The Trouble With noyb's Cookie Banner Campaign

Automated Privacy Signals Deserve Support, but Europe Needs to Reform the Law Behind the Banners

Dr M.R. Leiser (Mark)
DigiData Consulting Ltd · 12 September 2026

As the author of Dark Patterns, Deceptive Design, and the Law, I welcome efforts to end manipulative consent requests and give people usable privacy controls. Yet noyb's promotion of the Kill the Cookie campaign overstates what automated signals can resolve and dismisses the public benefits of broader reform.

A credible Digital Omnibus must address when consent should be necessary, how software communicates an informed choice, and who controls that software. It must also recognise that clearer rules supporting research, innovation and useful data processing can benefit the very people whose rights the campaign seeks to defend.

noyb's promotion of the "Kill the cookie banner" campaign invites readers to judge the Digital Omnibus through a remarkably narrow account of the public interest. Automated privacy signals apparently constitute the only simplification that benefits people; opposition comes from the "tracking industry", and support for Article 88b becomes a test of Europe's commitment to its values.

This is effective campaigning, but it leaves little room for the possibility that someone might want to abolish manipulative cookie banners while questioning the proposed solution. It also dismisses the benefits that clearer, more workable data protection rules could deliver to the same people the campaign claims to represent.

My work on deceptive design supports reform of the rules governing cookies and similar technologies. I have spent considerable time examining how businesses manipulate consent, and my Omnibus report expressly supports reusable privacy preferences alongside reform of the circumstances in which consent is necessary.

My criticism comes from that commitment: I regard the campaign's approach as ill-informed because its confidence in automated signals outpaces its analysis of the law and the systems through which people would exercise their choices. Moving a decision into a browser still leaves someone designing the options, selecting the defaults and determining which requests the user encounters. Meanwhile, automating consent requests leaves unanswered whether the law should require those requests in the first place.

A credible reform must address both questions.

I support legally binding privacy signals that allow people to communicate their choices without enduring repeated, manipulative requests. My Omnibus report expressly advocates reusable preferences alongside substantive reform of the consent rules. The weakness in noyb's post and the coalition letter lies in their confidence that signalling technology resolves the difficult questions surrounding consent.

By describing Article 88b as the only simplification that benefits people, while dismissing most of the remaining package as reducing protection, the coalition substitutes a political judgement for an assessment of what those reforms could achieve.

People benefit from legal certainty as patients, researchers, workers, entrepreneurs and users of new technologies. Clearer rules on contextual identifiability can support investment in privacy technologies; workable access to data can improve the conditions for European AI development; harmonised research provisions can remove obstacles to useful collaboration. Each proposal requires scrutiny, but a measure does not cease to serve the public because it also reduces costs for organisations.

The letter offers no analysis to sustain its sweeping dismissal. It effectively treats the existing regulatory burden as evidence of protection, although my report explains how uncertainty can discourage safer design and favour organisations that can afford prolonged disputes.

The underlying consent problem also extends beyond deceptive banners. Article 5(3) of the ePrivacy Directive regulates storage of, and access to, information on devices, whether or not that information constitutes personal data. Its exceptions therefore determine which technical operations require permission in the first place. Automating the answer leaves that underlying boundary untouched.

Sections 6.5 and 8.7 of my report propose carefully defined exemptions for activities such as fraud prevention, constrained audience measurement and advertising functions that avoid tracking people across services. Those exemptions would carry restrictions on retention, combination and reuse, while consent would remain necessary for tracking and behavioural profiling across services. Reducing unnecessary demands for permission should form part of the solution.

The letter does acknowledge that affirmative consent must identify controllers and purposes. That concession deserves more attention than the promise that users can settle their preferences upfront. A person can refuse tracking by unfamiliar organisations without studying every organisation's plans; affirmative authorisation requires sufficient information about the proposed processing.

The published ADPC draft cited by the coalition reflects precisely that distinction: it requires informed affirmative decisions, permits their repetition for the same requests, and expressly excludes a universal affirmative consent command. The ADPC specification (Sections 6.1–6.3) can therefore support valid consent, but its existence does not establish that a general preference can authorise future processing by unknown controllers.

The campaign's FAQ makes the difficulty clearer by suggesting that agents might act on lessons from earlier decisions or external consent lists. Neither prediction nor a list can, by itself, supply the user's informed authorisation (Campaign FAQ, question 6).

Although the annex refers to legally valid signals, it groups refusal, withdrawal and objection together when describing signals that should prevent processing. Those actions have different legal consequences. Article 21(5) GDPR already recognises automated objections, so the law does not start from a complete vacuum.

An objection to direct marketing requires cessation for that purpose; an ordinary Article 21(1) objection concerns the person's particular situation and allows continuation where the controller establishes compelling overriding grounds or the specified justification concerning legal claims. Withdrawal ends reliance on the consent concerned for future processing. Legislators must preserve those distinctions or expressly amend them.

The letter's assurance that the system would leave rights and general duties unchanged cannot resolve ambiguous instructions about which processing a signal prohibits (GDPR, Articles 7 and 21).

California provides a useful but narrower precedent. The cited California AB 566 requires browsers to offer a configurable signal concerning the sale and sharing of personal information, with that browser functionality duty commencing on 1 January 2027. It does not impose the equivalent duty on operating systems or establish a mechanism for obtaining informed consent under EU law.

California demonstrates that legislators can mandate signalling infrastructure; the European proposal still needs its own account of scope, legal effect and responsibility.

My work on deceptive design also makes me sceptical that relocating the interface is sufficient protection against manipulation. Browser controls have defaults, wording, prominence and timing, just as website controls do. Software that selects which requests users see can influence their decisions before they encounter the service seeking consent.

The Annex rightly recognises the danger of entrenched browser power, but legislators must translate that concern into enforceable requirements for independent agents, portable preferences, intelligible controls and scrutiny of preferential treatment. A fall in tracking following an informed refusal would reflect user choice; a browser steering choices to favour its own commercial interests would present a different problem. Both deserve explicit treatment.

The annex's contrast between a trusted local newspaper and an international platform illustrates why we must distinguish personal preference from regulatory classification. Users may favour whichever publisher they trust. The law, however, should assess purposes, data flows, retention and safeguards when determining whether processing warrants an exemption. A newspaper can integrate extensive tracking, while a large platform can undertake a tightly constrained operation.

My report therefore proposes usable exemptions for publishers under the same substantive conditions that apply elsewhere, while rejecting a categorical entitlement to disregard reusable preferences. That approach addresses funding and privacy together without making corporate identity a substitute for examining the processing.

The coalition correctly argues that legislation should determine legal effects and technical standards should implement them. Following that principle requires a much fuller settlement than a mandate to transmit signals. My report calls for cooperation among data protection, consumer, competition, communications, and cybersecurity authorities, supported by evidence on user comprehension, market effects, and feasible alternatives.

Civil society participation belongs in that process alongside the expertise needed to make the system work.

Europe should combine reliable control over intrusive tracking with reliable conditions for useful, appropriately safeguarded processing. Counting disappearing banners will tell us very little about whether the Omnibus has achieved either objective.

First published on DigiData on 12 September 2026.