Playing regulatory catchup?

Having regard to the ePrivacy Directive and previous opinions of the Article 29 Working Party (The Working Party on the Protection of Individuals with Regard to The Processing of Personal Data) and its earlier opinions, the European Data Protection Board (EDPB) ran its public consultation on its newly update technical guidelines for the ePrivacy Directive.[1]

Specifically and solely, the technical guidelines concern themselves with the elucidation of the phrase "'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 as set out in that Article." When looking at the actual wording though, it is not clear from the guidelines that this is somewhat rephrased when compared to the wording in Art. 5 (3) of the ePD.[2] In guidance on fingerprinting in WP29 Opinion 9 / 2014 and on the Cookie Consent Exemption in Opinion 4 / 2012, the WP29 already clarified that in its opinion the relevant phrasing applies to other technologies as well and brings them into the ambit of the clause, and that it does not only apply to cookies. The EDPB also states that perceived ambiguities 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" - while this is true, the selection of its example use cases does not seem to properly reflect the latest development in these technologies, but f.e. Includes technologies like tracking pixels which for a long time have been used also in addition to cookies, so cannot really be said to be used as a response to problematic use of cookies.
The EDPB steps through the phrasing of the sentence part word for word, and also points out specifically that exemptions to the consent requirement are not discussed. This for example also means that whether or not consent has been obtained, or whether other circumstances are present, are out of the scope of the guidelines, in that sense they are very technical, and only technical. This is perfectly fine and in line with their aim, however also strictly limits their usefulness, as it is doubtful if there was really that much ambiguity. With regard to reacting to a changing technical landscape, the EDPB specifically mentions technical identifiers embedded in machines or operating systems, as well as 'tools allowing the storage of information in terminals'. However on the face of it at least, none of these seem to be particularly new. Their description might fit certain new developments however, though you wouldn't know it directly from first reading.

In the detailed analysis, the guidelines step through four major criterions of the phrase of the ePD, which are information, terminal equipment, 'provision of publicly available electronic communications services in public communications networks' and 'gaining of access' or 'storage'. The first criterion is put into the context of its grounding in the private sphere of users and Art 7 of the EU Charter of Fundamental Rights (Respect for Private and Family Life) where

[1] ePrivacy Directive
[2] ePD https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058

the guidance interprets the information very broadly, though with good reason. Essentially, information is designated as all information on a user's device, independent of who or what put it there, and for how long it exists. The EDPB especially stresses that information does not only mean personally identifiable information (PII) as might be inferred by a casual observer. This is in fact a core pillar of its further arguments and the elaboration on the use cases.
The terminal equipment, or more commonly, the devices in question basically cover all kinds of devices according to the guidance, with the exception of relays or other pass-through devices. It also does not matter what ownership model the device employs or if it consists of one or more parts. Furthermore, according to the technical guidelines, it does not matter whether a protected communication was enacted by the user or not.
With regard to the communications technology and public networks, we see a further attempt to make the old ePD future proof, by stressing that it is expressly, as strengthened by recitals and other directives (), not dependent on a particular kind of communications technology or type of network. Even asynchronous or ad-hoc networks are covered, so long as at least potentially more than two devices are part of the network, even though intermittently there might only be two devices. This could for example apply to ad-hoc decentralized networks or transmission technologies that span nets using mobile devices. Further, it is expressly described that the ‘public’ portion of the phrase does not mean that a network has to be freely accessible to all, but just to some subset of the public.
Lastly, the analysis by the EDPB goes into the details of ‘gaining access’ and ‘stored information’ and ‘storage. In this part, the authors explicitly refer to Art 1 of the ePD which refers to ‘an equivalent level of protection … particular the right to privacy, with respect to the processing of personal data’ and the notion that at its core the ePD is a privacy instrument. By then again referring to the sphere of private life a user's terminal equipment is brought back into focus. (Recital 24) This user can also be a legal person, as their rights also should be protected against third parties according to recital 26 ePD. For the purpose of the interpretation of gaining access, the guidelines also describe this very broadly, stating in essence that it does not matter whether the data was actively requested, is sent out periodically or gathered in some other way and that it also does not have to take place cumulatively with the storage of information in that phrase.
Finally further elaborating on the storage part of the phrase at issue, the EDPB writes that usually access and information storage is not direct, but generated by specific software on a website or installed, such as a browser. It also states that the length of time, amount of time or storage medium is irrelevant, and that even networked storage, if functionally equivalent, would fall within the ambit of this phrase. Most importantly, stored information is said to not only refer to files, but to any kind of information by the user, a device, a third party, by sensors or generated locally.

Although the motivations for the technical guidelines are not explicitly stated apart from referring to ambiguities and the updated technical landscape that tries to find workarounds for example for thirds party cookies used for tracking for advertisements, I assume that the general aim of the technical guidelines is to future proof the interpretation of the ePD, without giving too specific examples or targeting any one vendor.

To put some more color on this topic, one most likely example is “Google Topics”, formerly FLoC, which as FLoC used cohorts of users for targeting, and as Topics locally generates categories for a specific site that a user visited (presumably using a small AI model or similar algorithm), and then based on that an advertiser can generate targeted ads. The move from cohorts to topics according to the developers, which include not only Google but also advertising industry bodies, is meant to be both more useful for advertisers, but also easier to understand for users (as they could check and understand categories.) To me, there is no doubt that based on the technical guidelines by the EDPB, a product such as Topics would fall under the ambit of the ePD. While information is processed locally and it is presumably more privacy friendly, it still falls under the regulation of the directive, unless no information at all would leave the device or would be accessed, which is not possible, as far as I know. In that sense, it is admirable that the EDPB succeeded in future-proofing the ePrivacy Directive, but what, if any, consequences remain to be seen. First, not only will the guidelines also have to be interpreted in line the GDPR and other legislation, but it is only a Directive so most likely no member state will soon take action and adapt implementing legislation, so we would have to wait for case law or other action to see if the guidelines and my interpretation holds up. For the mission of the EDPB, it is surprising that it has not been more direct in its description of potential updated technical systems that its new guidelines are meant for. In any case, if it really wanted to future-proof and push forward its interpretation, it would help to be more explicit and also approach companies directly and inform them of its new interpretation. And by approach I do not mean the consultation procedure. Lastly, a further system discussed by Google is the Web Integrity Environment, originally pitched as a sort of digital rights management and safe zone for the web, it was highly criticized, because it would take further control of the users’ devices away from them and solidify Google’s control of users devices and browsers. This API that is to be added to Google Chrome is for example meant to combat click-fraud on advertisements or fake engagement metrics on social media. While some of these goals might be laudable, it would also cement Google’s control, and within the ambit of the ePD, would likely also be caught under the meaning of Art. 5 (3).
Thus, to close this opinion - for more helpful and broadly applicable guidelines, it would help if the EDPB would be more explicit in at least its accompanying information, as like this it will likely only reach a very particular, specialized audience. Still, in so far as the ePD is still relevant, the guidelines are a good attempt a regulatory catchup, or more specifically, slowinh or stopping the spiral of regulatory catchup.