Dear Chair, dear members of the European Parliament Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware,

We – a group of civil society organisations and human rights defenders – are writing to you following the establishment of the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware to urge you, as members of the committee, to ensure that the systematic targeting of human rights defenders with these technologies is fully examined by the Committee, and that the voices of human rights defenders affected are heard.

We welcome the establishment of this Committee of Inquiry and are pleased to see that the Committee has been given the mandate to:

"(ascertain) whether Member States' authorities have used the Pegasus and equivalent surveillance spyware for political, economic or other unjustified purposes to spy on journalists, politicians, law enforcement officials, diplomats, lawyers, businessmen, civil society actors or other actor"

to:

"collect information on the extent to which Member States … or third countries use intrusive surveillance in a way that violates the rights and freedoms enshrined in the Charter of Fundamental Rights"

and to examine:

"whether the use of Pegasus or equivalent surveillance spyware, directly or indirectly involving entities linked to the EU, contributed to illegal spying on journalists, politicians, law enforcement officials, diplomats, lawyers, businessmen, civil society actors or other actor in third countries… with due regard to the United Nations Guiding Principles on Business and Human Rights and other rights enshrined in international human rights law."

The EU and its member states have made countless commitments to supporting human rights defenders, including through the EU's Guidelines on Human Rights Defenders. It is therefore crucial that this committee not only examines the use of spyware in, and by Member States, but also its use in third countries. Violations of the rights of human rights defenders in third countries is particularly relevant to the committee of inquiry for two reasons: Firstly, because NSO Group has been established to have links to companies registered in the European Union.[1] And secondly, because the purchase of Pegasus spyware by EU Member States whilst the technology was being used to violate the rights of human rights defenders, journalists and vulnerable groups in third countries could constitute a failure to "exercise adequate oversight in order to meet their international human rights obligations when they contract with… business enterprises to provide services that may impact upon the enjoyment of human rights"[2] as outlined in the UN Guiding Principles on Business and Human Rights.

A series of investigations by media organisations and civil society[3] have established the wide ranging and significant impact of the use of Pegasus and other surveillance technologies to spy on human

[1] Amnesty International, Operating from the Shadows: Inside NSO group's Corporate Structure, 31 May 2021
[2] OHCHR, Guiding Principles on Business and Human Rights, 2011
[3] Amnesty International, Forensic Methodology Report: How to catch NSO Group's Pegasus - Amnesty International, 18 July 2021; Frontline Defenders, AccessNow, Unsafe Anywhere: Women Human Rights Defenders Speak Out About Pegasus Attacks, 16 January 2022; Frontline Defenders, the Citizen Lab, Report: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware, 05 April 2022; Frontline Defenders, the Citizen Lab, Press Release: Front Line Defenders Investigation Finds Pegasus Software on 6 Palestinian HRD Phones, 08 November 2021; Multiple organisations, Exposed: civil society condemns use of

rights defenders around the world. Notably, the Pegasus Project coordinated by Forbidden Stories, and with the technical support of Amnesty International, exposed the massive scale and breadth of targeting of civil society actors around the world.[4] The prevalence of these technologies has led many human rights defenders to become fearful that they may be unknowingly targeted, and some have decided to halt or change the nature of their human rights work.[5] Women human rights defenders have described their social isolation following their targeting with Pegasus spyware.[6] Friends and families also distance themselves in fear of also being harmed or surveilled. Their homes and private spaces becoming no longer private and no longer safe.

Although many reports outline the devastating impact of these patterns of surveillance nothing can replace the testimony of those directly affected. To fully understand the impact of Pegasus and equivalent spyware, it will be important that the committee speak directly with human rights defenders, from the EU as well as third countries. With this in mind, we are open to supporting this committee to center the voices of civil society actors targeted with Pegasus around the world.

Lastly, we hope that the final report that will conclude the work of the committee will address in a substantial and in-depth manner the external dimension of the use of Pegasus and other spyware, notably in relation to human rights defenders in third countries, and draw ambitious and practical recommendations for EU actors, including the European External Action Service, the European Commission and the European Parliament, in this regard.

Signatories
Access Now
Al-Haq
Alternatif Bilisim (AiA-Alternative Informatics Association)
Amnesty International
Article 19
Cairo Institute for Human Rights Studies (CIHRS)
Državljan D - Citizen D
Electronic Frontier Finland
Electronic Frontier Norway
European Digital Rights (EDRi)
Front Line Defenders
Homo Digitalis
Indigenous Peoples Rights International
International Federation for Human Rights (FIDH)
International Service for Human Rights (ISHR)
IT-Pol Denmark
Michel Forst, Former UN Special Rapporteur on the Situation for Human Rights Defenders
Open Society European Policy Institute (OSEPI)
Project on Organizing, Development, Education, and Research (PODER)
Protection International
Statewatch

Pegasus in El Salvador to spy on journalists and activists, 12 January 2022; ARTICLE 19, #GobiernoEspia: Victims' lawyers in Narvarte case targets of Pegasus spyware, 09 August 2017.

[4] Amnesty International, Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, 19 July 2021

[5] Frontline Defenders, Action needed to address targeted surveillance of human rights defenders, 02 December 2021

[6] Frontline Defenders, Unsafe anywhere: Women human rights defenders speak out about Pegasus attacks.

The Palestine Institute for Public Diplomacy (The PIPD)
Vrijschrift.org