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

Submitted on 3 January 2024 by Robert Baugh, London, UK, linkedin.com/in/robertbaugh/

This document contains my feedback on Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive adopted 14 November 2023 ('**Guidelines**' and '**ePD**'). This feedback is my personal view only and not the view of any other person.

1. Summary

I do not believe the Guidelines are helpful as I believe they do not start from the correct point, which must be to embed an analysis of Art 5(3) in the accepted method and principles of interpreting EU law. The Guidelines' structure gives ammunition to well-discussed criticism of the Guidelines by allowing the envelope of discussion to be drawn in all sorts of directions, introducing uncertainties.

Much criticism on the Guidelines has been focussed on the broad applicability of the Guidelines' wording to apply, for example, to:

- all instances of any information leaving a device even when a website publisher unavoidably receives a person's IP address when that person visits their website using a browser,
- all instances of advertising including non-targeted adverts placed into a browser window, and even
- any deployment of text or an image to a user's device.

Further criticism has focussed on the EDPB trying to force its own, broad, reading of a 20-year-old law to modern technologies. The Guidelines open themselves up to the criticism of having an undefined and impossibly broad applicability, indeed arguably outlawing technologies from 2002 which most commentators do not believe the ePD was targeting, such as non-targeted and non-profiling banner ads.

I believe that the criticism can be negated by redrafting the Guidelines to base it within a clear analysis on the purpose and scope of Art 5(3), and relying on established mechanisms for interpreting EU law as described and applied, for example, in the recent CJEU decision of *Schufa*[1].

2. Interpretation of Art 5(3) in 2024

The CJEU recently dealt with a similar situation in *Schufa*, in paragraphs 40 to 73, namely the interpretation and application of Art 22 of the GDPR focussing on which party in a supply chain fell within that provision. One interpretation would arguably lead to Art 22 failing in its purpose to protect individuals' rights and freedoms. Another interpretation, favoured by the referring court and the CJEU, would mean Art 22 would achieve its purpose in that case.

In paragraph 41, the CJEU noted: '*In order to answer that [first] question, it should be borne in mind, as a preliminary point, that the interpretation of a provision of EU law requires that account be taken not only of its wording, but also of its context and the objectives and purpose pursued by the act of which it forms part (judgment of 22 June 2023, Pankki S, C-579/21, EU:C:2023:501, paragraph 38 and the case-law cited).*'

So, in redrafting the Guidelines, I strongly recommend that the EDPB first considers clearly:

1. the wording of the ePD, not just Art 5(3) but also the directly relevant Recitals and other wording,
2. the context of the ePD's relevant wording, which may include other Articles and Recitals, and
3. the objectives and purpose pursued by the ePD itself.

By doing so, I believe the EDPB can create Guidelines that are clear, that are relevant to today's technology, that do not overreach, and that do not impact activities that the ePD was not enacted to address.

3. Status of Recitals

[1] Case C-634/21, decision dated 7 December 2023

As the Joint Practical Guide on drafting EU law[2] notes:

'10. The purpose of the recitals is to set out concise reasons for the chief provisions of the enacting terms, without reproducing or paraphrasing them. They shall not contain normative provisions or political exhortations.'

'10.1 The 'recitals' are the part of the act which contains the statement of reasons for its adoption; they are placed between the citations and the enacting terms. The statement of reasons begins with the word 'whereas:' and continues with numbered points (see Guideline 11) comprising one or more complete sentences. It uses non-mandatory language and must not be capable of being confused with the enacting terms.'

'18.11. The recitals to an amending act have to fulfil the same requirements as the recitals to an autonomous act (see Guidelines 10 and 11). However, they have a special purpose in that they are intended only to explain the reasons for the changes made by the amending act: they therefore do not need to repeat the reasons for the act to be amended.'

'18.12. It is not good legislative practice to amend the recitals of the act to be amended. Those recitals set out, in a coherent manner, the reasons for the act at the time it was adopted in its original form. Only by means of codification or recast can the initial reasoning and the reasons for the successive amendments be consolidated coherently, with the necessary adaptations.'

It is established EU law that Recitals are not operative law and cannot contradict the wording of Articles, which are the operative law. However, Recitals must be included to set out the reason for the law, and to help understanding when Articles are ambiguous. For example, see the CJEU in *Parketthandel*[3].

The Recitals therefore particularly help us in particular in understanding the purpose of the ePD and interpreting Art 5(3) if there is ambiguity or uncertainty.

4. The wording of the ePD

Art 5(3) was first introduced in *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 (Directive on privacy and electronic communications)* ('**2002 ePD'**).

The 2002 ePD was later amended, with the current Art 5(3) being introduced in *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* ('**2009 ePD**').

Art 2 of the 2009 ePD sets out the amendments to the 2002 ePD. The 2009 ePD leaves the Recitals to the 2002 ePD, and the title of Art 5, untouched.

Art 5 is entitled: '**Confidentiality of the communications**'. This clearly sets Art 5(3) in the realm of confidentiality.

Art 2(5) of the 2009 ePD replaces the wording of Art 5(3) in the 2002 ePD with the following, which is the current law and the subject of the Guidance (my emphasis):

*'3. Member States shall 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 only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information,*

[2] https://eur-lex.europa.eu/content/techleg/KB0213228ENN.pdf
[3] Case C-134/08, decision 2 April 2009

in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. 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.'*

The wording of Art 5(3) on '*clear and comprehensive information'* reflects the requirements for information to be provided in the DPD and as expanded in the GDPR for consent to be valid. This demonstrates the focus of Art 5(3) on privacy (even though the information need not be personal data) and that use of technology caught by Art 5(3) and not exempted still have to satisfy consent-level information requirements.

There is clearly a debate on the meaning and scope of 'storing', 'gaining of access', 'already stored' and 'terminal equipment'. This is where the Recitals can support interpretation of Art 5(3), starting with the reasons for Art 5(3). There is no debate over the 'strictly necessary' wording.

We therefore need to understand the purpose, the reason, for the ePD and Art 5(3).

5. The purpose of the ePD and the reasons for Art 5(3)

As above, the title of Article 5 concerns confidentiality.

The reason for Art5(3) extends this concern on confidentiality to privacy and is set out in 2009 ePD's Recitals 65 and 66 (my emphasis):

R65 [2009]: *'****Software that surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party (spyware) poses a serious threat to the privacy of users****, as do viruses.* ***A high and equal level of protection of the private sphere of users needs to be ensured, regardless of whether unwanted 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****. Member States should encourage the provision of information to end-users about available precautions, and should encourage them to take the necessary steps to protect their terminal equipment against viruses and spyware.'*

R65 therefore clearly includes, within reasons for Art 5(3), the '*serious threat to the privacy of users*' posed by '*spyware*' which it defines as '*software [that] surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party*'.

R66 [2009]: *'Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to* ***those involving unwarranted intrusion into the private sphere (such as spyware or viruses)****. It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible.* ***Exceptions to the obligation to provide information and offer the right to refuse should be limited*** *to those situations where the technical storage or access is* ***strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user****. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.'*

As above, the Recitals to the 2002 ePD were not removed or amended. The relevant Recitals from the 2002 ePD are R24 and R25 (my emphasis):

R24 [2002]: *'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.'*

R25 [2002]: *'However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in **analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions**. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be **allowed on condition** that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user- friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.'*

These Recitals set out the original reasons for the 2002 ePD and for Art 5(3). They again talk of spyware and, again, the Recitals go further than simple writing or access to information. The intent is to also address spyware, web bugs, hidden identifiers and other similar software or devices whose purpose is surreptitiously monitor the actions of users or to trace the activities of the user to make the user's device do something to the benefit of a third party.

Historically, guidance from the Art29WP and other regulators have acknowledged that Art5(3) does not apply solely to cookies but to other, similar, technologies as well. The above gives clarity on what 'similar' means and confirms that the defining purpose for Art 5(3) – which is fundamental for its interpretation - is addressing threats to the user's privacy from such spyware and similar technology.

The Recitals set out an expansive definition of spyware and confirmation that exceptions should be limited as strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber.

6. Returning to Art 5(3)

These Recitals give much-needed clarity when one returns to the wording of Art 5(3):

*'3. Member States shall 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 only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. 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.'*

It is now clear that 'storing' information and 'gaining access' to information was to be read as covering the use of cookies, spyware, other software and any other technology that monitors or traces the actions of the user and software or which makes the user's device operate in any way beneficial to a third party – all in the context of addressing threats to the privacy of the user.

We can immediately see that:

- a website operator automatically receiving an IP address sent proactively by the user's device with no action by the website operator when a user visits their website is not in scope of Art 5(3) – though it is 'traffic data' subject to its own obligations, as well as potentially personal data subject to GDPR and

other data protection law. Conversely, if a third party makes a user's device send information such as an IP address outside the user's device, then that is caught.

- a 'plain-vanilla' ad presented in a webpage in the user's browser akin to a broadcast is not targeted by Art 5(3) if it does not attempt to identify or track the user or make the user's machine operate in a way to benefit the advertiser, website operator or any third party to the detriment of the user's privacy.

- a tracking pixel which, when called to be presented in the webpage or email, triggers tracing of the action of the user on their device, is caught.

- pixel code, which is typically code delivered within HTML in a webpage or email for example, and which runs on the user's device, typically in the browser, to obtain information from the device and send it to the advertiser, website or email operator or other third party, is caught.

- 'already stored' doesn't require any duration, it is simply that the information is within the individual's personal sphere, which would include the tracing of keystrokes on the device, the motion of a cursor in a browser on the device, etc.

This also means that I disagree with section 2.1 of the Guidelines on criteria, which I suggest is incomplete and incorrectly focussed, and with section 2.5 of the Guidelines on 'gaining access', which I suggest is confusing and not necessary if you take the approach recommended above.

a. Memory doesn't matter

I agree with paragraph 37 of the Guidelines. The type or location of the memory does not matter. This is logically clear from the above analysis, whether or not the actions take place in the hard drive, ROM, RAM, 'ephemeral' or otherwise.

And there is further support from the reasons given in Recital 65 [2009], which confirms that the intrusion on privacy can occur and protection is needed *'regardless of whether unwanted 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.'*

b. Terminal equipment isn't to be interpreted restrictively

The Guidelines take an overly technical definition of terminal equipment from the arena of electrical engineering when the scope and purpose of the ePD and Art 5(3) is clearly set out in the ePD. Akin to the logic in *Schufa*, where the CJEU decided on the interpretation of Art 22 GDPR to give effect to its purpose, the definition in the Guidelines would rob individuals of protection for their privacy in certain of the equipment and devices used by them but not all, for no logical reason and in a manner inconsistent with the clearly-stated purpose of the ePD.

'Terminal equipment' of a user or subscriber in the ePD must be given a broad interpretation in order to achieve the reason and purpose of the ePD. It should cover any device or other equipment in the private sphere of the individual. This would include any device they are using such as, without limitation: mobile phones, laptops, desktops, routers, relays, switches, IoT devices, boosters, and all connected household devices, whether or not they are owned by the individual and whether or not used temporarily. The purpose is to prevent threats to individuals' privacy regardless of device and ownership rights to it – 'device-neutral' if you will. I do not therefore agree with paragraph 15 of the Guidelines.

7. Impact on the Guidelines

I believe the above is a far better starting point and structure for the Guidelines to first clarify the purpose of the ePD and Art 5(3) and then move onto application. I recommend a wholesale redrafting of the Guidelines on this basis.

8. Context for the ePD and Art 5(3)

Art 5(3) and the above Recitals are directly relevant wording to the interpretation of Art 5(3). The following is also relevant for the context to be considered when interpreting Art 5(3). Some of the following is more directly applicable than other parts, however all are relevant for the context.

Art 2(1) of the 2009 ePD clarified the aim of the ePD as amended: Article 1(1) of the 2002 ePD shall be replaced by the following: *'1. This Directive provides for the harmonisation of the national provisions required to ensure an* ***equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, 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.'*

Recitals from 2002 ePD further illuminate the context for Art 5(3) and the directly relevant Recitals, as well as the purpose of the ePD itself.

R28 clearly notes that the user should decide what hardware and software they use.

R28 [2002]: *'End-users should be able to* ***decide what content they want to send and receive, and which services, applications, hardware and software they want to use*** *for such purposes, without prejudice to the need to preserve the integrity and security of networks and services.'*

R33 clearly states that users should not be included in directories without consent.

R33 [2002]: *'****Customers should be informed of their rights with respect to the use of their personal information in subscriber directories*** *and in particular of the purpose or purposes of such directories, as well as their right, free of charge, not to be included in a public subscriber directory, as provided for in Directive 2002/58/EC (Directive on privacy and electronic communications). Customers should also be informed of systems which allow information to be included in the directory database but which do not disclose such information to users of directory services.'*

R38 [2002]: *'Directories of subscribers to electronic communications services are widely distributed and public.* ***The right to privacy of natural persons and the legitimate interest of legal persons require that subscribers are able to determine whether their personal data are published in a directory and if so, which****. Providers of public directories should inform the subscribers to be included in such directories of the purposes of the directory and of any particular usage which may be made of electronic versions of public directories especially through search functions embedded in the software, such as reverse search functions enabling users of the directory to discover the name and address of the subscriber on the basis of a telephone number only.'*

R39 [2002]: '*The obligation to inform subscribers of the purpose(s) of public directories in which their personal data are to be included should be imposed on the party collecting the data for such inclusion.* ***Where the data may be transmitted to one or more third parties, the subscriber should be informed of this possibility and of the recipient or the categories of possible recipients. Any transmission should be subject to the condition that the data may not be used for other purposes than those for which they were collected****. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained either by the initial party collecting the data or by the third party to whom the data have been transmitted.'*

R52 notes that IP addresses may be problematic and difficult areas, and need careful review.

R52 [2009]: *'****Developments concerning the use of IP addresses should be followed closely****, taking into consideration the work already done by, among others, the [Art29WP]'.*

R53 and others deal with the use of traffic data and location data.

R53 [2009]: '*The processing of traffic data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by providers of security technologies and services when acting as data controllers is subject to Article 7(f) of Directive 95/46/EC. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.'*

R14 [2002]: *'Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.'*

R15 [2002]: *'A communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication.* ***Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network****.'*

R22 [2002]: *'The prohibition of storage of communications and the related traffic data* ***[such as IP addresses and any other information automatically sent by a user's device when visiting a webpage etc]*** *by persons other than the users or without their consent is not intended to prohibit any automatic, intermediate and transient storage of this information in so far as this takes place for the sole purpose of carrying out the transmission in the electronic communications network and provided that the information is not stored for any period longer than is necessary for the transmission and for traffic management purposes, and that during the period of storage the confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.'*

R26 [2002]: *'The* ***data relating to subscribers processed within electronic communications networks to establish connections*** *and to transmit information contain information on the private life of natural persons and concern the right to respect for their correspondence or concern the legitimate interests of legal persons. Such data may only be stored to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time. Any further processing of such data which the provider of the publicly available electronic communications services may want to perform, for the marketing of electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available electronic communications services about the types of further processing it intends to perform and about the subscriber's right not to give or to withdraw his/her consent to such processing. Traffic data used for marketing communications services or for the provision of value added services should also be erased or made anonymous after the provision of the service. Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.'*

R28 [2002]: *'The obligation to erase traffic data or to make such data anonymous when it is no longer needed for the purpose of the transmission of a communication* ***does not conflict with such procedures on the Internet as the caching in the domain name system of IP addresses or the caching of IP addresses to physical address bindings or the use of log-in information to control the right of access to networks or services****.'*

Art 2(6) of the 2009 ePD" Article 6(3) shall be replaced by the following:
'3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to

in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his or her prior consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.'

R56 envisages the proliferation of IoT devices etc

R55 [2009]: *'In line with the objectives of the regulatory framework for electronic communications networks and services and with the principles of proportionality and subsidiarity, and for the purposes of legal certainty and efficiency for European businesses and national regulatory authorities alike, [the 2002 ePD], and does not apply to closed user groups and corporate networks.'*

R56 [2009]: *'Technological progress allows the development of new applications based on devices for data collection and identification, which could be contactless devices using radio frequencies. For example, Radio Frequency Identification Devices (RFIDs) use radio frequencies to capture data from uniquely identified tags which can then be transferred over existing communications networks. The wide use of such technologies can bring considerable economic and social benefit and thus make a powerful contribution to the internal market, if their use is acceptable to citizens.* ***To achieve this aim, it is necessary to ensure that all fundamental rights of individuals, including the right to privacy and data protection, are safeguarded. When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply****.'*

R16 bolsters the argument that the ePD is focussed on actions that identify the user, not 'broadcast' actions.

R16 [2002]: *'Information that is part of a* ***broadcasting service*** *provided over a public communications network is intended for a potentially unlimited audience and does not constitute a communication in the sense of this Directive. However,* ***in cases where the individual subscriber or user receiving such information can be identified****, for example with video-on-demand services, the information conveyed is covered within the meaning of a communication for the purposes of this Directive.'*