Civil Society Open Letter in Response to Recent Spyware Abuse Cases in the EU

On behalf of the Spyware Coordination Group, a coalition of civil society and journalist organisations advocating for transparency, accountability, and the protection of fundamental rights in relation to spyware technologies, we call on European Union (EU) Institutions to take concrete action to respond to the growing threat posed by spyware, to enhance the security and resilience of our digital infrastructure and European cyberspace and address the proliferation of commercial spyware capabilities in the European Internal Market.

Spyware use and development still unchecked in the EU

Earlier this year, media reports revealed that several Italian journalists and human rights activists had been targeted with Graphite—a spyware developed by Paragon Solutions. According to reports, the victims had become aware of the targeting following an official notification of the intrusion by WhatsApp. This led the Italian authorities to launch an official investigation. In its March and June reports, the Citizen Lab confirmed these allegations and provided further evidence that the Graphite spyware may have been acquired and deployed in several Member States, including Italy, Denmark and Cyprus, likely affecting a higher number of victims than the 90 targets officially notified by WhatsApp. Concerningly, the reports also highlight a pattern of targeting human rights groups, government critics, and journalists, underlining the need for coordinated EU action to address these violations and protect fundamental rights in line with international and regional standards.

Several Member States, including Spain, Italy, Cyprus, have reportedly emerged as key hubs for the spyware industry, with a high concentration of vendors operating from these countries. The absence of a regulatory framework at the EU level, combined with the fragmentation of national legislation and varying degrees of regulatory oversight among Member States, has facilitated the establishment of certain jurisdictions as preferred entry points for the spyware industry within the EU Internal Market, as recognised by the European Parliament's Recommendations of 15 June

2023 and the Commission's White Paper on export controls published in 2024. This development raises significant concerns regarding the trade and proliferation of commercial spyware within the EU, as well as its potential human rights implications.

Urgent need of EU action

Given the risk posed by spyware to fundamental rights, including the right to privacy, rule of law, public debate, media freedom and pluralism, and the integrity of civic spaces, we respectfully urge EU Institutions to prioritise immediate policy and regulatory actions to address the challenges of commercial spyware. We are particularly concerned that spyware technologies, which disproportionately interfere with fundamental rights and for which no safeguards are adequate to prevent and redress harms to human rights, are simply too invasive to ever be compliant with International Human Rights Law (IHRL), as underscored by the European Data Protection Supervisor and the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. Hence, European action should include the swift introduction of red lines in order to be aligned with the EU Charter of Fundamental Rights.

The Pall Mall Process should be complemented by action at the EU level

The Pall Mall Process, an "iterative multi-stakeholder initiative" launched in 2024 by France and the UK, claims to tackle the threat posed by the proliferation and "irresponsible use" of commercial cyber capabilities. As part of this process, 25 countries, of which 18 are EU Member States have recently adopted a non-binding Code of practice for States through which signatories have committed to collaborate to "prevent irresponsible activity across the global cyber intrusion market and mitigate the threats presented by the proliferation and irresponsible use of" spyware. A similar declaration of intent was led by the U.S. in their Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware – endorsed by 23 States, including 10 Member States. While these objectives may outline good intentions and provide a voluntary multi-stakeholder forum in which to discuss the issue of spyware, the approach adopted within the Pall Mall process risks legitimising certain surveillance technologies and uses that are inherently incompatible with international human rights law. Although multilateral action to curb the spyware market is necessary, these initiatives are inadequate to fully prevent the proliferation and use of spyware.

Going beyond these initiatives, and echoing the Parliament's recommendations, we urge the EU Institutions to take a coordinated and transparent regulatory action – particularly in areas that fall squarely within the competence of the EU, such as fundamental rights and rule of law, EU single market regulation, export controls and cybersecurity – during this term, ensuring the protection of the rule of law, and fundamental rights enshrined in the EU Charter and European Convention on Human Rights.

The absence of a coordinated EU response is creating critical gaps in relation to the trade of these tools and the management of cybersecurity vulnerabilities that incentivise the proliferation of commercial spyware and their unlawful use by Governments. The EU can provide the necessary political momentum, regulatory coherence, and oversight to turn national pledges made by Member States through the Pall Mall Code of Practice into an effective, union-wide response that upholds democratic values and fundamental rights.

To address these pressing concerns and safeguard fundamental rights, we call for the following immediate actions:

- the publication of the long-overdue Commission communication to clarify the boundaries between EU law, in particular the data protection, privacy and rule of law acquis, and national security.
- the Commission's formal engagement in the Pall Mall process and participation in all international and regional efforts to address the threat posed by commercial spyware.
- the full implementation of the PEGA Committee's recommendations, including those pertaining to areas falling under EU competence such as internal market regulation, cybersecurity vulnerability management, export controls, EU cybersecurity and resilience and ensuring that Member States provide effective remedies for victims.
- continued commitment from the EU Parliament to advance the work of the PEGA Committee within the relevant Committees and leverage all available resources to further policy development in this area.

We stand ready to engage in a constructive dialogue with you and offer our expertise to support the development of policies that will effectively combat spyware use and strengthen the EU digital infrastructure. We are confident that under your leadership, the European Union can take

decisive action to respect and protect fundamental rights, uphold the rule of law, and address the challenges posed by the use of spyware technologies.

Yours sincerely,

Access Now

Amnesty International

ARTICLE 19

Centre for Democracy and Technology Europe

Civil Liberties Union for Europe (Liberties)

Committee to Protect Journalists (CPJ)

Electronic Privacy Information Center (EPIC)

Epicenter.works - for digital rights

European Digital Rights (EDRi)

European Federation of Journalists (EFJ)

European Centre for Press and Media Freedom (ECPMF)

Osservatorio Balcani Caucaso Transeuropa (OBCT)

Privacy International