Dear Member of The European Parliament,

A nuisance is troubling the internet and the digital life of Europeans: the consent or 'cookie' banner. Under the pretext of providing transparency and control, these banners are used to subvert user intent and coerce the handover of personal data. As the ePrivacy trilogue begins, we urge legislators to enable the necessary technological supports to effectively protect the rights provided by the GDPR and the EU Charter.

In the three years since GDPR has come into force, the promise to protect users from undesired processing has not been fulfilled.

Numerous studies show how a large majority of individuals, if given a fair choice, would reject cookies or tracking.[1] However, consent is being exploited, and deceptive interfaces nudge users to accept and

1 A 2019 RSA survey showed that 68 % of respondents regarded "tracking online activity to tailor advertisements" to be unethical, while only 29 % agreed that providing more data leads to better products and services. See: https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf
On a similar note, a 2019 study shows that "Once an explanation of adtech is shown, there is a notable shift in perceptions towards websites showing adverts as being unacceptable", and "All the information points typically used [for data driven adverts] are frequently deemed unacceptable". See: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/141683/ico-adtech-research.pdf
Finally, a recent poll conducted by YouGov found that up to 83% of German and French are feeling unease about sharing their data for targeted advertising. See: https://www.globalwitness.org/en/blog/do-people-really-want-personalised-ads-online/

surrender their privacy.[2] To refuse they must navigate a maze of dialogues, endless checkboxes, and redirects to off-site 'opt-outs' etc. without knowing if they may be locked out of the site as a result. And they must do this on every site individually.

Users have been asked to become full-time managers of their own privacy within an environment of manipulation and opacity, where consent cannot be 'informed' or 'freely given'. The result is that the rights granted to citizens by the law are not vindicated in practice.

A solution is at hand.

Article 21(5) of the GDPR already envisaged that users could exercise their right to object to processing by using automated signals. But this provision was never implemented, and a process to designate a signal was not included in the GDPR.

The ePrivacy Regulation is a chance to remedy this omission, extend the use of automated signals to the management of consent, and provide a working alternative to cookie banners. Legally binding privacy controls would allow users to communicate their preferences automatically and persistently to the sites they visit. Users should be able to tailor their choices for different websites, but via an interface under their control, and at a time of their choice. Publishers are free to try and persuade visitors to whitelist their site, but without forcing them with cookie walls or equivalent means.

Finally, and in contrast with industry proposals, this system would guarantee reliable communication without requiring users to identify themselves and participate in a register.[3] Users should be given technical means to assert their choices, rather than protections that can be respected or revoked by policy.

Automated privacy signals must be enforced against websites and platforms alike

It should be unnecessary to say so, but the law should apply equally to all, but this has not been the reality of the GDPR. Facebook and Instagram force their users to consent to behavioural tracking, while Google deceives them with carefully designed interfaces. Privacy signals must be binding also on the platforms Europeans use every day. So much of our digital life unfolds in these spaces that the privacy risks are higher: the videos we watch, pictures we like, items we purchase, and terms we search. The Cambridge Analytica affair illustrates the threat posed by the depth and breadth of this capacity to observe and profile.

---

2 The California Consumer Privacy Act Sec. 1798.140.(l) defines dark patterns as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice..."

3 This is the case with 'AdChoices' scheme which relies on a third party cookie to opt the user out of behavioural ads. It is also a feature of various industry proposals to replace third-party cookies with alternative identifiers such as SWAN and User ID 2.0.

These platforms usually require a log-in for functional reasons connected to their service. But this ability to identify users, and to profile them based on their activity, on and off the site, is being used to gain an unfair advantage in the advertising market. Empowering users to say no to their profiling practices will help return a level playing field to this sector. The competition issues which the Digital Markets Act seeks to address can in part be dealt with by empowering users through effective privacy controls.

In 2019, California state law created the first legal obligation to comply with automated opt-out signals.[4]

In US, the California Attorney General has already indicated that activation of the Global Privacy Control, a consumer-friendly opt-out signal supported by several browsers and extensions, is legally binding and will be enforceable under the CCPA[5]. Furthermore, starting in July a new California Privacy Protection Agency will be responsible for further clarification and enforcement of a signal for users to opt-out of the sale of their data to third parties.

The European Union needs to catch up, and build on these examples to include the broader protections provided under EU Law.

The EU data protection framework will require a more complex signal, capable of accommodating the respective needs of users and data controllers. We call on all parties to the ePrivacy trilogue to assign the European Data Protection Board the task of defining the requirements and technical specifications for signals to communicate and withdraw consent, and to object to processing based on legitimate interest.[6] The scope of these signals should encompass:

4 The 2020 California Privacy Rights Act amended and extended this opt-out right to the 'sharing' of data where there is no sale, and created an additional right to to direct business to 'limit the Use and Disclosure of Sensitive Personal Information' (1798.121). These amendments enter into force on January 1 2023.

5 https://twitter.com/globalprivctrl/status/1390756809611255808

6 Much of this was addressed by the EU Parliament in its position in October 2017. Article 10(1a) made signals legally binding for Article 8 ePrivacy and Article 21(2) GDPR purposes. However, experience since the entry into force of the GDPR in 2018 underlines the need for such specifications to encompass also the grant and withdrawal of consent. Article 19 of the Parliament's draft allocated the technical rule-making procedure to the EDPB.

- Article 8 of the ePrivacy Regulation (consent to terminal access)[7]
- Article 21(1) and (2) GDPR (objection to legitimate interest processing)
- Article 6(1)(a) and 7(3) GDPR (the grant and withdrawal of consent)

This is an opportunity for European Institutions to back a solution that is in line with their values, promote convergence among different legal frameworks, and reinforce their role as global standard-setters for data protection.

Yours sincerely,

- AccountableTech
- Amnesty International
- Bits of Freedom
- Center for Informatics and Society
- Coalizione Italiana Libertà e Diritti civili (CILD)
- Civil Rights Defenders (CRD)
- Civil Liberties Union For Europe
- Deutsche Vereinigung für Datenschutz e.V
- Electronic Frontier, Norway
- Electronic Frontier Foundation (EFF)
- European Digital Rights (EDRi)
- Ranking Digital Rights
- Fitug e.V.
- Free Knowledge Advocacy Group EU
- Global Witness
- Gong
- Homo Digitalis
- Human Rights Monitoring Institute (HRMI)
- Internet Society France
- IT-Pol
- MyData Austria
- Nederlands Juristen Comité voor de Mensenrechten (NJCM)
- New Economics Foundation
- NOYB – European Center for Digital Rights
- Open Rights Group (ORG)
- Platform Bescherming Burgerrechten
- Panoptykon Foundation
- Privacy First
- Ranking Digital Rights
- Sustainable Computing Lab, University of Wien
- The Irish Council for Civil Liberties
- The Peace Institute
- Vrijschrift
- Wikimedia France

7 Article 8 of the Commission's proposal set out the legal framework for the use the user's device ('terminal equipment') to set identifiers such as cookies. Where consent was required (as is the case for advertising purposes), its nature was covered in Article 9. The Council deals with these issues in Articles 8 and 4a.