European Data Protection Board

Ref.
Public consultation 2/2023

Comments of the Finnish Transport and Communications Agency on Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

The Finnish Transport and Communications Agency Traficom is responsible for monitoring compliance with Article 5(3) of the ePrivacy Directive ("ePD") in Finland. Traficom is also the national regulatory authority (NRA) for the supervision of the EU telecommunications regulatory framework in Finland.

Traficom welcomes the EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive ("Guidelines") and notes that they largely correspond with Traficom's earlier praxis. While Traficom supports the Guidelines on the whole, as an NRA we have some reservations as to the application of certain concepts of the EU telecommunications framework as well as on some aspects of the opinion that may lead to an overly broad scope of application of Art. 5(3) ePD. Below, we offer our comments paragraph by paragraph.

Paragraph 3 (ambiguities of Art. 5(3) ePD)

Paragraph mentions circumvention of legislation. If that were actually at issue, dealing with the problem would only be possible through the ordinary legislative procedure. Therefore, EDPB might consider replacing the word "circumvent" with "exploit ambiguity of" or similar in the first sentence of paragraph 3.

Paragraph 6 (criteria of applicability)

Paragraph 6 presents four criteria that are proposed as the key elements of the applicability of Article 5(3). In order to clarify the proposed guidelines, Traficom suggest that the guidelines state that the criteria are cumulative. However, see comment to paragraph 44, which may imply that criterion C is not actually a prerequisite in the present situation.

Paragraph 15 (devices acting as relays)

Paragraph 15 considers devices acting as relays. It would appear that the purpose of the paragraph is to discuss equipment that is part of the public ECN rather than terminal equipment of a user or subscriber. However, the text appears misleading and is too broadly formulated. In effect, it could be interpreted as saying that gaining access to information processed by a device acting as such a relay would not be subject to Art. 5(3) ePD. That is, the manufacturer of a switch or a router in switching mode (if routing would count as "performing [a] modification") or a third party would be allowed to process the relayed information (that is, information that is stored temporarily) by that device without the Art. 5(3) ePD limiting it. This would be untrue, because such a device is indeed terminal equipment, because it is connected to the interface of an ECN. It appears that this is unintentional, as paragraph 55 confirms that routers are within scope.

As quoted in paragraph 13, terminal equipment is defined in the telecommunications framework 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." This definition includes devices such as modems, routers, and switches. It is unclear what is meant in paragraph 15 by "performing … modifications to … information", but the presence or absence of such modification is irrelevant to the concept of terminal equipment. Consider, for instance, an xDSL modem or WiFi router. Regardless of whether they are operating in routing or switching mode, they may be terminal equipment in the sense of the ePD Article 5(3), and the information stored on the device may only be accessed on the conditions provided for in that Article.

Traficom advises the EDPB to take into account guidelines issued by BEREC on identification of the network termination point in different network topologies.[1] The network termination point (NTP), according to EECC Art. 2(9) is "the physical point at which an end-user is provided with access to a public communications network; in the case of networks involving switching or routing, the NTP is identified by means of a specific network address, which may be linked to an end-user's number or name." The NTP is crucial to the discussion in paragraph 15, as it determines whether a piece of equipment is terminal equipment or part of the public ECN. The EPDB should refer to this document in the determination of terminal equipment.

While the determination of the NTP may not always be simple, the BEREC guidelines provide guidance on this matter. According to BEREC, this determination by the NRA is based on whether there is an objective technological necessity for the equipment to be considered as part of the public network. If not, that equipment is considered terminal equipment; this applies, for instance, to all equipment not provided by the service provider or that the end-users are allowed to replace (BEREC guidelines, fn. 16).

In order to clarify the proposed guidelines, Traficom suggests that paragraph 15 instead state that equipment that are part of the public electronic communications network or used in the provision of an electronic communications service would not be considered terminal equipment within the meaning of Article 5(3) ePD.

Chapter 2.4 (Notion of 'electronic communications network', paragraphs 20-25)

Chapter 2.4 is problematic inasmuch it conflates the issues of whether there is an electronic communications network, whether that network is public, and whether there is a publicly available electronic communications service involved.

- *Paragraph 24*

Paragraph 24 states that Art. 5(3) would also apply in cases where there were only two peers communicating. While this could be true on a case-by-case basis, the statement fails to consider whether this network is *public* or whether that is a condition for the application of Art. 5(3). For instance, it may be possible to argue that Art. 5(3) might not apply to situations in which gaining of access or storage are limited to closed user groups such as in corporate networks (see Recital 55 to Directive 2009/136/EC) or in home networks. The paragraph is also at odds with paragraph 25, which states that the electronic communications service in question must be publicly available in order for Art. 5(3) to apply.

[1] BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies, BoR (20) 46, available at https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-common-approaches-to-the-identification-of-the-network-termination-point-in-different-network-topologies.

In the opinion of Traficom, the largest shortcoming of Chapter 2.4 is that it does not elaborate on whether Art. 5(3) is applicable to employer-issued devices vis-à-vis the employer or to BYOD scenarios (bring your own device). While devices such as laptops are often used in corporate networks, in distance working these devices communicate over publicly available electronic communications services (that is, the internet), with or without the use of technologies such as VPNs. Does this mean that the employer may only gain access to information stored on the device on the conditions provided for in Article 5(3), or should this situation be approached as one dealing with a closed user group? Traficom urges the EDPB to provide an opinion on this matter.

- *Paragraph 25*

Further, the final sentence of paragraph 25 is imprecise in its formulation of on what basis an ECN is considered *public*. Instead, the EDPB should refer to the formulation in the BEREC Guidelines on the Implementation of the Open Internet Regulation. According to paragraph 10 of the guidelines "[e]lectronic communication services or networks that are offered not only to a predetermined group of end-users but in principle to any customer who wants to subscribe to the service or network should be considered to be publicly available. Electronic communication services or networks that are offered only to a predetermined group of end-users could be considered to be not publicly available".[2]

Paragraph 31 (scope of application)

This is an important paragraph, as it states a fundamental concept behind the application of Art. 5(3), that is, where the accessing entity actively takes steps towards gaining accessing, such as sending instruction to the terminal equipment. While not mentioned in the present guidelines, Traficom notes that the same principle has previously been stated in different terms in WP29 Opinion 9/2014, p. 8: "any processing which the third-party undertakes which influences the behaviour of that device or otherwise cause it to store or give access to information on that device, or exposed by that device is within the scope of Article 5(3)." However, see below our comments to section 3.1.

Paragraphs 37-38 (terminal devices)

Paragraph 37 and 38 discuss network-attached storage devices. It should be clarified that they are undoubtedly within the scope of ePD Art. 5(3), because such a device constitutes terminal equipment in its own right. This is because they are either directly or indirectly, as the case may be, connected to the interface of a public telecommunications network. This means that paragraph 38 is unnecessary, and there is no need to consider these types of devices as part of other terminal equipment.[3]

Traficom proposes that the EDPB clarify that cloud-based virtual storage space that is accessible to the file system of the terminal device is also within scope. This is

[2] BEREC Guidelines on the Implementation of the Open Internet Regulation, BoR (22) 81, paragraph 10, available at https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-the-implementation-of-the-open-internet-regulation-0.

[3] The broad application of the concept of terminal equipment has also been mentioned in literature. For instance, it has been pointed out that the concept of terminal equipment includes "e.g. desk computers, laptop, pads, smartphones, but also other equipment such as wearable technologies, smart TVs, game consoles, connected vehicles, voice assistants, as well as any other object that is connected to an electronic communication network open to the public" (Cristiana Santos, Nataliia Bielova and Célestin Matte, "Are cookie banners indeed compliant with the law?" *Technology and Regulation*, 2020, pp. 91-135, 97).

because such information is at least intermittently stored on the device if such information is accessed through the device by a third party. However, that cloud-based service as such is not within scope.

Paragraph 42 ("abuse" of technologies)

Paragraph 42 is problematic inasmuch it states that "abuse" of certain techniques can trigger the application of Art. 5(3), as any kind of use of such technologies is enough to trigger the application of Art. 5(3) if Criterion D is fulfilled. The reference to abuse of certain techniques as a prerequisite of application of Art 5(3) can therefore be considered misleading.

Paragraph 44 (distribution of malicious software)

Paragraph 44 focuses solely on distribution over a network whereas recital 65 of directive 2009/136/EC does not make a distinction based on the method used to distribute malware. Moreover, it goes even further by specifying that "A high and equal level of protection of the private sphere of users needs to be ensured, regardless of whether un-wanted spying programmes or viruses are inadvertently downloaded via electronic communications networks or are delivered and installed in software distributed on other external data storage media, such as CDs, CD-ROMs or USB keys." In fact, as pointed out in relevant literature, directive 2009/136/EC specifically amended Art. 5(3) so that the text of the article no longer requires "the use of electronic communications networks" in order for the article to apply. This was intended to cover automatic and surreptitious installation of software (so called rootkits) by use of CDs.[4]

While the equipment needs to be connected to an interface of a telecommunications network in order to be considered terminal equipment, the application of Art. 5(3) might not require that the instructions accessing the information are delivered over a network, provided that Criterion D is fulfilled at some point.

Section 3.1 (URL and pixel tracking, paragraphs 49-51)

While Traficom agrees that pixel tracking is within scope, the believe that the Opinion does not currently consider all relevant arguments that might be made against including tracking links (URLs) in the scope of Art. 5(3) ePD. In principle, such URLs may be distributed through any kind of channel, as also noted in paragraph 49, also by non-electronic means (and typed by the user). While Traficom has not adopted decisions on the matter of tracking links and this opinion should not be considered as such, we believe that adopting an opinion on the matter would require considering the following arguments.

To our knowledge, the relevant recitals and preparatory works do not discuss application of the rules to situations such as tracking links, where any influence the putative accessing entity exerts as regards the functioning of a terminal equipment is more tenuous and indirect, requiring user interaction, compared to pixel tracking, for instance.

According to paragraph 50, distribution of tracking URLs would be deemed storage under certain conditions, apparently whether they are followed through or not. However, such a broad scope of application would seem to cover, beyond tracking links, also any other information that is sent to a terminal, such as emails, SMSs,

[4] Eleni Kosta, "Peeking into the cookie jar: the European approach towards the regulation of cookies." *International Journal of Law and Information Technology,* 21(4) 2013, pp. 380-406, 384-5 and Jan Tomíšek, "Cookies and EU Law: History, Future Regulation and Critique." *Technology and Regulation*, 2023, pp. 35-44, 38.

and HTTP responses. If this were found to be a result of this logic, this would seem to be an absurd outcome.

Further, paragraph 51 argues that tracking links should be considered as access to information already stored, as they constitute instruction in code to send back the identifier. However, it is debatable whether an URL qualifies as such an instruction (for instance, if the URL is distributed in plain text, it does not directly instruct the terminal equipment in any way). In order for there to be an action qualifying as an "access" as in an intrusion into the private sphere, it should normally be required that the transmission of such information is not initiated by the user. Instead, as also recognised in paragraph 31 of the Opinion, the accessing entity must take active steps toward gaining access to that information. While the creation and distribution of tracked URLs is indeed a processing operation, it seems not firmly established that this falls within the scope of Art. 5(1) ePD rather than (only) the GDPR, because the connection of that action with the functioning of a terminal equipment is so indirect and conditional as perhaps not qualifying as an instruction that influences the terminal's functioning.

While in the case of tracking pixels the web server directly instructs the terminal equipment to give access to certain information by requesting a web resource, this is not the case with tracking links. In the case of tracking links, the transmission of information does not take place until initiated by the user. It may not be possible to consider the distribution of an URL as an activity directly influencing the behaviour of that device in order to gain access to information stored on it.

It may be helpful to compare tracking links with situations where information pertaining to the terminal equipment is received passively, in order to ensure that the argumentative logic is able to appropriately deal with all relevant situations. For instance, an argument might be made that Art. 5(3) ePD would not apply to situations where an entity merely receives information without specifically instructing the terminal equipment to that effect, which might be the case in e.g., collecting automatically sent WiFi or Bluetooth radio signals[5] or in the case of simply receiving an email, or, indeed, a HTTP header of an original request for a web page. In fact, it has been argued in literature that data actively transmitted by a device about itself in the HTTP header would not be part of the private sphere that is protected by Art. 5(3) ePD; in contrast, when a script is run in that device to gain access to information, that process would be within the scope of the article. According to this line of argumentation, an active step towards access would exist, for instance, when the accessing entity instructs, by running a script on the terminal, for the terminal to transmit certain information about it to that entity. However, when and to the extent such information were transmitted at the initiative of the user and automatically by the terminal equipment (without the putative accessing entity instructing it), this line of argumentation would claim that situation to fall outside the scope of Art. 5(3) ePD; examples could be the receipt of IP address or HTTP headers in connection with a request for a URL or other connection initiated by the user.[6]

[5] The ambiguity of application of the article to passive tracking is recognised in WP29 Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), p. 11.
[6] See Jan Tomíšek, "Cookies and EU Law: History, Future Regulation and Critique." *Technology and Regulation*, 2023, pp. 35-44, 39. As also discussed in literature, it is to some extent unclear whether Art. 5(3) Art. 5(3) ePD applies to both active and passive fingerprinting, because if information is shared automatically, it might not be possible to deem this information "accessed" rather than simply collected (Paarth Naithani, "Regulating the 'Fingerprinting Monster' through EU Data Protection Law." *European Data Protection Law Review (EDPL)*, 7(4) 2021, pp. 597-608, 601-2; see also Tomíšek 39).

Section 3.3 (Tracking based on IP only, paragraphs 54-55)

Referring to the discussion above, it might be argued that the scope of Art. 5(3) ePD does not cover the collection of IP addresses when they are data that a device actively transmits about itself as part of the normal functioning of the internet, such as in connection with requests for web content. If the information is shared in the usual interaction of client and server without specific instruction, it might not normally be considered as "access".

This is supported by the fact that in case C-582/14 (Breyer), which dealt with the collection of IP addresses of visitors of websites, the Court makes no reference to the ePD. Instead, the Court analysed the situation based on Article 7(f) of Directive 95/46 and whether it precluded national legislation on the matter. This seems to imply that the issue at hand did not fall within the scope of Art. 5(3) ePD.

Paragraphs 57-60 (IoT devices as terminal equipment)

Traficom proposes that the EDPB clarify the text. If an IoT device is connected to a public ECN through WiFi or other home networking protocols, this is typically an example of an indirect (rather than direct as stated in the Opinion) connection to the interface of a public ECN, because it is often that WiFi router that has the direct connection. It is only where that WiFi base station were exceptionally part of the public ECN and operated by the provider of the public ECN that this would be a case of direct connection. However, in either case it is clear that the IoT device is within scope.

Paragraph 60 should be reformulated. If a networked device is connected to the interface of a public ECN through another device, it may be possible to consider this as an indirect connection to the interface of the public ECN. In that case, that IoT device should be deemed terminal equipment in its own right. It is not a condition that all communication happens over a public ECN, as it is undisputed that personal computers are within scope regardless of whether some of the communication happens over private networks such as home WiFi networks.

However, it is true that some devices that are connected to terminal equipment and whose data is eventually transmitted over a network are not necessarily terminal equipment in their own right. An example of such a situation would be printers without networking capabilities that are accessed over network using a discrete print server. In such a scenario the printer itself might not be commonly considered as terminal equipment. In contrast, it seems that in general any IoT device that is accessible from or has access to a public ECN (even if the information is relayed by another device) should meet the definition of terminal equipment under article 1(1)(a) of Directive 2008/63/EC.

Heidi Kivekäs
Head of Security Supervision

Marko Priiki
Chief Specialist

Yksikönpäällikkö Heidi Kivekäs
Hyväksytty 18.1.2024

Johtava asiantuntija Marko Priiki
Esitelty 18.1.2024