United Nations Special Rapporteur on the Promotion and Protection of Human Rights While Countering Terrorism

Professor Fionnuala Ní Aoláin

Statement on the Development, Use, and Transfer of Commercial Spyware

1. The mandate of the Special Rapporteur is deeply concerned about the use of sophisticated surveillance technology developed for counter-terrorism and national security purposes.[1] In her view, intrusive covert technology for surveillance of the content of individuals' digital communications, and other information including metadata (location, duration, source, and contacts) – commonly known as 'spyware' – has proliferated internationally out of all control and poses substantial risks to the promotion and protection of human rights.

2. The Special Rapporteur has increasingly recognized the sustained evidence that such tools are in fact being used to spy upon politicians, journalists, human rights activists, lawyers, and ordinary citizens with no links to terrorism and who pose no national security threat. Revelations of recent years have shown the ubiquity of covert digital surveillance technology originally designed for counter-terrorism purposes, typically known as 'spyware.' The persistent and global misuse of this technology by both democratic and non-democratic States poses grave risks to the promotion and protection of human rights, and particularly in respect of fundamental and non-derogable rights. While the companies which produce spyware insist that such technology is only intended for legitimate use by investigative authorities in line with relevant legal controls, in reality State agencies engage in persistent and documented abuse of these powerful tools to spy on political opponents, dissidents, human rights defenders, journalists, and ordinary citizens.

[1] A/HRC/52/39

3. In April 2023 the Special Rapporteur on Counter-Terrorism and Human Rights launched a ground-breaking report on the use of commercial Spyware in New York at an event co-sponsored by the European Union and the government of the Republic of Costa Rica's missions to the United Nations. This report has acted as a basis for extensive consultation with Member States across regional groups including GRULAC, the European Union, the African Union, ASEAN states, and the Organization of Islamic States. She has also consulted with several Member States of the Security Council, across both E10 and P5 membership. The Special Rapporteur has also met with representatives of the European Parliament, civil society representatives as part of RightsCon 2023, with Heads of National Delegations during UN High Level Counter-Terrorism Week in June 2023 and Heads of Delegation during General Assembly High-Level Week in September 2023. As an entity member of the UN Global Counter-Terrorism Coordination Compact, the Special Rapporteur has engaged with multiple UN entities concerning the interface with counter-terrorism with new technologies and corresponding human rights violations including the use of commercial spyware.

4. The Special Rapporteur's Spyware Report carried out an extensive survey to map the full range of human rights violations implicated by the misuse of commercially-available spyware technology, and then considered the existing legal and regulatory approaches to those potential harms and identified the inadequacy of existing regulatory regimes. The Report concludes by providing a set of minimum requirements, grounded in international human rights law, which any new regulatory approach would need to display to constitute effective regulation of the spyware industry if human rights harms are to be mitigated. **But proposals for regulation should not be interpreted as a tacit endorsement of spyware per se. On the contrary, the Report makes clear that, unless current and future capacities of spyware technology are consistent with international human rights law, it is unlikely that such technology can ever be used lawfully.**

5. The development of spyware technology by the private sector and its enthusiastic adoption by States is a vivid demonstration of the trends identified in the Special Rapporteur's 2023

report to the Human Rights Council. In particular, she has observed how new counter-terrorism technologies tend to be developed in a silo without due regard to the human rights implications of their eventual use, and how challenging it is to develop human rights-respecting systems of regulation after the fact when those technologies – and their adverse human rights impacts – have already become imbedded in counter-terrorism operations and practice worldwide.

6. The focus of the Mandate on this issue has coincided with movements worldwide urging action by governments and the global security technology industry. The Special Rapporteur welcomes the initiative of the second Summit for Democracy in this area, co-hosted by Costa Rica, the Netherlands, the Republic of Korea, the United States, and Zambia, including the March 2023 Joint Statement of the governments of Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States recognizing the threat posed by the misuse of commercial spyware and the need for strict domestic and international controls on its proliferation and use. She also welcomes the March 2023 Executive Order prohibiting the use by the United States of commercial spyware which is provided to States which have records of gross human rights abuse, or have used the technology to target dissidents.[2] The Special Rapporteur further notes the UK-France Joint Leaders' Declaration of March 2023 announcing a joint initiative to address the threat from commercial cyber proliferation, including spyware.[3]

7. **The Special Rapporteur urges more governments to join the international effort to reconsider and reduce the development, use, and transfer of spyware technology**. Spyware poses an existential threat to civil society, not only granting a powerful weapon to repressive regimes in their targeting of individuals, but undermining privacy, freedom of expression, assembly, and association, and fair trial rights. She strongly encourages governments who have taken the important first step of recognizing the danger of commercial spyware, to support in the first instance robust domestic legislation to prevent

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/
[3] https://www.gov.uk/government/publications/uk-france-joint-leaders-declaration/uk-france-joint-leaders-declaration

its misuse at home. Thereafter, she encourages these governments to pursue passage of a General Assembly Resolution that commits States to the prevention of the harms of commercial spyware through human rights compliant regulation. Such regulation is one building block to advance human rights and rule of law compliant global regulation. She also recognizes that the nature and harm of this technology may require a ban, should human rights compliant regulation prove technically or politically elusive. Certainly, the Special Rapporteur reiterates the growing international call for an immediate moratorium.

8. The Special Rapporteur welcomes in particular the report of the European Parliament Committee of Inquiry (PEGA) to investigate the use of Pegasus and equivalent surveillance spyware, released in May 2023.[4] The PEGA report considers substantial failings of purported *ex ante* and *ex post* regimes for controlling spyware misuse and recommends a series of reforms to strengthen human rights safeguards with a focus on the export control regime for dual-use technologies. In particular, the mandate of the Special Rapporteur on CT and HR wishes clearly to endorse the recommendations that, if commercial spyware is to continue to be lawfully developed and deployed at all, there must always be controls built into the technology to allow for its invasive capacities to be limited, and for its uses to be recorded, traced, and properly investigated after the fact**. In addition, the Special Rapporteur highlights and endorses PEGA's conclusion that the use of spyware must cease unless and until all recommended limitations and restrictions on its misuse have been implemented[5] – a call for a *de facto* moratorium[6] which echoes previous calls from UN human rights experts.[7]**

[4] See: European Parliament decision of 10 March 2022 on setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, and defining the subject of the inquiry, as well as the responsibilities, numerical strength and term of office of the committee (2022/2586(RSO).
[5] See: European Parliament Draft Recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration of the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)), paras 36-37.
[6] Adopting the language of the European Parliament Socialists and Democrats group. See: https://www.socialistsanddemocrats.eu/newsroom/pegasus-spyware-inquiry-sds-call-strong-eu-regulation-prevent-abuse-member-states
[7] See: Report of the Special Rapporteur on the Promotion and Protection of the Rights to Freedom of Opinion and Expression, A/HRC/41/35; and Office of the UN High Commissioner for Human Rights, 'Spyware scandal: UN experts call for moratorium on sale of "life threatening" surveillance tech,' available at: https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-

9. She recognizes and commends the PEGA Committee's extensive fact-finding process, leading to a compelling record of misuse of spyware in breach of human rights and EU law protections within the European Union, and the apparent complicity of EU-based corporations and Member States in the development and proliferation of that technology for harmful ends.

10. She calls upon States to engage directly with the specific recommendations in her report and in the report of the PEGA Committee, including:

    10.1. That States consider carefully harnessing the deterrent power of civil liability alongside government regulation, which will incentivize manufacturers to build in robust protections against abuse of their products and/or minimize their dealings with clients who pose a risk of human rights;

    10.2. That spyware which fails to display certain inbuilt limitations and controls should never be allowed, and at a minimum those controls should include powers to limit the scope of digital intrusion, markers and 'kill switches' in cases of misuse, and an indelible, permanent, uneditable and auditable record of actions taken by spyware users so that compliance can properly be assessed after the fact; and

    10.3. That international co-ordinated action is essential so as to ensure that broadly-similar rules apply in States where manufacturers are, or would prefer to be, based, so as to minimize opportunities for regulatory arbitrage.

11. The Special Rapporteur notes that the commercial spyware industry has belatedly voiced its support for some form of self-regulation. Voluntary efforts on the part of industry are certainly welcome, but the human rights stakes are too high to leave the solution to this global human rights crisis in the hands of those whose business model relies upon the

threatening#:~:text=GENEVA%20(12%20August%202021)%20–,with%20international%20human%20rights%20standards.

growth of the use of this technology internationally. She calls upon the United Nations and Member States to make clear that global regulation must take the course of multilateral, mandatory action with legal force, rather than piecemeal voluntary changes in the private sector. She highlights that:

11.1. While the mandate of the Special Rapporteur recognizes the added value of soft law standards including the Guiding Principles on Business and Human Rights, self-regulation based on soft standards may not be an appropriate regulatory basis for all industries. Soft law is most effective and relevant to protect and promote human rights when it adheres to and normatively reinforces existing hard law standards. Self-regulation is an inadequate basis to regulate risk and harm when applied to a technology which as in the case there is virtually no effective hard law regulatory standards in place;

11.2. Self-regulation is particularly unsuitable for a high-risk technology that has a demonstrated history of abuses and emanates from a sector that is marked by its lack of transparency and disregard of international human rights law.

11.3. The limits of self-regulation are self-evident given the evidenced violations of non-derogable and peremptory norms of international law.

12. The Special Rapporteur encourage States to take multiple multi-lateral opportunities to advance positive regulatory opportunities, not only using the mechanisms of the United Nations, but also organs such as the European Union and the Council of Europe to advance co-ordination and a united front on this pressing international threat to human rights protection. Accordingly, the Special Rapporteur:

12.1. **Welcomes** the September 2021 Recast Dual-Use Regulation, which updated the restrictions upon exports of cybersurveillance technology which may be intended for use in connection with internal repression or the commission of serious violations of human rights and international humanitarian law;

12.2. **Urges** the European Union to go further by tightening, specifying and enforcing the obligations on national legal systems to prevent the use and transfer of commercial spyware;

12.3. **Recommends** that regional human rights systems such as the Council of Europe, involving both CDCT and the Commissioner for Human Rights press forward with the development of regionally robust standards that address the misuse of spyware technology and provide guidance on regional human rights remedies to victims of spyware misuse;

12.4. **Recommends** that OHCHR, UN Special Procedures Mechanisms and UN Human Rights Treaty Bodies continue to address the misuse of spyware technology through the development of specific human rights guidance, provide regular SPB communications to Member States highlighting cases of individual and collective misuse, and provide guidance on regulation and remedy including through technical advice and assistance, and hold States accountable for both regulatory acts and omissions through treaty body reporting and individual cases under relevant Optional Protocols.