Google's Concerns Regarding the Proposed Requirements for Browser-Level Consent in the Digital Omnibus

Executive Summary

Article 88b of the Digital Omnibus proposal would implement a 'Browser-Level Consent' (**BLC**) for the use of non-essential cookies and similar technologies[1]. Instead of making specific cookie choices on individual websites (via a Consent Management Platform or 'cookie banner'), browsers would need to support users to make consents at a browser-level; those choices would then bind all EEA websites visited using that browser.

While the goal of the proposal is to improve the user experience, in reality it creates technical and legal complexities that could have a potentially catastrophic effect on the user experience, and the functionality of the ad-supported web as a whole. By detaching consent from the specific context of a website, the proposal will severely impact the ability of publishers to use advertising to support free content, inhibit the ability of brands (particularly SMEs) to reach and acquire customers, create significant challenges for achieving meaningfully informed consent, and ultimately **force many more websites to adopt a paywall to fund their services**.

This document briefly explains why non-essential cookies are so critical to the ad-funded internet. We then outline the technical and legal challenges, but above all the economic and societal impact, of implementing a centralised consent mechanism.

Why non-essential cookies are critical to the free internet

Non-essential cookies play three core functions in relation on online advertising, which in turn enables websites to offer their services free of charge:

1. **Personalisation** ensures advertising is relevant to the individual user's interests. It is essential for advertisers, particularly SMEs with limited budgets, to reach a specific target audience, maximising the efficiency of their marketing spend and driving higher conversation rates. Personalisation also improves the user experience by delivering commercial content that provides genuine utility and discovery. Personalised ads provide a critical revenue stream for publishers[2].

2. **Ad measurement**, whether in relation to personalised or contextual advertising, is the only way to connect advertising spend directly to business outcomes. It is the most important KPI for any advertising campaign, connecting ad spend directly to real business outcomes. Put simply, businesses will not risk investing capital in digital advertising without the ability to verify its impact.

3. **Other supporting advertising purposes.** For example, frequency capping is necessary for advertisers to increase reach by avoiding wasted impressions on the same users and to find the

[1] For simplicity, we use the term "cookies" in this paper. However, the proposal applies to any storing of personal data, or gaining of access to personal data already stored, in the terminal equipment of a natural person. EDPB guidance has supported a very broad interpretation of the technical scope of this provision.

[2] A personal touch - Implement Consulting Group, 2025: 60% of publishers' digital ad revenue is from personalised ads

right balance between brand/product/service memorization and overexposure. This is fundamental for both personalised and contextual advertising, and is also essential for optimising the user experience on websites by reducing advertising fatigue and frustration and offering a more varied ad experience. Non-essential cookies may also be used to help advertisers manage brand safety concerns related to ad placement.

This paper is focused on the impact of Art 88b on online advertising and the ad-funded ecosystem, because this is the dominant use case for non-essential cookies. However, we would emphasise that this is by no means the only function of non-essential cookies, and so there would be other consequences of a rapid decline in cookie consent rates.

1. Browser-level consents will collapse consent rates

Unfortunately, a BLC will almost certainly have a severely negative effect on cookie consent rates. When presented with a cookie banner on a specific website, users can make a choice taking into account their use of that service and their trust in the publisher. Publishers can help them contextualize that choice by explaining what consent achieves, beyond just their processing purposes. The user is more likely to appreciate the 'value exchange' in their consent being sought for advertising. The user has a direct relationship with the site, and so is more likely to make a positive choice.

When consent is detached from the specific website a user is visiting, and instead presented at a browser-level, this trust and nuance disappears. The user is being asked to give a broad consent which will apply to *all* websites they may visit in the future, regardless of their feelings towards those individual sites. When faced with such a broad request regarding future activity on unspecified, as-yet unvisited websites, the natural human psychology is to default to 'no'.

This drop in consent rates is not mere speculation. Apple's App Tracking Transparency (ATT) offers some illustrative guidance. Since its introduction in 2021, the global **opt-out rate** (i.e., people refusing tracking) for ATT has stabilized at approximately 78%.[3] This has resulted in a measurable decline in the monetisation (the ability to generate revenue) of online content by 20,55%[4] and significantly lower performance for advertising campaigns resulting in estimated revenue reductions of up to 40 % for brands relying on personalised advertising to acquire new customers, and primarily for SMEs.[5] And whilst some have argued that the high opt-out rate of ATT was driven by its specific, negative phrasing which was misaligned to GDPR consent requirements, a comparison of Apple's own interfaces proves that the centralised nature of the prompt itself is the primary barrier. When comparing the binary ATT prompt to Apple's GDPR-aligned "Personalized Ads" prompt, the opt-in rate only increases from 13% to 25%.[6], which is still far lower than what is typically observed in site-level dialogue (around 70% opt-in rate on the web in Europe).[7]

---

[3] Lennart Kraft, Bernd Skiera & Tim Koschella, *Economic Impact of Opt-in versus Opt-out Requirements for Personal Data Usage: The Case of Apple's App Tracking Transparency (ATT)*, October 2023.
[4] Idem.
[5] Guy Aridor, Yeon-Koo Che, Brett Hollenbeck, Maximilian Kaiser & Daniel McCarthy, *Evaluating the Impact of Privacy Regulation on E-Commerce Firms: Evidence from Apple's App Tracking Transparency*, May 2025.
[6] Sagar Baviskar, Iffat Chowdhury, Daniel Deisenroth, Beibei Li, D. Daniel Sokol, *ATT vs. Personalized Ads: User's Data Sharing Choices Under Apple's Divergent Consent Strategies*, July 2024
[7] Didomi, Consent Collection in 2025, 2025, p. 12-15

Recent economic modeling based on the ATT experience suggests that implementing BLC across the EU would precipitate a **60% to 65% reduction in current consent rates**. This projected drop in consent is estimated to shrink the revenue European businesses generate from digital advertising by **€40 billion to €50 billion annually—a total decline of 30% to 35%**. The sensitivity of this market is extreme: for every additional 1% reduction in the consent rate, the annual revenue generated by European businesses through advertising is projected to drop by a further €600 million to €800 million.[8]

To be clear, consent to non-essential cookies is absolutely critical to the value of advertising. Research indicates that inventory lacking a valid consent signal sells for 50% to 60% less than consented inventory.[9] As well as generating revenue for publishers, personalised advertising also has huge value for retailers, in particular smaller retailers looking to reach a more select market. Whilst large, universal brands may be able to advertise to broad cohorts and accept lost advertising revenue, this is not true for smaller enterprises.[10] For these businesses, it is essential that their advertising reaches users within their market. They simply cannot afford to serve advertising on a non-targeted basis.

In addition, the economic impact of reduced consent rates via a browser consent would not be limited to personalized ads. Browser level consent would equally reduce consent rates for contextual advertising (i.e. ads served based on the content of the page rather than user behaviour). **Non-essential cookies are equally critical for contextual ads, and accompanying – and advertiser business-critical – purposes including measurement, attribution and frequency-capping.**

This drop in advertising revenue will have very real implications for the huge proportion of the internet that relies on advertising to fund free content and services for users. **With this decline in advertising revenue, these independent publishers will no longer be able to offer free content. Their only alternatives will be (1) to close down, (2) require customers to change their browser settings to access the website, or (3) operate behind a paywall.** Given that users may only pay for a limited number of subscriptions (and some may not be able to afford them at all), it is inevitable that a large number of these independent publishers will simply cease to exist, and access to the breadth of the world's information becomes reserved for those who can pay for multiple subscriptions.

Google believes this would be devastating for freedom of information, freedom of speech, democracy, and the sharing of pluralist ideas.

2. **The media service provider carve-out will not shield European media services from economic impact**

The Digital Omnibus proposal itself recognises that BLC will inevitably have an impact on consent rates: so as not to "undermine the economic basis" for independent journalism, the proposal includes

[8] Implement consulting group, Gone in one click, April 2025.
[9] Consent or pay: What publishers should expect, 2024 https://usercentrics.com/knowledge-hub/consent-or-pay-what-publishers-should-expect/.
[10] SMEs represent 99% of European companies: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20241025-1

a carve-out for media service providers[11]. However, this exemption is flawed, because it treats online advertising as a siloed activity rather than an interconnected ecosystem. In reality, it breaks critical links within the ecosystem - without being able to rely on third-party cookies placed on other sites, a media service provider will not meaningfully benefit from the exemption.

To offer an example, a personalised advert on 'Die Welt' for, say, running shoes, will rely on data collected when the user previously visited a site about running clubs in their area; and this requires consent to have been obtained by the third party site. Likewise, if that individual clicks on the ad and makes a purchase, the shoe retailer will rely on cookies to attribute that purchase to the advert on Die Welt.

Consequently, even if a media publisher has greater ability to secure its own consent, the inability to match its audience against external websites and advertisers data breaks the critical link required for personalisation and measurement, rendering the exemption effectively meaningless.

3. Browser-level consent will force publishers towards paywalls – leaving users worse-off

As well as the economic and societal impact outlined above, there will also be a negative impact on the user. **The most significant of these is the proliferation of paywalls, and a reduction in content freely available online**. The ad-funded internet has offered very real benefits to internet users, who can access a plurality of content for free. This enables users to browse across multiple websites, deciding which content to read and interact with. It has enabled democratic debate and the free exchange of ideas, as well as allowing users to fact-check from a variety of different sources.

Once online services can no longer rely on advertising to fund their services, they will be faced with a stark choice: implement a paywall, present new consent banners to users requiring them to change their browser settings, or close down. It is users who will suffer most from this. They will suffer financially, from having to pay numerous subscriptions to access content; but they will also suffer as access to information becomes more limited. As explained above, the media service exemption will not solve this, because advertising on media platforms cannot be treated in silo.

We acknowledge that the proliferation of cookie banners can create friction for the user experience. However, we must also recognise the value such banners provide, in giving users the ability to choose their own digital relationships. Ultimately, the BLC deprives users of the ability to make granular choices: giving consent to the websites they trust, and refusing consent for those they don't. **Research, including a recent survey by the CNIL, shows that 69% of users do not make the same privacy choices across all online services.**[12] A user's willingness to share data often depends on their relationship with a specific brand or the value of the content they are consuming. A single, global preference removes the user's agency to support the specific creators or local news outlets they value.

---

[11] See Recital 46: "In light of the importance of independent journalism in a democratic society and in order not to undermine the economic basis for that, media service providers should not be obliged to respect the machine-readable indications of data subject's choices."

[12] Survey commissioned by the CNIL, *Are we ready to pay for online services without targeted advertising?*, October 2025.

We would also argue that personalised advertising can, in itself, be of benefit for the user - enabling them to see more relevant content, and engage with brands they like. Many consumer benefits, such as "abandoned cart" discounts or loyalty rewards, rely on cookies. However, this value is far less obvious to the user when they are making the choice at a browser-level. As explained above, when presented with a binary choice *outside* the parameters of a trusted relationship with a familiar website, users will naturally default to no.

4. **Browser-level consent risks failing to meaningfully inform users**

Valid consent to non-essential cookies must meet the GDPR requirements of being specific, informed and freely given[13]. This means users should genuinely understand to what they are consenting – and they must be told the identity of the parties processing their personal data, and the reasons why. It also means that users should be given granular choices as to which websites they give their consent to. Clearly, a browser cannot provide meaningful information, or offer any level of granularity, for the literally millions of different web services that exist online. Instead, users will be presented with a binary choice: to accept or reject non-essential cookies across the internet as a whole.

This challenge creates uncertainty for publishers and advertisers who will then need to rely on a consent obtained by the browser. The legality of their own processing operations is contingent on the notice and online choice architecture of a third party, over which the publisher has no control. It also has consequences for the privacy of each user who says 'accept all': in effect, they relinquish their right to transparency and control, and authorise the processing of their information by anyone, and for anything.

5. **Browser-level consent will confuse users in a global Internet**

A further challenge is that browsers will not *enforce* the choice (they cannot, as they do not have server-side access to publisher servers, so cannot know the true purposes for which cookies are used) – only send a signal. In the EEA, that signal will be backed up by the law (websites will be required to comply with it). But outside the EEA, it will be purely voluntary for sites to comply with it.

This leads directly to another type of user confusion, as European users will not clearly understand their choice only applies to EEA sites – or which sites even *are* EEA sites in any meaningful sense – likely in contravention of their expectations and the choices they have made on the browser.

[13] Article 4(11) GDPR.