Originally published on the Privacy Laws & Business International Report 193, February 2025

Avoiding the scope of the ePrivacy Directive in advertising

The European Data Protection Board's (EDPB) October 2024 Guidelines on the Technical Scope of Art. 5(3) address the emergence of new tracking methods to replace cookies. In light of the Guidelines, a blanket consent requirement will now be triggered by any act of temporary storage or access on a data subject's device, well beyond the use of cookies and encompassing multiple practices that many considered either privacy-preserving or mostly innocuous and inherent to the inner workings of the internet (including pixels, local processing, URL parameters, or browser-based APIs).

A good illustration of the former is Protected Audiences, an API (or Application Programming Interface) developed over the past few years under the umbrella of Chrome's Privacy Sandbox. A recent Boston University study has concluded that such protocol, which does not track devices individually, can be just as effective as a means of retargeting as third party cookies, provided that a significant number of publishers adopt it. It is however unlikely that such adoption will materialise in the short term, or that there is any benefit in making the effort, given that consent will still be required.

As interpreted, article 5.3 of the ePrivacy Directive is not only resulting in a further departure from the principle of data minimisation, but also running counter to Network Centricity, an essential quality attribute of common privacy engineering and Privacy by Design frameworks. Whereas a decentralisation of data processing activities results in a lower risk of data leakage and enhanced user controls, it is precisely the proximity to a device that will result in greater scrutiny under the ePrivacy Directive.

Should the severe impact of the new guidelines not appear sufficient, supervisory authorities are simultaneously stepping up the enforcement of valid consent standards in the context of digital marketing and online tracking activities. For the leading Data Protection Authorities these actions have become increasingly easier to handle and automate. As an additional incentive, fines based on the ePrivacy Directive can circumvent the One-Stop-Shop otherwise applicable in the context of the GDPR.

Beyond cookies, unique identifiers... and consent

A considerable drop in consent rates for cookies or their ID-based substitutes (browser-based technologies that can replace third-party cookies) has followed the wider adoption of "reject all" options on consent banners, rendering the effort futile for smaller

stakeholders who lack large enough data volumes to give significance to the resulting sample. This has led to a loss of reliable grounds for campaign planning, targeting, or measurement. Things are likely to get even worse when Chrome's announced introduction of a single cross-site consent prompt for third-party cookies takes effect in the coming months.

With all of this in mind, two areas of focus have taken prominence among privacy engineers and legal advisors in the marketing technology space: server-side processing and data anonymisation. In other words, avoiding the scope of the ePrivacy Directive and escaping the data protection regime altogether, respectively.

Revisiting server-side solutions

A circumvention of the data subject's terminal equipment allows data controllers to potentially avail themselves of other legal bases provided by the GDPR, namely legitimate interest and contractual necessity. Both are surely a tall order, but they appear preferable to a direct violation of the core elements of valid consent through the use of dark patterns. We are also putting aside the use of "Consent or Pay" prompts - highly controversial and only available to online publishers in certain countries.

Both Conversion APIs (server-side APIs that allow servers to contact directly third-party advertising platforms) and Data Clean Rooms (secure digital spaces where organisations can share and analyse data from multiple sources while protecting user privacy) rely on a combination of server-side processing techniques and a data controller's ability to collect relevant signals about their own actual or potential customers.

Conversion APIs

When so-called "walled gardens" (large online platforms such as Meta, TikTok, Amazon or Google) are involved, advertisers are being encouraged to regularly upload a batch of online or offline signals associated with a given campaign ("conversion data") that can then feed the optimization loop. This does not always require a parallel effort to broadcast successful events in real time through tracking pixels, but most platforms will encourage a combination of both practices. In the latter case, the *lex specialis* will apply.

Although the EDPB has made it clear that social media platforms (in the specific context of Meta) would not be able to rely on either legitimate interest or contractual necessity for the purposes of behavioural advertising, there may be room for a less restrictive approach whenever it is an advertiser, with limited access to user data, that act as the sole data controller, as appears to be the case when Conversion APIs are in use.

That said, the ePrivacy Directive will once again show its teeth whenever the signals being uploaded have been collected through client-side technologies.

Data Clean Rooms

Data Clean Rooms ("DCR") have been evolving for quite some time now, in parallel to the explosive growth of alternative digital advertising networks and platforms. In particular, retail media networks have given these data collaboration environments increased prominence.

Various DCR offerings (and in-house initiatives) are built on well-known Privacy Enhancing Technologies like "trusted execution environments" in order to isolate an advertiser's first-party data in a securely locked repository, ensuring that all operations performed on such data remain within the control and supervision of a data controller. In other cases, "multiparty computation" will allow different business partners to perform joint operations on separate, previously encrypted datasets.

Given that first-party data has been collected in the context of direct relationships between advertisers, retailers or publishers and their own customers, no need arises for additional consent requests if it can be understood that data collaboration efforts do not fall out of the scope of the originally stated purpose.

However, the generation of look-alike audiences that can be targeted on either the open market or walled gardens, will require matching encrypted identifiers, and the associated data processing could still require consent if it is understood that personal data will be shared with new recipients or categories of recipients. Additionally, both parties to the audience deduplication effort are likely to be deemed joint controllers.

Contextual ads and AI-generated synthetic data

A more drastic measure, beyond avoiding the ePrivacy Directive, would be circumventing the data protection framework altogether. This can be done by working with fully anonymous data. How far can such data be taken?

There is little use for fully anonymous data beyond a basic statistical analysis of aggregated data for audience planning purposes. Recent progress in "differential privacy" (or the programmatic addition of noise) allows for more sophisticated queries on combined datasets, but these efforts tend to cross the very thin line that would render such data pseudonymised, and thus subject to the GDPR.

As a matter of fact, even contextual advertising, considered by many the holy grail of privacy-preserving advertising, relies on IP addresses and requires basic fraud-detection

signals to function, contrary to the recently expanded interpretation of the ePrivacy Directive. In other words, albeit it may technically avoid personal data per se, consent is still required regardless of the level of intrusiveness of the chosen formula, be it purely contextual ads or cross-site, interest-based ads.

As a recent addition to the range of options at hand, generative AI-powered synthetic data does however allow companies to work with truly anonymized data that is both granular and impossible to re-identify. This enables more advanced solutions for cohort definition or targeting criteria, either in isolation or in combination with a common taxonomy of interests. Although previously-trained large language models (LLM) will underpin the generation of such data, the very intentional process of generating a synthetic audience facilitates the introduction of the necessary safeguards, compensating for bias or introducing additional levels of noise.

Exceptions and opportunities

Needless to say, all of the above would change considerably if competent authorities (not necessarily the EDPB) were to subject article 5.3 exceptions to a similar update to the one that the notions of storage and access have now been subjected to. In particular, the concept of "technical necessity" was originally conceived to give cover to technical solutions addressing the so-called "statelessness" of HTTP environments, in a way that shopping carts, language preferences, or account details would be remembered throughout a session. More than twenty years have gone by, and it would make sense to extend these exceptions to the inner workings of privacy-preserving advertising that is inherent to a news publisher, retailer, or otherwise content-based offering.

In the absence of an ePrivacy Regulation that brings device-level protections in line with a risk-based approach, such exceptions would open up the door to a legitimate interest test or data minimisation efforts along the lines of those expressly accepted, under certain conditions, by the French or Spanish data protection agencies with regards to certain cookies previously deemed non exempt: those required for analytics purposes.

Author: Sergio Maldonado