

Privacy, plurality, prosperity: designing a workable Digital Omnibus



05



05

Cover image credits: Shutterstock | Jack_the_sparow

Co-organised with



Introduction

At a critical moment for Europe's digital policy agenda, policymakers, civil society representatives, consumer advocates, publishers and technology stakeholders convened for a dinner-debate hosted by Friends of Europe and co-organised with Google. The discussion focused on the European Commission's Digital Omnibus, with particular attention to proposals and concerns raised around cookie consent mechanisms, browser-level consent, data protection, ad-supported online services and the sustainability of Europe's digital ecosystem.

Held under Chatham House Rules, the exchange encouraged candid reflection on how Europe can maintain high standards of privacy while supporting innovation, competition, media plurality and open access to information. Several interventions suggested that the current consent experience is difficult for many users to navigate, while others cautioned that simplified approaches should be carefully assessed for their potential impact on citizens, small businesses, publishers and the wider digital economy.

The debate was anchored by new citizen survey findings from Debating Europe, Friends of Europe's citizen engagement unit, which explored public expectations around free online services, advertising, paid access, cookies and data control across France, Germany, Ireland, Italy and Poland.

Key recommendations

- **Simplify consent without weakening protection**, ensuring reforms make choices clearer for users while preserving meaningful control over personal data.
- **Assess approaches to centralised browser settings carefully**, particularly where concerns were raised that they could create new gatekeepers or undermine direct relationships between users and selected services.
- **Clarify when consent is genuinely necessary**, distinguishing between data-use practices that require active consent and lower-risk uses such as security, fraud prevention, analytics or functional services.
- **Consider legitimate interest where appropriate**, backed by transparency, clear safeguards, easy opt-outs and strong accountability for organisations using data.
- **Take account of Europe's media plurality and open web**, recognising that many publishers and online services rely on advertising revenues to remain accessible.
- **Improve legal certainty and harmonisation across the Digital Single Market**, reducing fragmentation in interpretation, enforcement and compliance obligations.
- **Invest in digital literacy and user empowerment**, ensuring citizens can understand choices and risks rather than being overwhelmed by repetitive interfaces.

- **Develop standards collaboratively**, involving regulators, consumer groups, publishers, SMEs, civil society and technology providers in co-designing workable policy solutions.

Opening reflections: privacy, competitiveness and the open web

The discussion opened with recognition that Europe's digital policy debate is often framed as a choice between privacy and competitiveness. Participants challenged this binary, arguing that strong data protection and a sustainable digital economy should be mutually reinforcing rather than competing objectives.

The Digital Omnibus was presented as part of a broader legislative moment for Europe, with institutions examining how to simplify the regulatory environment while preserving core rights. Cookie banners and cookie consent mechanisms were discussed as seemingly technical issues with wider implications: they affect how citizens experience the internet, how businesses comply with the law, how publishers finance quality content and how Europe maintains a diverse information environment.

A central question guided the discussion: how can Europe uphold high privacy standards while enabling a competitive, innovative and pluralistic digital ecosystem? Several contributions stressed that any answer should consider not only large platforms, but also for SMEs, publishers, content creators and the many businesses that depend on ad-supported access to online services and content.

The discussion also underlined the importance of Europe's regulatory legacy. The General Data Protection Regulation (GDPR) was widely recognised as a global benchmark. At the same time, some participants noted that implementing Europe's digital rulebook has become increasingly complex, with overlapping obligations, divergent interpretations and uneven enforcement contributing to uncertainty for some organisations and citizens.

Citizens' expectations: free access, privacy and consent fatigue

Debating Europe's survey provided a citizen-centred starting point for the discussion. Respondents showed a clear preference for maintaining access to free online content, particularly when supported by non-personalised advertising. A slight majority expressed a preference for free content funded by non-personalised ads, while fewer respondents favoured advertising that uses some personal data or paid access without ads or data use.

Awareness of the link between cookies and free access was mixed. Some respondents understood that advertising and cookies can support free services, while others had

only a vague understanding or were not aware of the connection. This highlighted a broader challenge: citizens are increasingly asked to make frequent privacy decisions in an environment where many do not fully understand the trade-offs.

The survey also suggested limited willingness to pay for online content if rejecting cookies led to more paywalls. Many respondents indicated they would seek free alternatives rather than subscribe, while only a minority said they would be willing to pay for most websites. Affordability emerged as a recurring concern, with many respondents believing that paying for multiple subscriptions would not be realistic for most people.

Cookie consent banners themselves were viewed with ambivalence. Some respondents considered them helpful, but many described them as frustrating, disruptive or something they simply ignored. Reported behaviour reflected this: a substantial share said they accept everything quickly, while others adjust settings or reject non-essential cookies. Participants noted that these behaviours do not necessarily indicate meaningful consent in all cases, as they may also reflect consent fatigue, time pressure or limited understanding of available choices.

The findings also showed openness to contextual advertising, where ads are based on the content being viewed rather than on broader tracking. However, views remained divided on browser-level consent and centralised browser settings. While reducing the number of consent banners was viewed positively by many respondents, others emphasised the importance of retaining flexibility and context-specific choices, particularly for websites and services they value.

The consumer perspective: reducing friction while preserving user control

A recurring theme of the discussion was that simplification should be understood as a tool, not an end in itself. Some interventions framed the goal as a more competitive Europe supported by empowered consumers, rather than simply fewer rules or fewer prompts.

From a consumer perspective, one contribution argued that the current cookie consent experience does not always deliver meaningful user control in practice. The example was given of users repeatedly clicking “accept all” merely to access a service quickly. In that view, consent prompts can become unnecessary friction rather than meaningful user control.

At the same time, other comments cautioned against approaches that remove meaningful choice altogether. A single blanket consent decision was described as potentially too blunt, particularly because users may trust some services more than others. They may be comfortable sharing data with certain websites or providers while rejecting similar practices elsewhere. According to this perspective, a more

effective system should allow consumers to express preferences in ways that are simple, contextual and reversible.

Several ideas were put forward during the discussion. One was to make legitimate interest a more usable basis for certain forms of content or service personalisation, provided that transparency requirements, clear opt-out mechanisms and safeguards against misuse are maintained. Another was to exempt some analytical or functional cookies from repeated consent requirements where they pose limited privacy risk and are necessary for services to operate, improve or remain secure.

The broader message was that Europe should reduce unnecessary friction while preserving genuine empowerment. Effective consumer protection requires not only safeguards, but also innovation, trustworthy services and usable digital experiences.

Industry and European tech: simplification as a route to competitiveness

Technology stakeholders broadly welcomed the ambition to simplify Europe's digital rules, while also arguing that simplification must be grounded in practical realities. One participant described Europe's regulatory environment as a "jungle" of overlapping obligations, multiple regulators and divergent interpretations. For companies operating across the EU, such fragmentation can require adaptation to different interpretations in different member states, limiting scale and slowing innovation.

The discussion highlighted several areas where the Digital Omnibus could improve legal certainty. These included clarification of personal and non-personal data, clearer rules for AI training, and a single entry point for data breach notifications. Participants also discussed practical areas where simplification could improve legal certainty, including possible refinements to Article 13 information requirements in certain contexts and the development of more harmonised approaches to pseudonymisation. These were presented as examples of measures that some participants believed could reduce administrative burdens while maintaining strong data protection safeguards.

However, concerns were raised about browser-level consent or centralised browser settings. Some participants argued that centralising consent could do so in a way that risks disintermediating the direct relationship between local publishers and their audiences, while also reducing the flexibility of user choice in favour of a rigid, binary system. Rather than relying solely on rigid browser settings, several participants highlighted the potential of flexible, user-centric tools such as 'consent assistants' or 'consent profiles' – frameworks already being explored under German law – to help users manage preferences across sites without creating market consolidation.

Several comments also pointed to privacy-enhancing technologies as a possible area for European leadership. These tools could enable companies to use data in ways that protect privacy by design. A clearer European framework for such technologies could allow European businesses to compete on trust and innovation, rather than relying solely on compliance services provided by larger global platforms.

Consent, legitimate interest and the search for a better model

Several participants argued that the problem is not consent itself, but the way cookie banners have been designed and deployed. Interfaces that nudge users toward acceptance, overwhelm them with vendor lists or ask them to repeat choices every few days do not necessarily reflect real control.

Other comments suggested that consent fatigue shows the current system requires further attention. One view was that the widespread presence of consent banners shows that regulation has succeeded in making data practices visible, but that the next step must be to make consent more usable, durable and meaningful.

Potential alternatives included consent profiles, consent assistants or automated preference tools that would allow users to set choices once and apply them across services. Such tools could, in principle, let users express values-based preferences: for example, allowing certain data-use practices by selected services, declining others, or supporting services they value. It was also stressed that any such model would need clear legal and technical standards, interoperability and safeguards against concentration of power.

Legitimate interest was also discussed as an underused part of the GDPR framework. Some interventions argued that the GDPR does not create a hierarchy in which consent is always superior. In certain cases, legitimate interest serves as a robust, high-accountability alternative for lower-risk processing, such as essential analytics, security and basic service improvement. Far from bypassing protection, this framework places the entire burden of proof and strict balancing tests on the controller, while ensuring users are protected by clear transparency and easily accessible opt-out options.

Some participants considered this approach particularly relevant for activities such as security, fraud prevention, frequency capping, analytics and certain forms of service improvement.

Civil society voices cautioned that moving too much data processing away from consent could weaken user control, especially where data-use practices are opaque. The challenge, therefore, is to distinguish between practices requiring active consent and those that can be managed through accountability, transparency and enforceable safeguards.

Publishers and media plurality: the economic stakes of consent reform

Publisher representatives warned that changes to consent rules could have significant consequences for Europe's media landscape. Ad-supported content remains central to the accessibility of news and information, particularly as print revenues decline and willingness to pay for digital content remains limited.

Several comments stressed that data is not used only for advertising. Publishers also rely on data to improve user experience, develop products, understand audiences and compete for attention in a crowded digital environment. Without workable approaches to cookie consent and data use, publisher representatives argued, they may struggle to attract readers, monetise content and sustain investment in quality journalism.

The discussion also challenged the tendency to treat all advertising practices as equivalent. It was argued that there is a wide spectrum of data use, from broader forms of cross-site data use involving multiple vendors to more limited, in-house approaches that keep data within a publisher's own environment. A more nuanced legal framework could incentivise lower-risk, privacy-conscious business models rather than treating them in the same way as more invasive practices.

The potential expansion of paywalls was a recurring concern. Participants warned that if consent reforms reduce advertising revenues without providing viable alternatives, more services may move towards subscription models. This could restrict access to information, particularly for lower-income users, and potentially affect the diversity of Europe's public sphere.

The Digital Single Market and regulatory fragmentation

The debate around cookie consent mechanisms was repeatedly linked to the broader challenge of Europe's Digital Single Market. While the EU has adopted major digital legislation, companies continue to face fragmented interpretation, implementation and enforcement across member states.

This fragmentation creates compliance costs and legal uncertainty, particularly for SMEs and scale-ups. Several interventions called for clearer rules, more consistent guidance and better coordination among regulators. As single rulebook should not result in 27 different practical interpretations.

The question of enforcement was also raised. E-privacy rules are enforced differently across member states, sometimes by data protection authorities and sometimes by telecom regulators, with different powers and procedures. Bringing parts of the framework closer to the GDPR could improve coherence, but some comments warned that such changes must be carefully designed to avoid new confusion.

From a policy perspective, the Digital Omnibus was presented as an attempt to clarify, simplify and provide legal certainty. Proposed clarifications on personal data, scientific research, AI training, data subject rights, data breach reporting and data protection impact assessments were described as efforts to reduce fragmentation and support more consistent interpretation. Participants nevertheless stressed that legal certainty should be pursued through dialogue and impact assessment, rather than rushed compromises.

Security, resilience and democratic safeguards

The debate also moved beyond privacy and advertising to consider security and resilience. Several participants noted that Europe's digital framework operates in a geopolitical environment marked by cyber threats, foreign interference, disinformation and growing dependence on digital infrastructure.

Simplification should be considered alongside broader policy objectives. Parliamentary and member state representatives emphasised that efforts to streamline data rules should continue to support cybersecurity, fraud prevention, democratic resilience and the protection of citizens, while providing greater legal certainty for organisations. The influence of digital platforms and data-driven systems on elections and public debate was cited as a reminder that digital policy is inseparable from democratic security.

Participants also highlighted the growing sophistication of AI-enabled threats and automated attacks. As digital systems become more complex, policy must account for cybersecurity, fraud prevention and the operational realities of defending infrastructure. Consent models should not make essential security practices harder to implement.

Towards co-produced digital policy

A recurring message from participants was that effective digital policy should not be designed in isolation. Many called for a more collaborative approach involving policymakers, industry, consumer groups, civil society, publishers, SMEs and technical experts.

While several participants welcomed consultation efforts, some expressed concern that the pace of the Omnibus process could limit meaningful engagement. Given the potential impact of changes to consent, privacy and data governance, some interventions urged policymakers to take the time needed to understand practical consequences and explore alternatives.

Co-production was presented not as a means of diluting regulation, but as a way of improving its effectiveness. Digital policy affects complex ecosystems, and small changes can create significant economic, social and technical consequences. Better

policy requires understanding how rules operate in practice, how users behave, how businesses comply and how safeguards can be enforced.

The discussion therefore ended with a call for pragmatic experimentation, clearer standards and continued dialogue. While participants differed on the best approach, there was broad agreement on the need to improve the current system. The debate centred less on the general ambition of simplification than on how it should be achieved: namely, how consent can be simplified in a way that supports privacy, preserves user choice, sustains open access and contributes to Europe's competitiveness.

Conclusion and call to action

The dinner concluded with a broad recognition that Europe should avoid framing privacy and prosperity as competing objectives. Citizens deserve meaningful control over their data, but they also need accessible digital services, reliable information, innovation and security. Businesses need legal certainty and workable rules, but they must also earn and maintain public trust.

The Digital Omnibus offers an opportunity to address challenges identified in the current system, particularly around cookie banners, fragmented interpretation and regulatory complexity. Yet several interventions warned that reforms should be carefully calibrated. Browser-level consent or centralised browser settings may appear simple, but concerns were raised that such approaches could create new gatekeepers, reduce context-specific choice and have wider implications for ad-supported online content.

A key challenge identified during the discussion was designing a digital governance framework that is user-centric, enforceable and innovation-friendly. Achieving this will require clearer distinctions between types of data use, stronger accountability where consent is not the right tool, better digital literacy and standards developed with those who must implement them.

Ultimately, participants suggested that combining high privacy standards with practical, competitive and pluralistic digital policy was crucial to strengthening citizens' rights while preserving an open, innovative and sustainable digital ecosystem.



Friends of Europe

Connect. Debate. Change.

info@friendsofeurope.org
friendsofeurope.org

Friends of Europe is a leading think tank that connects people, stimulates debate and triggers change to create a more inclusive, sustainable and forward-looking Europe.

