in24 April 2024, Brussels

For the attention of European Commissioner for Internal Market, Thierry Breton, Vice-President of the European Commission, Věra Jourová, and European Commissioner for Home Affairs, Ylva Johansson

CC/ Cabinet of European Commissioner for Justice

Re: Underscoring the Importance of Protecting Fundamental Rights When Modernising ePrivacy Legislation

In January 2017, the European Commission proposed an update to the 2002 ePrivacy Directive aimed at establishing new rules governing confidentiality of electronic communications and the use of cookies and other online tracking technologies. Seven years later, EU member states and corporations (namely advertising companies, publishers and telecom operators) have successfully blocked this critical reform, despite the desires of civil society and individuals who openly advocate for enhanced privacy and security in online communications. However, pervasive harms persist within the digital sector, as underscored in the Council Conclusions on the Future of EU Digital Policy. We, the undersigned organisations, continue to **assert the necessity for robust legislation, now more urgently than ever, to complement and particularise the General Data Protection Regulation (GDPR), and call upon the next European Commission to include comprehensive plans for reforming the EU's ePrivacy legislation**.

In recent years, we have observed concerning debates about some aspects covered by the ePrivacy Directive within related legislation such as the Digital Services Act (DSA) and Member States' political pressure to maintain their national data retention laws. The current regulations prove inadequate in addressing the well-proven harms stemming from commercial and state surveillance technologies. As we expressed in the past, certain Member States seem inclined to prioritise the narrow business interests of a few major tech companies and the national security blanket exception, which risks allowing state interference and abuses, over the fundamental rights of individuals. Additionally, we are troubled by the promotion of alternatives that fail to fully protect fundamental rights, such as voluntary business pledges, or the growing acceptance of the 'pay or okay' paradigm, which signals the erosion of genuine and free choice, and the emergence of a period where privacy may be commodified. Last but not least, spyware and other state surveillance-related recurrent scandals serve as reminders that deploying spyware violates the right to protect terminal equipment as outlined in the ePrivacy Directive. This prohibition should persist within any future legal framework.

The ramifications of maintaining our online privacy standards at the level of 2002 are alarmingly evident in the recent proposition to prolong the supposedly temporary exemption from specific sections of the 2002 ePrivacy Directive. This extension is primarily targeted at facilitating the detection of online child sexual abuse material by communication companies. However, this approach entails mass surveillance, as it permits them to engage in the automated scanning of individuals' private communications continuously. Furthermore, it lacks a solid legal foundation and has been chosen over less intrusive alternatives that could potentially restrict surveillance to legitimate suspects, aligning with the principles of due process and the necessity and proportionality standards consistently emphasised by the European Court of Justice.

If the EU aims to enhance fundamental freedoms and ensure a functional Digital Single Market, updating the ePrivacy Directive is imperative. The privacy standards for confidentiality of

communications and protection against online tracking in the 2002 ePrivacy Directive must be maintained while they are modernised to reflect technological developments since 2002. It is imperative that the protection of personal data afforded by the GDPR is not undermined by predominant commercial interests in tracking-based advertising and other data-driven business models, or state-led interventions relying on the massive collection of personal data. We acknowledge that this can be achieved through various means and legislative avenues. Therefore, we urge the European Commission to include plans to ensure the protection of the following issues in the next mandate:

- Enshrine robust provisions to ensure the effective protection of the privacy and security of communications, including mandatory privacy by design and by default standards in both software and hardware.
- Ban tracking walls that put a price on the enjoyment of fundamental rights.
- Protect encryption (including end-to-end encryption) and the confidentiality of communications.
- Put an end to surveillance advertising in favour of privacy-preserving forms of ad targeting such as contextual targeting.
- Limit the processing of electronic communications data to concrete, strictly defined purposes.
- Institute robust protections against invasive online surveillance and intrusions into terminal equipment.
- Uphold the integrity of the Court of Justice's case law protecting confidentiality of communications against unlawful state and commercial interference.
- Encourage collective actions by civil society groups against infringements of the legislation.

Yours sincerely,

EDRi European Digital Rights
IT-Pol Denmark
Homo Digitalis
Zavod Državljan D
ApTI
Access Now
Privacy International
Politiscope
ARTICLE 19
Digital Rights Ireland
Bits of Freedom
Aspiration
Digitalcourage
Deutsche Vereinigung für Datenschutz e.V.