Cookie Fatigue and the Digital Omnibus

EDAA Summit: Consent, Browser Signals and Regulatory Reform

Dr M.R. Leiser (Mark) | 17 November 2026

Core Position

Reduce unnecessary consent requests through a purpose-based statutory whitelist. Make refusals durable and portable. Preserve specific permission for intrusive tracking, and require evidence that the entire processing chain respects the choice. Browser controls can support that settlement; their convenience does not settle consent validity or market neutrality.

Objectives

Session Objective	Concrete Outcome
User Agency	Identify unnecessary requests; distinguish a portable refusal from valid permission; verify downstream execution.
Risk and Proportionality	Assess likelihood and severity against actual capabilities and safeguards, including foreseeable vulnerability.
Usable Transparency	Explain the purpose, responsible actors and consequences at the decision point, with effective withdrawal and redress.

Status checked 17 November 2026. The Council mandate and Commission proposal are negotiating positions. Parliament's procedure file still records a pending committee decision. Existing GDPR and ePrivacy obligations continue to apply. [2–4]

INTERVENTION 1 | BEYOND CONSENT

Browser Signals and Valid Consent

Question 1 Can a Central Signal Preserve Specific and Informed Choice

Cookie fatigue exposes a failure of regulatory architecture. We ask people to negotiate repeatedly over operations with very different consequences, then treat the resulting clicks as evidence of control. My starting point is to reduce the operations that require permission. A more convenient interface cannot repair an excessive consent requirement.

The research supports reusable choices, but requires careful interpretation. Decarolis and his colleagues found that an inferred signal matched 90 per cent of later explicit choices, falling to 65 per cent when non-response counted. Silence cannot supply GDPR consent. Farronato, Fradkin and Lin find substantial modelled welfare gains from browser-level choice because repeated decisions consume time. That strengthens the case for reducing interruption; it does not establish the legal validity of a blanket yes.

We also need to update the question. The Council's October mandate deletes Article 88b and keeps device access in ePrivacy, with easy one-click refusal or equivalent and at least four months before another same-purpose request. Parliament's position remains pending. I support tackling unnecessary prompts at source and would restore the Commission's six-month minimum. The expiry of that period should not itself trigger another request.

Refusal and permission perform different legal functions. A deliberate refusal can travel with a defined scope. An affirmative instruction must still identify the controller and purpose, reflect an informed and freely given decision, and remain easy to withdraw. Selecting personalised advertising during laptop setup cannot authorise every future recipient and use. Shared devices

make that assumption weaker. Software can transmit valid consent; automation cannot manufacture the missing specificity.

Nor does centralisation remove deceptive design. The browser operator chooses the defaults, labels and friction. Test whether users understand the setting, whether independent tools can carry it, and whether changing it is straightforward. A deliberate site-specific permission can express a different choice. A fresh interruption designed to exhaust a standing refusal should not. Record refusal without creating a new cross-site identifier.

My proposed settlement combines a bounded whitelist of low-risk purposes with portable refusals and specific permission for the remaining uses. Then inspect execution. Does refusal stop the relevant processing at the publisher and its partners? Does withdrawal reach everyone relying on that consent? Do users retain control when the software changes? Those are the outcomes legislation should secure. Counting fewer banners tells us about interruption. It cannot tell us whether the system respects the decision.

Outcome to Secure Secure fewer unnecessary requests, a six-month minimum against same-purpose re-asking, and verifiable execution of refusals and withdrawal.

Sources 1–6 and 10. The six-month preference and wider safeguards state my proposed settlement.

INTERVENTION 2 | BEYOND CONSENT

The Open Web and AI Agents

Questions 2 and 3 Who Controls the Choice and Who Sets the Standard

A browser-level privacy control also allocates economic power. Its operator decides how other businesses reach users and which forms of measurement remain available. A publisher dependent on external partners starts from a different position from a platform with extensive signed-in activity. The legislature should examine that distribution before making the browser the compulsory intermediary for everyone else's relationship with the user.

Apple's App Tracking Transparency provides a concrete warning. The French competition authority accepted the privacy objective but found the implementation disproportionate and particularly burdensome for smaller publishers. The decision is under appeal. The lesson concerns discriminatory implementation; it does not establish that privacy protection necessarily damages competition. Compare equivalent processing by the operator's own services and independent publishers, including what each can still do after refusal.

An impact assessment should separate fixed compliance costs, lost measurement and changes in advertising revenue. Report effects by publisher size, business model and access to first-party data. Test whether spending moves into closed ecosystems. Revenue loss cannot authorise unlawful tracking. Equally, a privacy objective cannot exempt a dominant intermediary from scrutiny of the conditions it imposes on others.

If legislators revive Article 88b, they must define the instruction's scope, precedence and withdrawal before standards bodies encode it. Independent choice tools should participate on equivalent terms. Instructions should travel between browsers, apps and agents without requiring a universal user identifier. Publishers should benefit from the same bounded low-risk routes as other services. A categorical media exception allowing them to ignore reusable preferences would undermine the claimed consumer benefit.

EDAA has practical experience through AdChoices and YourOnlineChoices. Its most useful contribution would be open implementation trials: can users find and understand a control, does the instruction reach participating firms, and does processing change? Publish failures as well as successes, allow independent verification and provide redress. Membership of a scheme cannot

supply a lawful basis. Technical conformity cannot establish that the underlying permission was valid.

Now put an AI agent between the user and the advertiser. I ask it to find a weekend in Lisbon. It can share dates and a budget without disclosing my booking history. I should know who sponsored the recommendation, what information the agent disclosed and how to revoke its authority. Permission to search does not itself authorise a purchase. The future-proofing test is whether that limited authority remains intelligible and enforceable across the transaction, even when no browser banner appears. Legislation should protect that relationship across technologies; the standard should make the instruction work.

Outcome to Secure Require neutral and interoperable controls, evidence of effects on independent publishers, and limited, revocable authority when agents act for users.

Sources 1–4, 7, 8 and 10. Neutrality, portable authority and published execution tests are proposed safeguards.

INTERVENTION 3 | BEYOND CONSENT

Proportionate Reform Beyond Consent

Question 4 Which Uses Need Permission and What Should Regulators Deliver

We are asking consent to resolve questions the legislature should answer. Counting an audience and building a profile across services create different capabilities. Requiring the same ritual for both conceals that distinction and makes users absorb the cost of regulatory indecision. Reform should make constrained, useful processing predictable before anyone designs another banner.

The Council's routes for audience measurement, technical security and contextual advertising measurement provide a starting point. My proposed whitelist goes further: constrained analytics, authentication, necessary service and transaction fraud prevention, and first-party advertising delivery, measurement, frequency capping and brand safety. These are bounded functions, not sectoral immunities. The law should specify permissible inputs, recipients, retention and reuse. Cross-service tracking and behavioural profiling would remain outside those exemptions and require valid consent under my proposed settlement.

Risk assessment must examine likelihood and severity. Map the operation, the technical and organisational measures reducing exposure, and the controls preventing harmful outputs or reuse. Assess children's and other users' foreseeable vulnerability through the design and context, without constructing vulnerability databases. A first-party label does not make processing low risk. Pseudonymisation alone does not establish anonymity, and anonymous outputs do not erase obligations governing identifiable inputs.

The Board's final guidelines of 10 November confirm that legitimate interests are an ordinary legal basis. Under current law, GDPR legitimate interests cannot override an independent ePrivacy consent requirement. Where Article 6(1)(f) applies, establish the legitimate interest, necessity and the balance against individuals' rights. KNLTB confirms that commercial interests can qualify; it does not make them prevail. Reasonable expectations and less intrusive alternatives remain central. A direct-marketing objection stops processing for that purpose, including related profiling; it does not automatically prohibit every audience count.

AI needs its own assessment. Retain an operative clarification that qualifying development and operation can rely on legitimate interests, subject to the full test. Require source-selection discipline, minimisation and safeguards against data leakage and harmful outputs. Article 9 remains a separate requirement for sensitive data. An opt-out cannot cure an unlawful collection or substitute for a missing legal basis.

The EDPB and EDPS already invite a narrow contextual advertising exception. They also support machine-readable choices, so their support for exemptions cannot be presented as opposition to

Article 88b. Helsinki promises practical clarity and cooperation. The Board should publish a timetable and joint guidance that turn those commitments into usable compliance routes. My duty to cooperate would require early engagement across overlapping mandates and reasons for unresolved disagreement. My Innovation Mandate would require evidence of risk and reasons for rejecting less burdensome lawful alternatives. Neither permits a regulator to waive statutory protection. Cookie reform should deliver fewer unnecessary decisions and stronger accountability for the processing that remains.

Outcome to Secure Agree a purpose-based statutory whitelist with enforceable safeguards and coordinated guidance that organisations can use before deployment.

Sources 1–5 and 9–13. The wider whitelist and institutional duties are my reform proposals, not current exemptions.

Supporting Analysis

Research findings, negotiating text and proposed safeguards.

What the Research Supports

Evidence	Interpretation
Firullo and Colleagues CEPR DP22078 Revised 27 October 2026	789 US Chrome users. An inferred signal matches 90% of later explicit choices and 65% of encounters including non-response. This tests consistency with observed behaviour, not informed EU consent or choices made in an actual browser setting. [6]
Farronato and Colleagues Paper dated 25 October 2026	A field experiment and structural model support substantial time-cost savings from browser-level choice. Treat welfare gains as modelled counterfactuals. They support reusable controls, but do not establish GDPR validity or predict the effects of a particular Article 88b design. [6]
Apple ATT Decision 25-D-02	The French authority challenges the design and implementation, including disproportionate burdens on smaller publishers. The decision is under appeal. Use it as an implementation warning, not proof that every centralised privacy control harms competition. [7]

Negotiating Text and Proposed Changes

Council Article 5(3) The mandate retains a single device-access trigger regardless of data status. Points (c)–(f) cover distinct measurement and security functions with conditions. The contextual advertising limb separates ad selection from measurement data, which it requires to be pseudonymised after collection. It also addresses subsequent processing strictly necessary for the same qualifying purpose. That proposed rule does not authorise unrelated reuse. [2]

My Proposed Extensions Constrained first-party functions, service and transaction fraud prevention, a six-month refusal floor, interoperable receipts and neutral choice tools extend beyond the Council text. First-party status alone supplies no exemption. Retain a later evidence-based review of whether a directly applicable instrument or GDPR consolidation should replace the fragmented Directive. [1]

EDPB Position Joint Opinion 2/2026 supports both a bounded contextual advertising exception and automated signals. The final Article 6(1)(f) guidelines, adopted on 10 November, reject treating legitimate interests as a last resort, while retaining necessity, balancing and independent ePrivacy requirements. [5, 13]

Institutional Outcome Seek joint implementation guidance and a published review timetable. The proposed duty to cooperate requires consultation and reasons, without giving another regulator a veto. The Innovation Mandate governs choices within the law; it supplies no defence to unlawful processing. [1, 11]

Sources

Primary legal texts and research checked on 17 November 2026. Numbered references support the answers and notes; policy recommendations remain expressly identified as proposals.

1 Present Position Leiser, Restoring Legal Certainty in EU Data Protection Law, August 2026, especially sections 8.7–8.9. Report

2 Council Mandate ST 14756/26, agreed 21 October and circulated 22 October 2026. Deleted Articles 88a–88b, pp. 143–145; Article 88 bis, pp. 145–146; revised ePrivacy Article 5(3), pp. 156–158. Mandate

3 Commission Proposal COM(2025) 837 final, 19 November 2025. Proposed Articles 88a(4)(c) and 88b: six-month refusal floor, machine-readable choices, media exception and standardisation. Proposal

4 Status and Current Law Procedure 2025/0360(COD), pending committee decision. GDPR Articles 4(11), 5, 6, 7, 9 and 21; ePrivacy Directive Article 5(3). Procedure · GDPR · ePrivacy

5 Joint Supervisory Opinion EDPB–EDPS Joint Opinion 2/2026, adopted 10 February 2026, paragraphs 104, 106 and 108–117: bounded contextual advertising, non-identifying refusal flags and automated choices. Opinion

6 Current Empirical Research Firullo, Decarolis, Cheyre and Acquisti, Consent and Choice, CEPR DP22078, revised 27 October 2026; authors' Bocconi account, 2 November. Farronato, Fradkin and Lin, Designing Consent, paper dated 25 October 2026. US Chrome samples limit direct extrapolation. CEPR · Bocconi · Current Paper

7 Apple ATT Autorité de la concurrence, Decision 25-D-02, 31 March 2025. Official decision summary records the appeal. Decision

8 EDAA Controls YourOnlineChoices, Your Ad Choices: company-specific controls and explanations of what an advertising preference changes. Portal

9 Commercial Interests CJEU, KNLTB, C-621/22, EU:C:2024:858, paragraphs 37–56. Commercial interests can qualify; necessity and balancing remain obligatory. Judgment

10 Consent Validity EDPB Guidelines 05/2020, version 1.1, sections 3 and 5. Specificity, information, affirmative action, demonstration and withdrawal. Guidelines

11 Helsinki EDPB Helsinki Statement, agreed 1–2 July and published 3 July 2025: practical compliance, consistency and cross-regulatory cooperation. Statement

12 AI Models EDPB Opinion 28/2024, adopted 17 December 2024, section 3.3. Read alongside the Council's proposed Article 88 bis; Article 9 remains independent. Opinion

13 Latest Legitimate Interests Guidance EDPB Guidelines 1/2024, version 2.0, adopted 10 November 2026; executive summary and sections 2 and 4.4. This supersedes the 2024 consultation draft. Final Guidelines