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

First of all, I would like to thank the European Data Protection Board (EDPB) for taking ownership of the ePrivacy Directive and constantly clarifying how the rather legal and non-technical text should be interpreted given the constantly changing technical landscape. It's thanks to these guidelines that the organisation across Europe can constantly improve for the better of the privacy of EU citizens and residents.

While the Guidelines are useful, I would like to raise two issues that are particularly problematic:

Clause 42

> *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 or HSTS) or other functionalities (cookies being one of them). Once again, the abuse of those mechanisms (for example in the context of fingerprinting or the tracking of resource identifiers) can lead to the application of Article 5(3) ePD.*

It would be great if the EDPB could take a position regarding so-called "cookieless" analytics.

Indeed, Matomo implements so-called "cookieless" analytics. It works by sending code to the user's browser. This code then uses various browser-generated information to compute a 24-hour unique visitor hash. Such information includes:

- Browser user agent
- Screen resolution
- Installed fonts
- Installed plugins

I see a risk that Clause 42 could be interpreted as disallowing "cookieless" analytics without a cookie consent banner: "abuse of [HTTP headers including user agent] can lead to the application of Article 5(3) of ePD". This would be, of course, very sad. "Cookieless" analytics are the results of the ePrivacy Directive and are as privacy-friendly as it gets when it comes to analytics.

If even "cookieless" analytics require a cookie consent banner, then it's likely EU residents will see even more cookie consent banners. This would also lead to more organisations trying to employ every possible trick, such as dark patterns, to force analytics onto website visitors.

It would be great if the Clause could be amended as follows: “Sending a time-limited hash over the network, even if said time-limited hash is based on context data, does not lead to the application of Article 5(3) ePD, assuming that (a) the hash cannot be used to extract context data, (b) the hash cannot be used to identity a user, especially not across domains, (c) the hash is renewed after a few hours.”

Note that “after a few hours” is in harmony with “3.6 UI customization cookies” in Opinion 04/2012 on Cookie Consent Exemption adopted by the Article 29 Data Protection Working Party on 7 June 2012.

References

- CNIL's assessment on cookieless tracking
- Matomo Cookieless tracking

Clause 48

> Tracking links are functioning in the same way, but the identifier is appended to the website address. When the URL (Uniform Resource Locator) 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 websites to identify the origin of their inbound source of traffic. For example, e-commerce 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.

Shortlinks are extensively used by the European Commission. These are URLs like https://europa.eu/!gB67HB, which essentially acts like tracking links. However, shortlinks feel more “necessary” for the purpose of directing the user to the right website resources, hence, one could interpret shortlinks as not needing application of Article 5(3) of ePD.

Does the EDPB mean to essentially tell the whole industry to use shortlinks instead of tracking links?

References

- https://wikis.ec.europa.eu/display/WEBGUIDE/03.+Short+URLs