case for cookies, where the accessing entity instructs the terminal equipment to proactively send information on each subsequent Hypertext Transfer Protocol ('HTTP') call.

33. That is equally the case when the accessing entity distributes software on the terminal equipment of the user that is stored and will then proactively call an Application Programming Interface ('API') endpoint over the network. Additional examples would include JavaScript code, where the accessing entity instructs the browser of the user to send asynchronous requests with the targeted information. Such access clearly falls within the scope of Article 5(3) ePD, as the accessing entity explicitly instructs the terminal equipment to send the information.

34. In some cases, the entity instructing the terminal equipment to send back the targeted data and the entity receiving information might not be the same. This may result from the provision and/or use of a common mechanism between the two entities. Instructing the device to send already stored information (for example, through the use of a protocol, or an SDK[21] that imply the proactive sending of information by the terminal equipment) makes an intrusion into the terminal equipment possible, therefore such an access triggers the applicability of Article 5(3).) ePD. As noted in WP29 Opinion 09/2014, this can be the case when a website instructs the terminal equipment to send information

[19] Recital 26 ePD, see paragraph 17 above.
[20] WP29 Opinion 9/2014, p. 8.
[21] An SDK ("software development kit") is a bundle of software development tools made available to facilitate the creation of application software.

to third-party advertising services through the inclusion of a tracking pixel[22]. This use-case is further developed in section 3.1.

2.6 Notions of storage of information' and 'stored information' – Criterion C.2

35. Storage of information in the sense of Article 5(3) ePD refers to placing information on a physical electronic storage medium that is part of a user or subscriber's terminal equipment[23].

36. Typically, information is not stored in the terminal equipment of a user or subscriber through direct access to the memory of the device by another party, but rather by instructing software on the terminal equipment to generate specific information. Storage taking place through such instructions is considered to be initiated directly by the other party. This includes making use of established protocols such as browser cookie storage as well as customized software, regardless of who created or installed the protocols or software on the terminal equipment.

37. The ePD does not place any upper or lower limit on the length of time that information must persist on a storage medium to be counted as stored, nor is there an upper or lower limit on the amount of information to be stored.

38. Similarly, the notion of storage does not depend on the type of medium on which the information is stored. Typical examples would include hard disc drives ('HDD'), solid state drives ('SSD'), electrically-erasable programmable read-only memory ('EEPROM') and random-access memory ('RAM'), but less typical scenarios involving a medium such as magnetic tape or central processing unit ('CPU') cache are not excluded from the scope of application. The storage medium may be connected internally (e.g. through a SATA connection), externally (e.g. through a USB connection)

39. 'Stored information' refers to information already existing on the terminal equipment, regardless of the source or nature of this information. This includes any result from information storage in the sense of Article 5(3) ePD as described above (either by the same party that would later gain access or by another third party). It furthermore includes results of information storage processes beyond the scope of Article 5(3),) ePD, such as: storage on the terminal equipment by the user or subscriber themselves, or by a hardware manufacturer (such as the MAC addresses of network interface controllers), sensors integrated into the terminal equipment or processes and programs executed on the terminal equipment, which may or may not produce information that is dependent on or derived from stored information.

3 USE CASES

40. As pointed out in the introduction of these guidelines[24], they do not analyse the application of the exemptions to the obligation to collect consent provided by Article 5(3) ePD. The EDPB reminds that for all of the cases where there is a storage of information or a gaining of access to information already stored, it would have to be assessed if a consent is needed or whether an exemption under Article 5(3) ePD could apply. The reader should therefore consider the exemptions in their use case, in conjunction with this technical analysis.

41. Without prejudice of the specific context in which those technical categories can be used which are necessary to qualify whether Article 5(3) ePD is applicable, it is possible to identify, in a non-exhaustive

[22] WP29 Opinion 9/2014, p. 9.
[23] As defined in section 2.3 of these Guidelines.
[24] See paragraph 4 above.

manner, broad categories of identifiers and information that are widely used and can be subject to the applicability of Article 5(3) ePD.

42. Network communication usually relies on a layered model that necessitates the use of identifiers to allow for a proper establishment and carrying out of the communication. The communication of those identifiers to remote actors is instructed through software following agreed upon communication protocols. As outlined above, the fact that the receiving entity might not be the entity instructing the sending of information does not preclude the application of Article 5(3) ePD. This might concern routing identifiers such as the MAC or IP address of the terminal equipment, but also session identifiers (SSRC, Websocket identifier), or authentication tokens.

43. In the same manner, the application protocol can include several mechanisms to provide context data (such as HTTP header including 'accept' field or user agent), caching mechanism (such as ETag[25]) or other functionalities (cookies being one of them, or HSTS[26]). Once again, relying on those mechanisms to collect information (for example in the context of fingerprinting[27] or the tracking of resource identifiers) can lead to the application of Article 5(3) ePD.

44. On the other hand, there are some contexts in which local applications installed in the terminal equipment uses some information strictly inside the terminal, as it might be the case for smartphone system APIs (access to camera, microphone, GPS sensor, accelerator chip, radio chip, local file access, contact list, identifiers access, etc.). This might also be the case for web browsers that process information stored or generated information inside the device (such as cookies, local storage, WebSQL, or even information provided by the users themselves). The use of such information by an application would not constitute a 'gaining of access to information already stored' in the meaning of Article 5(3) ePD as long as the information does not leave the device, but when this information or any derivation of this information is accessed, Article 5(3) ePD would apply.

45. Finally, in some cases malicious software elements are distributed by actors, for example crypto mining software or more generally malware, exploiting the processing abilities of the terminal equipment for the benefit of the distributing actor. The distribution of said malicious software in user's terminal equipment would constitute a 'storage' in the meaning of Article 5(3) ePD. In addition, should the software establish a network connection to send information at a later stage, it would constitute a 'gaining of access' in the meaning of Article 5(3) ePD

46. For a subset of these categories that present a specific interest, either because of their widespread usage or because a specific study is warranted with regards to the circumstances of their use, a specific analysis is provided below.

3.1 URL and pixel tracking

47. A tracking pixel is a hyperlink to a resource, usually an image file, embedded into a piece of content like a website or an email. This pixel usually fulfils no purpose related to the requested content itself; its sole purpose is to automatically establish a communication by the client to the host of the pixel, which would otherwise not have occurred. This is however not systematic and tracking pixels can also be created by adding additional information to hyperlink loading images that are relevant

[25] The HTTP ETag is an identifier that allows to do conditional request based on the validity of the cached client data.

[26] HTTP Strict Transport Security (HSTS) allow servers to specify which resources should always be requested using HTTPS connections.

[27] As noted in the introduction, please see Opinion 9/2014 of the Article 29 Working Party on the application of ePrivacy Directive to device fingerprinting

to the content displayed to the user. Establishment of the communication transmits various information to the host of the pixel, depending on the specific use case.

48. In the case of an email, the sender may include a tracking pixel to detect when the receiver reads the email. Tracking pixels on websites may link to an entity collecting many such requests and thus being able to track users' behaviour. Such tracking pixels may also contain additional identifiers, metadata or content as part of the link. These data points may be added by the owner of the website, possibly related to the user's activity on that website so that analytical usage reports can be generated. They may also be dynamically generated through client-side applicative logic supplied by the entity.

49. Tracking links can function in the same way, but the identifier is appended to the website address. When the Uniform Resource Locator ('URL') is visited by the user, the targeted website loads the requested resource but also collects an identifier which is not relevant in terms of resource identification. They are very commonly used by eCommerce websites to identify the origin of their inbound source of traffic. For example, such websites can provide tracked links to partners to use on their domain so that the e-commerce website knows which of their partners is responsible for a sale and pay a commission, a practice known as affiliate marketing.

50. Both tracking links and tracking pixels can be distributed through a wide variety of channels, for example through emails, websites, or even, in the case of tracking links, through any kind of text messaging systems. That distribution to the user's terminal equipment does constitute storage, at the very least through the caching mechanism of the client-side software. As such, Article 5(3) ePD is applicable, even if this storage is not permanent.

51. The addition of tracking information to URLs or images (pixels) sent to the user constitutes an instruction to the terminal equipment to send back the targeted information (the specified identifier). In the case of dynamically constructed tracking pixels, it is the distribution of the applicative logic (usually a JavaScript code) that constitutes the instruction. As a consequence, it can be considered that the collection of identifiers provided through such tracking mechanisms constitutes a 'gaining of access' in the meaning of Article 5(3) ePD, thus it applies to that step as well.

3.2 Local processing

52. Some technologies rely on local processing instructed by software distributed on users' terminal equipment, where the information produced by the local processing is then made available to selected actors through client-side API. This may for example be the case for an API provided by the web browser, where locally generated results may be accessed remotely.

53. If at any point and for example in the client-side code, the processed information is made available to a third-party, for example sent back over the network to a server, such an operation (instructed by the entity producing the client-side code distributed on the user terminal equipment) would constitute a 'gaining of access to information already stored'. The fact that this information is being produced locally does not preclude the application of Article 5(3) ePD.

3.3 Tracking based on IP only

54. Some providers are developing solutions that only rely on the collection of one component, namely the IP address, in order to track the navigation[28] of the user, in some case across multiple domains. In that context Article 5(3) ePD could apply even though the instruction to make the IP available has been made by a different entity than the receiving one.

55. However, gaining access to IP addresses would only trigger the application of Article 5(3) ePD in cases where this information originates from the terminal equipment of a subscriber or user. While it is not systematically the case (for example when CGNAT[29] is activated), the static outbound IPv4 originating from a user's router would fall within that case, as well as IPV6 addresses since they are partly defined by the host. Unless the entity can ensure that the IP address does not originate from the terminal equipment of a user or subscriber, it has to take all the steps pursuant to the Article 5(3) ePD.

56. While the present guidelines do not analyse the application of the exemptions to the obligation to collect consent provided by Article 5(3) ePD, it is important to once again recall that the applicability of this article does not systematically mean that consent needs to be collected. The EDPB thus reminds that in each case it would have to be assessed if a consent is needed or whether an exemption under Article 5(3) ePD could apply[30].

3.4 Intermittent and mediated IoT reporting

57. IoT (Internet of Things) devices produce information continuously over time, for example through sensors embedded in the device, which may or may not be locally pre-processed. In many cases, information is made available to a remote server, but the modalities of that collection can vary.

58. Some IoT devices have a direct connection to a public communication network with a cellular SIM card. Other may have an indirect connection to a public communication network, for example through the use of WIFI or the relay of information to another device through a point-to-point connection (for example, through Bluetooth). The other device can for example be a smartphone or a dedicated gateway which may or may not pre-process the information before sending it to the server.

59. IoT devices might be instructed by the manufacturer to always stream the collected information, yet still locally cache the information first, for example until a connection is available.

60. In any case the IoT device, where it is connected (directly or indirectly) to a public communications network, would itself be considered a terminal equipment. The fact that the information is streamed or cached for intermittent reporting does not change the nature of that information. In both situations Article 5(3) ePD would apply as there is, through the instruction of code on the IoT device to send the dynamically stored data to the remote server, a 'gaining of access'.

3.5 Unique Identifier

61. A common tool used by companies is the notion of 'unique identifiers' or 'persistent identifiers'. Such identifiers can be derived from persistent personal data (name and surname, email, phone number, etc.), that is hashed on the user's device, collected and shared amongst several controllers to uniquely identify a person over different datasets (usage data collected through the use of website

[28] This is additional to and independent of the use and function of an IP address for the establishment and conveyance or transmission of underlying technical communications, or the fact that it may or may not be personal data (in respect of ePrivacy analysis, it is "information")

[29] Carrier-grade NAT or CGNAT is used by Internet service providers to maximise the use of limited IP address space. It groups a number of subscribers under the same public IP address.

[30] WP29 Opinion 9/2014 provides for some example when consent might not be needed.

or application, customer relation management (CRM) data related to online or offline purchase or subscription, etc.). On websites, the persistent personal data is generally obtained in the context of authentication or the subscription to newsletters.

62. As outlined before, the fact that information is being entered by the user would not preclude the application of Article 5(3) ePD with regards to storage, as this information is stored temporarily on the terminal equipment before being collected.

63. In the context of 'unique identifier' collection on websites or mobile applications, the entity collecting is instructing the browser (through the distribution of client-side code) to send that information. As such a 'gaining of access' is taking place and Article 5(3) ePD applies.