BRIEFING ON RECOMMENDATIONS TO THE EUROPEAN UNION TO END UNLAWFUL TARGETED SURVEILLANCE

The Pegasus Project revealed how spyware sold by the cybersurveillance company NSO Group to state clients has been used to target activists, journalists, lawyers, and politicians. It has exposed the devastating impact that the poorly regulated cybersurveillance industry has had on the rights and well-being of individuals unlawfully targeted, as well as their friends, families, and colleagues, but also the extremely destabilizing consequences it has on global human rights and the security of the digital environment at large. In particular, the findings reveal that individuals' rights to privacy and freedom of expression have been egregiously violated. It is also important to recognise that the unchecked use of surveillance technologies is shrinking the space for human rights work, and rapidly exacerbating digital threats against human rights defenders that are spilling over to the offline world.

This has led the UN High Commissioner for human rights, as well as several UN experts to call for urgent action to combat the issue of unlawful targeted surveillance, including calling for a moratorium on the sale and transfer of surveillance technologies.

The Pegasus Project's revelations disprove any claims by NSO Group that such attacks are rare or anomalous, or arising from rogue use of their technology. While the company asserts its spyware is only used for criminal and terrorism-related investigations, it has become clear that its technology facilitates large-scale, systemic abuse, in which NSO Group appears to be complicit.

Amnesty International would like to draw attention to its briefing, entitled *Uncovering the Iceberg: The digital surveillance crisis wrought by states and the private sector*, as well as a joint NGO statement calling for robust new European Union (EU) Export Control Rules and an investigation into the role of EU member states in the Pegasus Project revelations.

In this briefing document, Amnesty International outlines key measures urgently needed to ensure greater regulation over the cybersurveillance industry, accountability for human rights violations and more independent oversight over this opaque industry. Given the wide-ranging impact of these revelations, we would urge the EU and its member states to draw on both their internal and foreign policy instruments to address these abuses, and ensure robust and meaningful regulation over the cybersurveillance industry.

These include the following recommendations toward the EU and its member states:

Recommendations for action within the European Union

- **EU member states must immediately put in place a moratorium on the sale, transfer, and use of cybersurveillance technologies.** Given the breadth and scale of these findings, there is an urgent need to halt surveillance technology enabled activities of all states and companies, until there is a human rights-compliant regulatory framework in place.

- **EU member states must ensure effective remedy to victims of unlawful targeted surveillance and hold perpetrators to account for the violations. Further, member states must commit to reforming existing laws that pose barriers to remedy for these victims and ensure that both judicial and non-judicial paths to remedy are available in practice.**

- **EU member states must adopt and enforce legislation that requires all corporate actors to respect human rights and implement human rights due diligence measures as prescribed by**

the UN Guiding Principles. Corporate actors should be required to identify, prevent, and mitigate potential and actual adverse human rights impacts of their operations and throughout their value chain.

- **EU member states must adopt and implement domestic legislation that imposes safeguards against human rights violations and abuses resulting from unlawful digital surveillance.** This should be in line with the 2015 European Court of Human Rights judgment in *Roman Zakharov v. Russia*, as well as the Necessary and Proportionate Principles, and should establish accountability mechanisms, causes of action, etc. designed to provide victims of surveillance abuses a pathway to remedy.

- **EU member states and the European Commission should ensure the robust implementation of the new EU Export Control Rules that entered into force on 9 September 2021 with the recast Dual-Use Regulation.** This includes taking immediate action toward underscoring the human rights due diligence obligations that follow from the Dual-Use Regulation and creating a transparent market in cybersurveillance technologies that is bound by effective human rights safeguards.

    - The new Regulation establishes that the Commission shall publish an annual public report to the Parliament and Council. These reports should at a minimum include the number of license applications per item, the exporter name, a description of the end user, destination, and intended use, the government agency involved, the value of the license, and whether the license was granted or denied and why.

    - Further, transaction screening measures by member states should include an assessment of the strategic nature of the items and the risks they represent to the violation of human rights. National authorities should report on the implementation of due diligence responsibilities and obligations and encourage companies to inform the public about the scope, nature, and findings of the human rights due diligence procedures they implemented.

    - Member states should ensure that exporting countries establish mechanisms to provide effective remedy for human rights violations committed using the transferred technology. The guidelines that will be published pursuant to art. 26(1) Dual-Use Regulation 2021/821/EU, must detail requirements for internal compliance programs and due diligence that is expected from exporters in the Dual-Use Regulation based on the United Nations Guiding Principles on Business and Human Rights (UN Guiding Principles) and the OECD Guidelines for Multinational Enterprises.

- **The Council and EU member states should address concerns regarding Hungary's use of unlawful surveillance technologies in the ongoing Article 7 Treaty on European Union (TEU) proceedings.** They should urge Hungary to remedy the violations of fundamental rights and the rule of law.

- **In light of the of the unlawful targeted surveillance in Hungary, the European Commission should investigate the abuse of digital surveillance technologies by Hungarian authorities, as well as whether any other EU member states have engaged in such abuses.** This investigation should assess whether Hungary or any other member state has respected its obligations under EU Treaties, the EU Charter of Fundamental Rights, the General Data Protection Regulation, the Law Enforcement Directive, and the e-Privacy Directive. **If Hungary is found to be in breach of its obligations, the European Commission should initiate infringement procedures.**

- **The European Commission should immediately conduct an investigation into all EU and member states' export licenses granted, including EU General Export Authorisation EU005 that includes software designed for the use of monitoring and interception equipment, and ensure that EU members states revoke all marketing and export licenses in situations where there is a significant risk that such technology could contribute to human rights violations.** NSO Group has a corporate presence in Luxembourg and according to the NSO Group's 2021 Transparency and Responsibility Report the company also exports its products from Bulgaria and Cyprus. **If members**

states' granting of export licenses are found to be in violation of export regulation standards, the European Commission should initiate infringement proceedings.

- **The European Parliament (EP) should engage in a cross-committee and cross-party efforts to properly assess the internal and external elements of this matter and demand a proper European response.** The European Parliament and its members should urge the European Commission, the Council and EU member states to draw on both their internal and foreign policy instruments to address these violations and ensure robust and meaningful regulation over the surveillance industry, including pushing for all the recommendations in this briefing.

Recommendations for action by the European Union and its member states through their foreign policy instruments

- **The EU and its member states must clearly articulate their position on the findings of the Pegasus Project, including through official statements.** The violations exposed by the Pegasus Project have been wide-ranging, with the full scale and breadth of the targeting likely extending well beyond the cases exposed to date. Given its ambition to be a global standard setter, the EU can and must play a role in ensuring the protection of human rights and adherence to the rule of law in the digital realm at home and abroad. This is rooted in the EU's and its member states' human rights obligations to protect and promote human rights globally as laid out in the Article 21 of The Lisbon Treaty. Further, this aligns with EU commitments in the Council Conclusions on Shaping Europe's Digital Future, the EU action plan on Human Rights and Democracy and the EU's human rights guidelines. EU leaders, including Commission President Von Der Leyen and High Representative Borrell, have already underlined the importance of protecting civil society and upholding the right to privacy and freedom of expression online in the digital age. Further statements by the EU and its member states should:

    - Express concern about the media revelations that the NSO spyware has been used to target journalists, activists and heads of state on a widespread and systematic scale, stressing that such practices are unacceptable and violate the rights to freedom of expression, peaceful assembly and privacy.

    - Stress that the revelations underscore the urgent need for greater transparency and legal accountability of the surveillance industry.

    - Stress that these cases are illustrative of the rising digital attacks and targeted surveillance of human rights defenders, journalists and civil society by governments seeking to silence and intimidate such actors around the world.

    - Call on states to take urgent measures toward ensuring greater regulation over the cybersurveillance industry, accountability for related human rights violations and greater oversight over this poorly-regulated industry.

- **EU member States should reach out bilaterally and organize démarches toward the relevant authorities in third states identified in the Pegasus Project as suspected NSO Group clients:** The Pegasus Project identified individuals who were persons of interest who were selected for potential targeting by the following countries: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates. The EU and its member states should seek clarifications from the authorities in these countries, and among other things:

    - Urge the relevant authorities to conduct an immediate, independent, transparent and impartial investigation of any cases of unlawful surveillance revealed by the Pegasus Project, and where appropriate, pursue legal avenues to provide remedies to victims and hold perpetrators to account, in accordance with international human rights standards.

- Underline that the use of spyware by governments for surveillance is lawful only when it meets certain strict criteria, as set out in international human rights law, and that any such surveillance must be lawful, necessary, proportionate, and time bound.

- Urge these states to uphold their obligations and commitments under international human rights law, including those outlined in the ICCPR and the UN Declaration on human rights defenders.

- Raise the cases of targeted human rights defenders, journalists and activists with the authorities at the highest levels and offer these individuals political, technical and other support in line with the EU guidelines on human rights defenders, the EU guidelines on freedom of expression and the EU action plan on human rights and democracy.

- **EU member states must call on Israel and any other exporting states in third countries to immediately revoke all marketing and export licences issued to NSO Group and conduct an independent, impartial, transparent investigation to determine the extent of unlawful digital surveillance.** This should include a full review and subsequent reform of the export licensing regime to ensure that it is fit for purpose in law and practice, and it prevents future human rights abuses related to the export of cybersurveillance equipment from their jurisdictions. This should culminate in public disclosure of results of the investigation and steps taken to prevent future abuses. These states should also take measures to ensure that the NSO Group:

  - Immediately terminates the use, support and sale of Pegasus to all states until robust human rights regulations govern the sale, transfer, and use of surveillance technology adequately.

  - Provides adequate compensation or other forms of effective redress to victims of unlawful surveillance using NSO Group's products.

  - Takes proactive steps to ensure that it does not cause or contribute to human rights violations, and responds to any human rights violations – including those that feature in the Project Pegasus investigation – when they do occur. In order to meet that responsibility, NSO Group must carry out adequate human rights due diligence and take steps to ensure that HRDs, journalists and civil society do not continue to become targets of unlawful surveillance.

- **EU member states should participate in key multilateral efforts, including at the UN Human Rights Council, UN General Assembly, and Universal Periodic Review cycles, to develop robust human rights standards that govern the development, sale, transfer, and use of surveillance equipment, and identify impermissible targets of digital surveillance.** This includes by supporting the call for an immediate moratorium on the sale, transfer and use of surveillance technology.