CIVIL SOCIETY JOINT STATEMENT ON THE USE OF SURVEILLANCE SPYWARE IN THE EU AND BEYOND

We are a coalition of civil society organisations and journalists' organisations committed to the protection of fundamental rights, transparency, and accountability in relation to spyware technologies. Spyware poses a significant threat to EU democratic values, public debate and healthy civic spaces by undermining critical pillars such as independent decision-making among lawmakers and the ability of journalists and activists to hold power accountable. Furthermore, as highlighted by the European Data Protection Supervisor, the level of intrusiveness of modern spyware tools undermines the essence of the fundamental right to privacy and data protection, which makes them illegal under Union law.

The European Parliament Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA Committee) concluded in May 2023 that the majority of EU Member States had purchased spyware tools and that some of them have used spyware to unlawfully and arbitrarily surveil journalists, human rights defenders, and politicians within the EU, as reported by several civil society organisations.

We deeply regret that the EU Institutions have failed to provide effective solutions and a more comprehensive approach to the numerous reports of maladministration and abuse of power by Member States during the last legislative term.

Moreover, the recently adopted European Media Freedom Act (EMFA) sets a troubling precedent. Despite its commendable intentions, the law fails to fully protect journalists from spyware, lacking essential safeguards against their surveillance and creating sweeping legal grounds for its use against them in the EU. Consequently, both spyware victims and EU society as a whole still await an appropriate institutional response to this threat to fundamental rights.

We, the undersigned organisations, believe that the new legislative term provides an opportunity for the incoming EU Institutions to take more decisive action and implement the EU acquis on this matter. The Commission, the Council and the Parliament must urgently take robust measures to curtail the abuse of spyware in the EU and uphold EU values by respecting and protecting fundamental rights, introducing effective accountability mechanisms and delivering remedies to victims of illegal spyware surveillance. Moreover, Member States are responsible for safeguarding the fundamental rights of all individuals under their jurisdiction.

We urge the incoming EU Institutions and EU Member States to adopt the following measures without delay:

EU Commission

- Propose a new EU legal framework that addresses the challenges posed by spyware, which includes an EU-wide ban on the production, export, sale, import, acquisition, transfer, servicing and use of spyware, which disproportionately interfere with fundamental rights and for which no safeguards are adequate to prevent and redress harms to human rights.

- Impose a moratorium in the EU until this new legal framework is put in place.
- Push for the implementation of a complete ban on the development and sale of commercial spyware by private companies.
- Make sure that existing legal framework is adequately implemented by the MS, by conducting a comprehensive and in-depth assessment of Member States' compliance with the ePrivacy and Law Enforcement Directives and with the Dual-Use Regulation and launch infringement procedures against those whose trade and use of spyware breach those instruments.
- Strengthen the export control regime by reviewing and amending the EU Dual-Use Regulation, notably by incorporating spyware into the definition of cyber-surveillance tools and including obligations guaranteeing these goods are not used for repression or human rights violations.
- Utilise the instruments available within the rule of law toolbox to monitor the use of spyware by Member States, including deploying the Rule of Law Framework, incorporating findings into the Annual Rule of Law Report, initiating infringement procedures where necessary and applying the Conditionality Regulation to suspend EU funds in cases where spyware use undermines the rule of law and in case of failing oversight mechanisms.
- Mandate transparency in EU Member States government contracts and operations involving spyware, ensuring accountability for abuses.
- Propose a harmonised legal definition of national security and set guidelines for Member States to determine a genuine and serious threat to national security.
- Enforce a ban on the commercial trade of vulnerabilities for any purpose other than strengthening systems security and mandate the responsible disclosure of vulnerability research findings.
- Ensure that any future legislative proposal potentially replacing the ePrivacy Regulation proposal provides for stronger guarantees to protect the confidentiality of communications, notably by strengthening the right to protection of terminal equipment already afforded by the ePrivacy Directive.

Council of the EU

- Refrain from introducing wide national security exceptions into EU legislation, as such carve-outs create significant gaps in the applicability and enforcement of EU legal instruments and expose citizens to further fundamental rights violations.
- Organise a debate on the use of spyware within the EU in the General Affairs Council and adopt relevant conclusions.

EU Member States

- Suspend all exports out of the EU on the sale and transfer of surveillance technology that have been authorised in breach of international human rights standards.
- Refrain from derogating from their fundamental rights obligations under the EU Charter of Fundamental Rights and the European Convention on Human Rights by claiming national security exemptions.
- Impose sanctions on vendors found to have infringed their due-diligence obligations under EU law.
- Commit to maintaining the higher or absolute level of protection at national level, by not relying on the derogation under Article 4, Paragraph 5, of the EMFA concerning the possibility for Member States to deploy intrusive surveillance software.

- Eliminate all existing obstacles preventing victims of spyware from accessing justice and appropriate remedies and ensure that all police and judicial investigations are dealt with promptly, effectively and transparently.

EU Parliament

- Continue its work investigating, monitoring and proposing recommendations to curtail the abuses of surveillance spyware by Member States and continue calling for the full implementation of the recommendations of the PEGA committee.
- Make use of all resources at its disposal to exercise its scrutiny powers over the EU Commission and Council and to hold them accountable for their inaction, insufficient actions or non-compliance with existing Union acquis.

We emphasise that all the decision-makers concerning the aforementioned recommendations, without exception, should make their decisions only after consulting publicly and transparently with relevant national and international stakeholders, including civil society organisations, human rights groups, and representative bodies of surveillance victims.

We, the undersigned organisations, representing a diverse cross-section of civil society and journalists' organisations, stand united in demanding immediate action to respect and protect the rights of all individuals in the EU from the pervasive threat of spyware.

Members of the Coordination Group

Access Now
ARTICLE 19
Centre for Democracy & Technology Europe (CDT Europe)
Civil Liberties Union for Europe (Liberties)
Data Rights
Electronic Privacy Information Center (EPIC)
Epicenter.works - for digital rights
European Digital Rights (EDRi)
European Federation of Journalists (EFJ)
The Hungarian Civil Liberties Union (HCLU)
Privacy International (PI)
Wikimedia Europe

Additional signatories

Aspiration
Bulgarian Helsinki Committee
Digital Rights Ireland
Data Privacy Brasil
Centre for Peace Studies
Citizen D / Državljan D
Civil Rights Defenders
European Center for Not-for-Profit Law (ECNL)
Fundación Karisma (Colombia)
Homo Digitalis
Italian Coalition for Civil Liberties and Rights (CILD)
IT-Pol Denmark
Ligue des droits humains (Belgium)
Nederlands Juristen Comité voor de Mensenrechten (NJCM)
Panoptykon Foundation
Peace Institute (Slovenia)
Sflc.in (India)
Vrijschrift.org
Xnet, Institute for Democratic Digitalisation (Spain)