

That's The Way The Cookie Crumbles



Who Pays When Browser-level Consent Reshapes The Open Web

Dr Diana Năsulea

Programmes Manager and Researcher, IES Europe

8 July 2026

Summary

- Article 88b of the Digital Omnibus makes non-consent the default. By shifting cookie permissions to a single browser-level setting, it replaces site-specific consent choices with a single default setting that most users are unlikely to change.
- The economic cost is expected to be substantial, as reported by multiple sources. Evidence, including a 2026 peer-reviewed field experiment, projects that publisher and advertiser revenues will decline by about 30% when cross-site data is withdrawn. An industry-commissioned modelling study estimates that European advertiser revenue will decline by €40–50 billion, with every additional percentage point decline in consent reducing annual revenue by an estimated €600–800 million per year.
- Revenue losses and compliance costs are likely to be heaviest for smaller market participants. Independent publishers and SMEs that depend on advertising on the open web will experience the greatest losses, while large integrated platforms with extensive first-party data and a large logged-in user base will be comparatively insulated. A measure intended to curb large technology platforms could instead strengthen their market position.
- A default is not a neutral simplification. Making the no-tracking option the default represents a policy judgement about the value of advertising-funded content that is made on consumers' behalf rather than by consumers themselves.
- A better approach would be to standardise consent interfaces, broaden exemptions for clearly low-risk processing, and enable users to express genuine preferences rather than predetermining outcomes through legislation.

Table of contents

SUMMARY	1
TABLE OF CONTENTS	2
INTRODUCTION	3
WHAT ARTICLE 88B WOULD DO	3
THE ANALYTICAL QUESTION: WHO BEARS THE COST?	5
FINDING 1: BROWSER-LEVEL CONSENT IS ASSOCIATED WITH LOWER CONSENT RATES AND REDUCED ADVERTISING REVENUE	5
FINDING 2: THE COSTS FALL DISPROPORTIONATELY ON SMALLER MARKET PARTICIPANTS	7
FINDING 3: BROWSER-LEVEL CONSENT MAY STRENGTHEN INCUMBENT PLATFORMS	9
ASSESSMENT: WEIGHING THE PRIVACY CASE	10
POLICY RECOMMENDATIONS	11
CONCLUSION	11
REFERENCES	12

About the author

Dr Diana Năsulea holds a PhD in Economics and serves as Programmes Manager and Researcher at IES Europe (Institute for Economic Studies Europe), where she designs and coordinates educational programmes, international seminars, and policy research projects promoting classical liberal ideas and economic freedom across Europe. Her research focuses on EU digital and trade policy, exploring their effects on competitiveness, SMEs, and national economies. She has authored numerous research and academic papers in these areas. Beyond her work with IES Europe, Diana is a Teaching Associate at the University of Bucharest's Faculty of History.

About EPICENTER

EPICENTER, the European Policy Information Center, is an independent initiative of thirteen leading think tanks from across Europe. It seeks to inform the European policy debate and promote the principles of a free society by bringing together the expertise of its members.

EPICENTER is formed by the Center for Political Studies (Denmark), Civil Development Forum (Poland), Fundalib (Spain), the Institut économique Molinari (France), the Institute of Economic Affairs (UK), the Institute of Economic and Social Studies (Slovakia), the Institute for Market

Economics (Bulgaria), Istituto Bruno Leoni (Italy), KEFIM (Greece), the Lithuanian Free Market Institute, Prometheus (Germany), the Institute of Economic Studies – Europe (Romania), and Timbro (Sweden). Like its members, EPICENTER is politically independent and does not accept taxpayer funding.

Introduction

The European Commission's Digital Omnibus,¹ published on 19 November 2025, is presented as a simplification package intended to reduce consent fatigue, streamline compliance, and reduce the number of cookie banners. At its core is a technical provision with potentially significant economic consequences. Article 88b of the proposed amendments to the General Data Protection Regulation (GDPR) aims to shift cookie consent settings from site-specific banners to an automated, machine-readable signal set once in the browser or device.

The rationale behind the reform is reasonable. Cookie banners are widely disliked, frequently ignored, and generally regarded as a poor mechanism for obtaining meaningful consent. However, the design of the proposed replacement is as important as the problem it seeks to address. A browser-level consent signal does more than simplify the interface. It establishes a default setting, and evidence from behavioural research suggests that default settings substantially influence user choices. While site-specific banners ask users to make a decision for each website, the browser-level signal will apply a single preference across all websites. The available evidence suggests that most users are unlikely to change the default setting.

Since its publication, the proposal has entered negotiations between the Council of the European Union and the European Parliament. The Council's latest compromise text, which provides an indication of the direction of negotiations rather than the final legislative outcome, retains Article 88b while introducing amendments examined later in this briefing.²

This briefing assesses the economic and structural consequences of this shift. It does not challenge the objective of reducing consent fatigue, nor does it defend the current system of cookie banners, which has well-recognised shortcomings. Instead, it argues that browser-level consent, as proposed in Article 88b, extends beyond addressing a general usability problem and will redistribute billions of euros in economic value, imposing disproportionate costs on the smallest European businesses and publishers, and potentially strengthening the market position of large digital platforms that other elements of the EU's digital agenda seek to constrain. These potential consequences suggest that the proposed simplification may involve important economic trade-offs that warrant careful consideration.

What Article 88b would do

The Digital Omnibus (European Commission, 2025) consolidates cookie rules, previously governed by the ePrivacy Directive, directly into the GDPR through two new provisions. Article 88a sets out

¹ 'Proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework (Digital Omnibus) (COM(2025) 837 final)', European Commission, 2025 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837>).

² 'Proposal for a regulation amending regulations (EU) 2016/679 and others as regards the simplification of the digital legislative framework (Digital Omnibus), Presidency compromise text', Council of the European Union, document

the narrow list of purposes for which storage of or access to information on a user's device is permitted: transmitting a communication, delivering a service the user requested, basic audience measurement by the provider for its own use, and security.³ Article 88b governs how consent, refusal, and objection must be expressed. It requires website operators to ensure their services recognise and respect automated, machine-readable indications of a user's choice, typically set in the browser or operating system, rather than re-prompting users through individual banners. Browser providers other than SMEs (small- and medium-sized enterprises) are required to build the infrastructure, and European standardisation bodies are expected to draft the technical standards.

Two features of the proposed design have economic implications. First, the signal is global: a single setting applies across all websites at once, rather than the user making a separate decision for each site. Second, in the absence of an affirmative signal, the default setting is non-consent. A legal analysis of the proposal observes that the default position of no tracking implies that relatively few will be likely to change it.⁴ Together, these features create a system in which rejecting tracking across all websites is straightforward, whereas providing affirmative consent requires users to change browser settings that relatively few are expected to access.

Independent legal commentators have already identified a structural asymmetry in how this provision is likely to be enforced. Wessing (2026) warns that Article 88b risks becoming a 'one-way ratchet': supervisory authorities are likely to interpret a negative browser signal as a broad, global refusal, while treating a positive signal as too generic to constitute the 'specific' and 'informed' consent required under the GDPR.⁵ If this interpretation prevails, the mechanism would enable universal opt-out but would not provide an equivalent means for universal opt-in. This would create an asymmetry in how user preferences are expressed.

There is also a legal concern. The GDPR requires consent to be freely given, specific, and informed (Article 4(11)); it is not immediately apparent how a single browser-level toggle satisfies these requirements. Specificity should be assessed on a service-by-service basis: consent is meaningful only when it relates to a particular controller and a particular purpose. A uniform signal applied across all websites may reduce specificity, making a negative signal easy to apply as a blanket refusal, while a positive one is less likely to satisfy the requirements for valid consent. The design also assumes that users access the web through a browser, when much of European digital life now operates on apps, connected devices, and AI-driven interfaces that the mechanism does not cleanly govern, and it offers no reliable way to synchronise preferences across domains and devices.

10677/26 (LIMITE), 2025/0360 (COD), Articles 88a(5), 88b(5) and 88b(7). A restricted Council negotiating text, not adopted law.

³ 'The Digital Omnibus: cookies, consent and digital advertising', Taylor Wessing, February 2026 (<https://www.taylorwessing.com/en/global-data-hub/2026/the-digital-omnibus-proposal/gdh---the-digital-omnibus---cookies>).

⁴ 'Digital Omnibus: what the proposed changes mean for GDPR, privacy and cookies', Loyens & Loeff, March 2026 (<https://www.loyensloeff.com/insights/news--events/news/digital-omnibus-what-the-proposed-changes-mean-for-gdpr-privacy-and-cookies/>).

⁵ 'Comments to the European Commission on GDPR and ePrivacy in the digital omnibus', International Center for Law & Economics, 13 March 2026 (<https://laweconcenter.org/resources/icle-comments-to-the-european-commission-on-gdpr-and-eprivacy-in-the-digital-omnibus/>).

The analytical question: who bears the cost?

The case for browser-level consent rests on a tacit assumption: that changing the default allows users' 'true' preferences to emerge, free of nagging banners. From a market perspective, this is the central claim that requires examination. Defaults do not simply reveal preferences. They also shape them. Evidence from behavioural economics (Krishnamurthy and Wills, 2008; Johnson and Goldstein, 2003; Samuelson and Zeckhauser, 1988), together with studies on previous changes to tracking defaults, suggests that users frequently accept the default option presented to them. The relevant policy question is therefore not 'What is the cleaner interface?' but 'Who gains and who loses when the default flips, and is that distribution one the law should impose?'

This briefing evaluates Article 88b against three propositions central to a market-oriented assessment. First, mandating a default setting is a policy choice and not a simplification because it replaces individual user choice with a regulator-defined default regarding ad-funded content. Second, the costs are concentrated rather than evenly distributed, falling primarily on businesses and publishers that depend on the open web. Third, the measure could strengthen the position of dominant platforms, widening the competitive gap that EU digital policy seeks to reduce. The following sections consider each of these propositions by applying the available evidence.

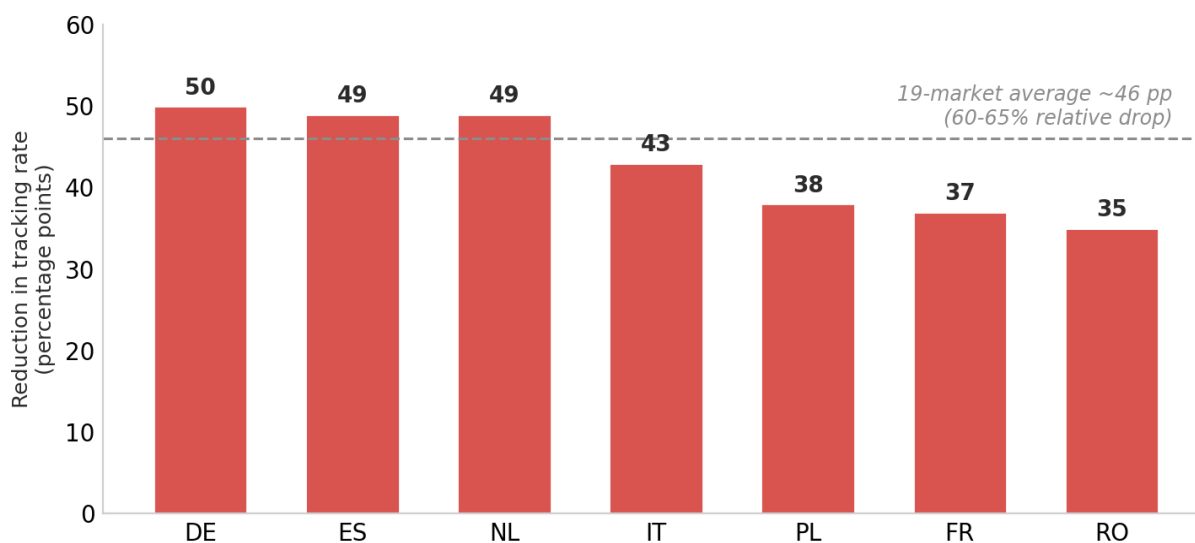
Finding 1: Browser-level consent is associated with lower consent rates and reduced advertising revenue

Studies show that most Europeans will not opt to share their data. Existing studies suggest a consistent pattern when users are presented with balanced consent choices. When users in Germany and France are presented with a cookie permissions banner that gives 'accept' and 'reject' equal prominence, fewer than 25% accept cookies. Aggregate EU consent rates across studies in 2024 and 2025 were in the low-to-mid 40s, with ad-supported media recording substantially lower rates.⁶ Behavioural studies on cookie banners find a similar pattern: interest in actively configuring tracking preferences is 'universally low', with under 2% of users in Germany ever opening cookie settings.⁷ A browser-level default of non-consent would extend this behavioural pattern by making browser settings the primary means to opt in.

⁶ 'Cookie consent rates by industry: 2026 benchmarks', Kukie.io, March 2026 (<https://kukie.io/blog/cookie-consent-rates-industry-benchmarks>); and 'Cookie consent trends by country', CookieYes, January 2026, citing Advance Metrics. Multiple independent CMP datasets converge on sub-25% acceptance in Germany and France given equal-prominence banners.

⁷ 'Cookie behaviour study: 5 years after GDPR', Advance Metrics, 2024 (<https://www.advance-metrics.com/en/blog/cookie-behaviour-study/>).

Figure 1. Reduction in the tracking rate across the seven EU markets covered in the study, following the launch of Apple’s App Tracking Transparency



Source: Kraft, Skiera, and Koschella (2023)

The closest real-world evidence on user behaviour when tracking requires an explicit opt-in comes from Apple’s App Tracking Transparency (ATT). A peer-reviewed analysis of billions of ad impressions across nineteen countries found that ATT cut the share of trackable traffic in the US from 73% to 18% and reduced the tracking rate by an average of around 46 percentage points across all markets studied (Figure 1) – a relative reduction of approximately 60–65%. The authors are clear about their conclusions: the opt-in approach ‘makes the no-tracking (versus tracking) alternative the default option’, and ‘this design decision matters tremendously’ (Kraft, Skiera, and Koschella, 2023).⁸ ATT is a conservative proxy because users are prompted on an app-by-app basis, whereas a browser-level signal applies a single preference across websites, making active opt-in potentially less likely.

A substantial reduction in consent rates would not merely reduce the targetable audience. It will degrade the effectiveness of the whole digital display market. Personalised open-web advertising that depends on third-party data will no longer be able to reach users who do not consent and will have to rely on less effective contextual advertising. Social advertising, built on first-party data, will continue to work, but the ability to measure conversions among non-consenting users will diminish. Even contextual advertising will become less efficient because publishers will no longer be able to optimise campaigns using reliable engagement metrics.

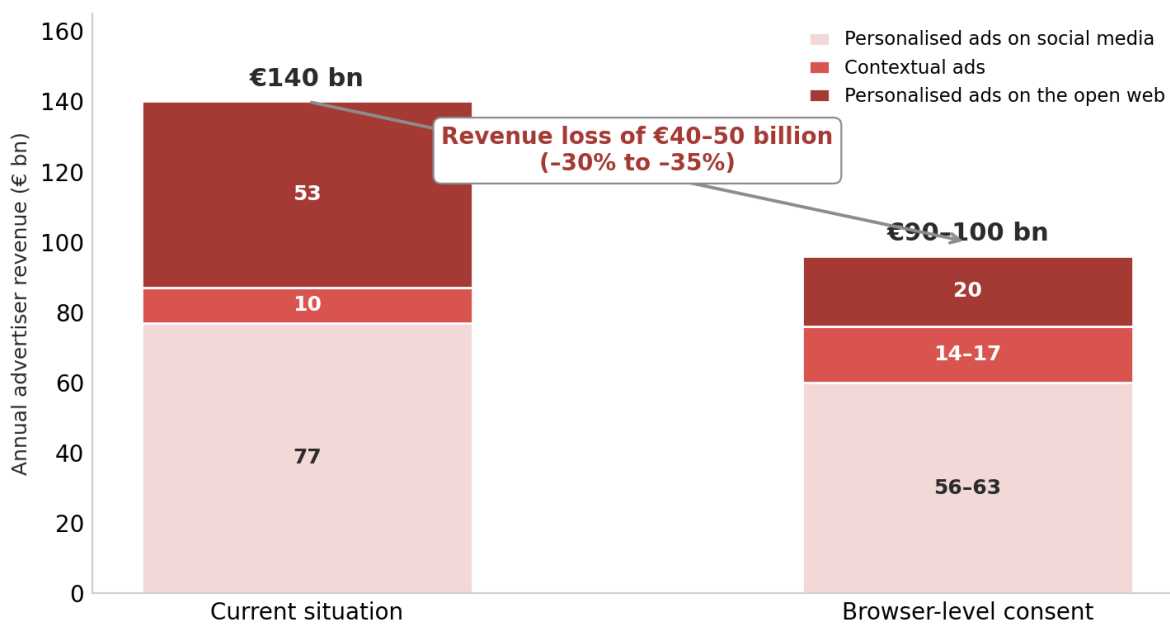
The order of magnitude of the anticipated revenue loss is corroborated by independent and, in one case, peer-reviewed evidence, not just a single study. A market-wide field experiment by Gu, Johnson, and Kobayashi (2026) estimates that removing third-party cookies will reduce publisher advertising revenues by 29.1%, and browser-based privacy-enhancing alternatives will recover only 4.2% of that loss at observed adoption levels. This figure aligns with the broader literature: Ravichandran and Korula’s (2019) Google experiment found a median per-publisher revenue decline of 64% when third-party cookies were disabled, and Johnson, Shriver and Du (2020) found that ads

⁸ Reductions in the tracking rate (before–after estimates) across the seven EU markets studied: 50 pp (DE), 49 pp (ES), 49 pp (NL), 43 pp (IT), 38 pp (PL), 37 pp (FR), and 35 pp (RO).

for opt-out users earn 52% less than for trackable users, both consistent with the reductions estimated here.

The headline figure from the most detailed EU-specific modelling study to date broadly aligns with these findings. An industry-commissioned analysis estimates that European advertiser revenue could fall by €40–50 billion, or 30–35%, assuming advertising expenditure remains constant. The estimated losses are expected to result primarily from reduced advertising efficiency rather than reduced reach: cost per conversion could increase by up to 73% if third-party data is eliminated, and contextual advertising could become 66% less efficient than its personalised equivalent (Figure 2). The same analysis estimates that each additional 1% relative fall in the consent rate could reduce annual advertiser revenues by €600–800 million (Thelle et al., 2026).

Figure 2. Estimated annual advertiser revenues in the EU: current situation versus if browser-level consent settings are introduced



Source: Thelle et al. (2026)

This revenue is not abstract. It is the income European businesses currently earn as a return on the money they have spent to reach customers. A one-third reduction in these returns, due to a change in the consent protocol rather than in firms' products or commercial performance, would represent a significant adjustment for the advertising-supported internet economy on which many European businesses rely.

Finding 2: The costs fall disproportionately on smaller market participants

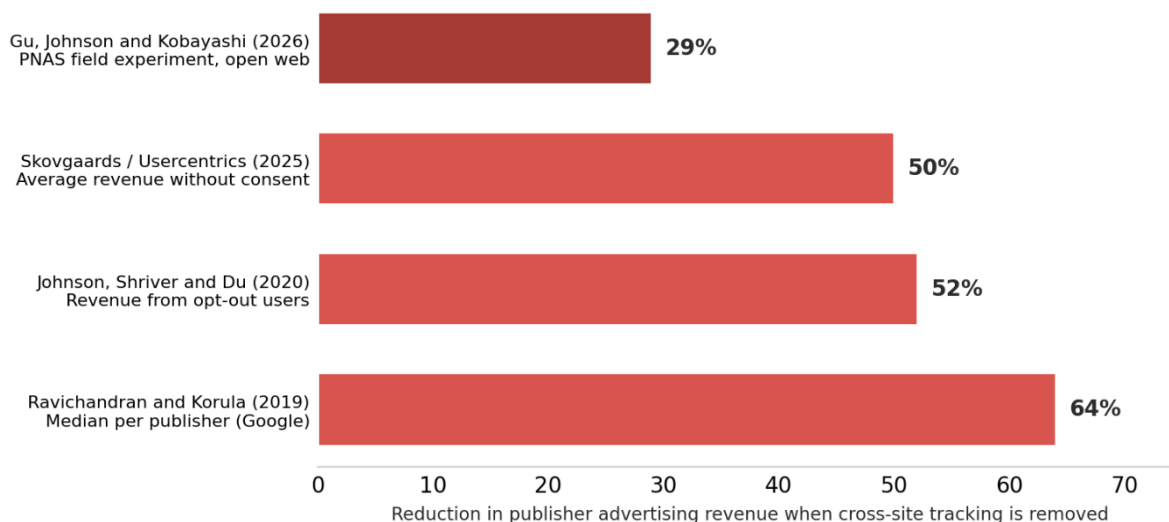
If the €40–50 billion were spread evenly across the digital economy, it would still be a significant cost. However, it is not spread evenly. The losses are likely to fall disproportionately on the parts of the European market least able to absorb them: independent publishers and small and medium-sized enterprises that depend on advertising on the open web rather than on their own logged-in platforms.

The reason is structural. A large integrated platform can monetise its logged-in user base using first-party data, which will not be affected by a no-tracking signal. An independent news site, a niche

recipe blog, a regional classifieds service, or a small e-commerce shop has no comparable stock of first-party data. They earn revenue by selling open-web advertising space on their websites, whose value depends on the third-party data that browser-level consent will switch off. Similarly, they buy open-web advertising to find customers they cannot reach any other way. When the default changes, large platforms are likely to retain a greater share of their existing business, while smaller publishers will face disproportionately larger revenue losses.

The co-legislators are aware of this objection. The Council’s compromise text addresses this concern by exempting media service providers from the obligation to honour the browser signal. The recitals justify this exemption by referring to ‘the importance of independent journalism in a democratic society’ and the need ‘not to undermine the economic basis for that’.⁹ The inclusion of this carve-out suggests that the Council recognises the potential adverse effects on media organisations. But it does not solve the problem; instead, it narrows and relocates it. The exemption protects a defined class of recognised media services. It does nothing for the far larger open web that operates outside that definition – SMEs, niche blogs and community sites, regional classifieds, small e-commerce shops, and independent ad-tech intermediaries – none of which is a ‘media service provider’ yet all of which depend on third-party data. The losses will not disappear. Instead, they are likely to become more concentrated among the businesses the carve-out excludes. The exemption therefore mitigates potential effects for one sector without addressing comparable impacts on other businesses. The proposal therefore differentiates between business models by exempting one category of organisation while leaving others subject to the default browser signal.

Figure 3. Independent estimates of the reduction in publisher advertising revenue when cross-site tracking data is removed



Sources: Gu, Johnson, and Kobayashi (2026); Skovgaards (2025); Johnson, Shriver, and Du (2020); Ravichandran and Korula (2019)

Sector estimates provide quantitative evidence of the impact on publishers as well. A widespread reduction in consent could trigger a 50–60% revenue decline for independent EU publishers, given the risk that the EUR 10.6 billion in annual cookie-reliant advertising spend the sector earns could

⁹ Council compromise text 10677/26, Article 88b(3), and recital 46. The exemption applies to ‘controllers that are media service providers when providing a media service’. https://noyb.eu/sites/default/files/2026-06/5th_compromise_text_Politico.pdf

shift away from European publishers altogether.¹⁰ The distribution of these losses is particularly important and has been documented by other studies. The field experiment by Gu, Johnson and Kobayashi (2026) found that revenue losses will be concentrated among news publishers; Google's own randomised experiment likewise estimates the steepest income declines for smaller publishers, while larger sites that can lean on first-party data are expected to fare better. An analysis of the GDPR's opt-in requirement reached the same conclusion: it is the ability of smaller third-party firms to predict and serve customers, rather than that of internet giants with cross-domain reach, which will be most weakened when consent becomes scarce (Aridor et al., 2023). Advertising expenditure is unlikely to disappear. Instead, it is likely to shift to more efficient channels, which are overwhelmingly the largest first-party platforms. A measure intended to protect Europeans thus risks transferring revenue from European publishers to a handful of non-European incumbents.

A well-functioning market enables the value of ad-funded content to be discovered through countless individual exchanges, in which users trade attention and data for content they would otherwise have to pay for. A browser-level default consent setting can change the nature of that exchange. By setting non-consent as the default, it inadvertently favours tech giants with the resources to lobby for, comply with, and survive changes of this kind.

Finding 3: Browser-level consent may strengthen incumbent platforms

A central objective of the EU's digital agenda is to address the substantial market power of a small number of large digital platforms. The Digital Markets Act, initiatives to promote interoperability, and the measures to address self-preferencing all reflect the objective of fostering competition, protecting European markets from the dominance of overseas incumbents, and enabling new market entrants. The likely effects of Article 88b appear difficult to reconcile with that objective.

By reducing the effectiveness of the open web's principal monetisation mechanism while leaving first-party data comparatively unaffected, browser-level consent may strengthen the competitive position of the largest platforms. The possibility is consistent with evidence from studies examining the market effects of the GDPR. Peer-reviewed research on the GDPR's market effects demonstrates that websites' choices following the regulation entrenched Google and Facebook. Although both companies lost partners in absolute terms, their relative shares of the web technology vendor market rose, because larger vendors were better able to secure consent and offer compliance at scale (Johnson, Shriver, and Goldberg, 2023). Analysis by Stanford's Institute for Economic Policy Research reached the same conclusion: there is clear evidence that the GDPR benefits larger firms at the expense of smaller ones, because large sites can collect consent more successfully and suffer smaller revenue losses, producing a sustained competitive advantage.¹¹

A similar mechanism may apply to Article 88b. If consent becomes scarce, the advantage of owning a logged-in, identified audience is likely to multiply. Firms with a diversified portfolio of consumer-facing products can obtain consent across their own estate and reuse first-party data across their

¹⁰ 'Consent or pay: what publishers should expect', Usercentrics, 31 March 2025 (<https://usercentrics.com/knowledge-hub/consent-or-pay-what-publishers-should-expect/>). Usercentrics estimates an average advertising revenue drop of around 50% should consent be significantly withdrawn; this is an estimate contingent on the final scope of Article 88b and on national enforcement.

¹¹ 'Balancing act: protecting privacy, protecting competition', Stanford Institute for Economic Policy Research (SIEPR), January 2023 (<https://siepr.stanford.edu/publications/policy-brief/balancing-act-protecting-privacy-protecting-competition>).

own services; a standalone publisher or a small advertiser dependent on the open web cannot¹². Industry submissions similarly argue that Article 88b risks 'creating new digital gatekeepers' by concentrating effective advertising in the hands of firms that already control large authenticated user bases.¹³

This illustrates a broader regulatory concern that policy outcomes may differ from policy objectives. Large firms are often better placed to absorb compliance costs, adapt to regulatory change, and maintain existing revenue streams than smaller competitors. A likely consequence of Article 88b may therefore be a widening of existing competitive advantages rather than a reduction in market concentration.

Assessment: weighing the privacy case

The strongest argument for Article 88b is genuine and deserves to be addressed directly. Cookie banners are a failure of regulatory design. They train users to click 'accept' reflexively, bury refusal behind extra steps, and produce consent that is neither informed nor freely given in any meaningful sense. A browser-level signal that allows users to express a single preference once, and have it honoured everywhere, would in principle be a clear improvement in both user experience and the quality of consent. The European Data Protection Board and the European Data Protection Supervisor have welcomed the mechanism for exactly these reasons.¹⁴

However, there are three other aspects we need to consider. First, the privacy benefit and the economic cost are not independent: the aspect that makes the browser-level consent setting attractive, that it can be set once and applied globally, will also likely produce a substantial reduction in consent rates, on the order of 60–65%. The simplification achieved by a browser-level interface depends on the default it implements. Second, the choice of default is central to the policy's effects, and it is being made for citizens rather than by them. An alternative approach would be to standardise the interface while allowing users to make site-specific decisions. Mandating that non-consent be made the default pre-commits everyone to a single evaluation of ad-funded content. Third, the proposal's own narrow exemptions make the problem worse: by excluding common low-risk uses such as basic advertising measurement, frequency capping, and fraud detection from the list of permitted purposes, it pushes ordinary commercial activity into the consent bottleneck rather than out of it.

A fair assessment must also credit the Council's attempt to mitigate harm. The media carve-out in the compromise text is a genuine improvement for the news publishers it covers, and it shows that the co-legislators are taking the economic objection seriously rather than dismissing it. The difficulty is that a targeted exemption treats the symptom while preserving the cause. The existence of a sector-specific exemption suggests that legislators recognise the possibility of uneven economic effects. However, because the exemption applies only to recognised media organisations,

¹² Geradin, Karanikioti and Katsifis (2021) and Johnson (2022) survey evidence that the GDPR increased data-vendor concentration and disproportionately harmed smaller firms.

¹³ 'Digital omnibus: alternative for browser-level consent management (Art. 88a and 88b)', joint position paper by Digital Poland Association, ZPP, IAB Polska, European Tech Alliance, Local Media Association, Employers of Poland, Lewiatan, KIGEiT, Chamber of Digital Economy, and Izba Wydawców Prasy, May 2026 (<https://www.iab.org.pl/wp-content/uploads/2026/05/Digital-Omnibus--Alternative-for-the-browser-level-consent-management-Art.-88a-and-88b-.docx-2.pdf>).

¹⁴ 'EDPB-EDPS Joint Opinion on the Digital Omnibus', European Data Protection Board and European Data Protection Supervisor, February 2026 (https://www.edps.europa.eu/data-protection/our-work/publications/edps-edpb-joint-opinions/2026-02-10-edpb-edps-joint-opinion-digital-omnibus_en). Supports the aim of Article 88a, welcomes Article 88b, and suggests broadening the exemption list to include contextual advertising.

comparable effects on other businesses that depend on the open web may remain. An alternative default could potentially reduce these effects without requiring sector-specific exemptions.

None of this requires defending surveillance advertising or dismissing privacy. It requires recognising that privacy and the open web both have real value, but Article 88b gives greater weight to privacy objectives, with potentially significant consequences for the economics of the open web. A more careful design could protect privacy without the associated economic costs. The policy objective should be to design a mechanism that allows users to express their preferences clearly without predetermining them by mandating a certain default choice.

Policy recommendations

To reduce consent fatigue while minimising unintended economic consequences, the co-legislators should consider the following measures.

1. **Avoid legislating a non-consent default.** The central concern is that Article 88b establishes a default preference rather than requiring users to express one. Standardise the consent interface and the machine-readable signal, but design them so that no preference is presumed: an absent signal should be read neither as blanket refusal nor as blanket consent. The mechanism's task is to signal a real choice once a user makes one, service by service, rather than infer one on the user's behalf. This keeps the design consistent with the GDPR's requirement that consent be freely given and unambiguous, which may be difficult to reconcile with a presumed response in either direction.
2. **Ensure a workable opt-in mechanism.** If a negative browser signal is honoured as a global refusal, a positive signal must be considered as constituting valid consent. Otherwise, the mechanism risks becoming a 'one-way ratchet', allowing universal refusal without an equivalent mechanism for universal consent.
3. **Broaden exemptions for low-risk processing.** Extend Article 88a's permitted purposes to cover basic advertising measurement, frequency capping, fraud detection, and contextual advertising, so that routine, low-risk activities do not depend on a consent signal that many users may never provide.
4. **Assess distributional impacts before adoption.** Require a dedicated impact assessment that quantifies the effect of Article 88b on independent EU publishers and SMEs, and on the competitive position of large first-party platforms, rather than treating the cost as evenly spread.
5. **Avoid reinforcing the position of existing gatekeepers.** Ensure consistency with the EU's own competition objectives by designing the consent framework such that it does not disproportionately advantage platforms that control large first-party data ecosystems over the open-web challengers the Digital Markets Act seeks to protect.
6. **Sequence implementation around evidence.** The compromise text already staggers application out to 24 months for controllers and 48 months for browser providers. Use that runway to pilot and measure real consent and revenue effects across member states, and across business sizes, before adopting a default whose long-term effects may prove difficult to reverse.

Conclusion

Browser-level consent offers a promising response to an important policy question: how to replace the current system of cookie banners, which often fails to secure meaningful consent. However, Article 88b goes further by establishing a default that extends beyond simplifying the consent

interface. In doing so, it gives greater weight to reducing consent fatigue than to preserving the economics of the advertising-supported open web. Evidence from peer-reviewed field experiments and EU-specific modelling suggests that browser-level consent could reduce advertising revenues by roughly one-third, with the largest effects borne by independent publishers and smaller businesses, while strengthening the competitive position of large, first-party platforms.

The fix is not to keep the banner. It is to separate the two questions that the proposal currently fuses. Simplify the interface, by all means. But let Europeans, not their browsers and not their regulators, decide what their attention and data are worth. A reform that does the first while quietly determining the second is not simplification. Such an approach risks producing significant distributional effects that concentrate revenue in the hands of a few.

References

Aridor, G., Che, Y.-K., Nelson, W., and Salz, T. (2023). The effect of privacy regulation on the data industry: empirical evidence from GDPR. *RAND Journal of Economics* 54(4): 695–730.
<https://doi.org/10.1111/1756-2171.12455>

Geradin, D., Karanikioti, T., and Katsifis, D. (2021). GDPR myopia: how a well-intended regulation ended up favouring large online platforms. *European Competition Journal* 17(1): 47–92.
<https://doi.org/10.1080/17441056.2020.1848059>

Gu, Z., Johnson, G. A., and Kobayashi, S. J. (2026). Can privacy technologies replace cookies? Ad revenue in a field experiment. *Proceedings of the National Academy of Sciences* 123(19): e2603752123. <https://doi.org/10.1073/pnas.2603752123>

Johnson, E. J., and Goldstein, D. (2003). Do defaults save lives? *Science* 302(5649): 1338–1339.
<https://doi.org/10.1126/science.1091721>

Johnson, G. (2022). Economic research on privacy regulation: lessons from the GDPR. NBER working paper 30705. Cambridge, Massachusetts: National Bureau of Economic Research.

Johnson, G. A., Shriver, S. K., and Du, S. (2020). Consumer privacy choice in online advertising: Who opts out and at what cost to industry? *Marketing Science* 39(1): 33–51.
<https://doi.org/10.1287/mksc.2019.1198>

Johnson, G. A., Shriver, S. K., and Goldberg, S. G. (2023). Privacy and market concentration: intended and unintended consequences of the GDPR. Federal Trade Commission.
https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-garrett_johnson.pdf

Kraft, L., Skiera, B., and Koschella, T. (2023). Economic impact of opt-in versus opt-out requirements for personal data usage: The case of Apple's App Tracking Transparency (ATT). Working paper. European Research Council (Horizon 2020, grant 833714).
<https://dx.doi.org/10.2139/ssrn.4598472>

Krishnamurthy, B., and Wills, C. E. (2008). Characterizing privacy in online social networks. *Proceedings of the First Workshop on Online Social Networks (WOSN '08)*: 37–42.
<https://doi.org/10.1145/1397735.1397744>

Ravichandran, D., and Korula, N. (2019, August 27). Effect of disabling third-party cookies on publisher revenue. Google. https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf

Samuelson, W., and Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty* 1(1), 7–59. <https://doi.org/10.1007/BF00055564>

Skovgaards, K. (2025, March 31). Consent or pay: What publishers should expect. Usercentrics. <https://usercentrics.com/knowledge-hub/consent-or-pay-what-publishers-should-expect/>

Thelle, M. H., Woltman, H. H., Østergaard, B., and Tranholm-Mikkelsen, N. (2026). Gone in one click: Assessing the socio-economic impact of browser-level consent in the EU. Implement Consulting Group. <https://implementconsultinggroup.com/article/gone-in-one-click>