Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology

We, the undersigned civil society organizations and independent experts, are alarmed at the media revelations that NSO Group's spyware has been used to facilitate human rights violations around the world on a massive scale.

These revelations are a result of the Pegasus Project and are based on the leak of 50,000 phone numbers of potential surveillance targets. The project is a collaboration of more than 80 journalists from 16 media organizations in 10 countries coordinated by Forbidden Stories, a Paris-based media non-profit, with the technical support of Amnesty International, who conducted forensic tests on mobile phones to identify traces of the Pegasus spyware.

The Pegasus Project's revelations prove wrong any claims by NSO 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 legitimate criminal and terror investigations, it has become clear that its technology facilitates systemic abuse. As the UN High Commissioner for Human Rights said, "if the recent allegations about the use of Pegasus are even partly true, then that red line has been crossed again and again with total impunity."

From the leaked data and their investigations, Forbidden Stories and its media partners identified potential NSO clients in 11 countries: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates (UAE). NSO claims it only sells it to government clients.

The investigation has so far also identified at least 180 journalists in 20 countries who were selected for potential targeting with NSO spyware between 2016 to June 2021. Deeply concerning details that have emerged include evidence that family members of Saudi journalist Jamal Khashoggi were targeted with Pegasus software before and after his murder in Istanbul on 2 October 2018 by Saudi operatives, despite repeated denials from NSO Group that its products were used to target Khashoggi or his family members.

The revelations are only a tip of the iceberg. The private surveillance industry has been allowed to operate unchecked. States have failed not only in their obligations to protect people from these human rights violations, but have themselves failed in their own human rights obligations, clearly letting these invasive weapons loose on people worldwide for no other

reason than exercising their human rights. Additionally, the targeting may in fact reveal only part of the picture of human rights violations that they signify. This is because violations of the right to privacy impact on numerous other human rights and show the real-world harm caused by surveillance that is inconsistent with international norms.

In Mexico, journalist Cecilio Pineda's phone was selected for targeting just weeks before his killing in 2017. Pegasus has been used in Azerbaijan, a country where only a few independent media outlets remain. Amnesty International's Security Lab found the phone of Sevinc Vaqifqizi, a freelance journalist for independent media outlet Meydan TV, was infected over a two-year period until May 2021. In India, at least 40 journalists from major media outlets in the country were selected as potential targets between 2017-2021. Forensic tests revealed the phones of Siddharth Varadarajan and MK Venu, co-founders of independent online outlet The Wire, were infected with Pegasus spyware as recently as June 2021. Amidst this revelation, Moroccan journalist and human rights activist Omar Radi was sentenced to six years in prison. Radi's phone had previously been forensically examined by Amnesty International in 2020 and was determined to be targeted by Pegasus. In Morocco, of the 34 other journalists whose phones were selected for potential targeting by Pegasus, two are imprisoned. The investigation also identified journalists working for major international media including the Associated Press, CNN, The New York Times and Reuters as potential targets. One of the highest profile journalists was Roula Khalaf, the editor of the Financial Times. These targets represent only a small part of the revelations and the full picture is yet to emerge.

This is not the first time NSO's Pegasus software has been linked to human rights violations. Researchers, journalists, activists and others have uncovered significant evidence over the years of the use of NSO Group's surveillance technology to target individuals. Previous research by Citizen Lab exposed how Ahmed Mansoor, a human rights defender imprisoned in the United Arab Emirates, was targeted with NSO Group technology in 2016. In Mexico, journalists, lawyers, and public health experts have also been previously targeted.

Where surveillance is operated without adequate legal frameworks, oversight, safeguards and transparency, its harms have an impact far beyond those who may have actually been targeted. In the face of opacity and inadequate safeguards, and especially in situations where surveillance is known or suspected to be carried out in unlawful ways, human rights defenders and journalists are forced to self-censor out of fear of being persecuted for their work, even where such surveillance may in fact not be taking place. Indeed, in the immediate aftermath of revelations journalists and activists are already noting the chilling effect on their work.

Importantly, the use of targeted digital surveillance tools such as Pegasus infringe the right to privacy and many other rights. Pegasus impacts the right to privacy by design: it is

surreptitious, deployed without the knowledge of the rights holder, and has the capacity to collect and deliver an unlimited selection of personal, private data (along with data of any contacts with which a target interacts). Moreover, as noted above, a violation of the right to privacy can have cascading effects on other rights, including the rights to freedom of expression, association, and peaceful assembly. It is evident from these disclosures that these uses of the tool are abusive and arbitrary, and do not constitute a permissible interference with the right to privacy. Further, states' unchecked deployment of these tools does not meet the tests of necessity, proportionality, and legitimate aim as outlined under international standards.

A culture of impunity specific to targeted digital surveillance has developed that must be urgently countered. These disclosures show just how states' use of the targeted digital surveillance tools supplied by one of the industry's most prominent participants is utterly out of control, destabilizing, and threatening to individuals' human rights, including physical safety. The revelations shine a light on an unaccountable industry, and an unaccountable sphere of state practice, that must not continue to operate in their current forms. Our rights and the security of the digital ecosystem as a whole depend on it.

We back the call of the UN High Commissioner that "Governments should immediately cease their own use of surveillance technologies in ways that violate human rights, and should take concrete actions to protect against such invasions of privacy by regulating the distribution, use and export of surveillance technology created by others."

Thus, we urge all states to urgently take the following steps:

To all states:

a. Immediately put in place a moratorium on the sale, transfer, and use of surveillance technology. 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 human rights regulatory efforts catch up.
b. Conduct an immediate, independent, transparent and impartial investigation into cases of targeted surveillance. Further, investigate export licenses granted for targeted surveillance technology, and revoke all marketing and export licenses in situations where human rights are put at risk.
c. Adopt and enforce a legal framework requiring private surveillance companies and their investors to conduct human rights due diligence in their global operations, supply chains and in relation to the end use of their products and services. Under this legislation, private surveillance companies should be compelled to identify, prevent,

and mitigate the human rights-related risks of their activities and business relationships.

d. Adopt and enforce a legal framework requiring transparency by private surveillance companies, including information on self-identification/registration; products and services offered; the results of regular due diligence including details of how they addressed identified risks and actual impacts; and sales made as well as potential clients rejected for failing to meet standards of human rights or good governance. States should make this information available in public registries.
e. Ensure that all surveillance companies domiciled in their countries, including sales intermediaries, affiliates, holding companies, and private equity owners, are required to act responsibly and are held liable for their negative human rights impacts. They must require by law that these companies undertake human rights due diligence measures in respect of their global operations. This should include liability for harm caused and access to remedy in the home states of the companies, for affected individuals and communities. Governments should therefore initiate or support domestic proposals for corporate accountability legislation.
f. Disclose information about all previous, current and future contracts with private surveillance companies by responding to requests for information or by making proactive disclosures.
g. As a condition to continued operation of surveillance companies, demand immediate establishment of independent, multi-stakeholder oversight bodies for NSO Group and all other private surveillance companies. This should include human rights groups and other civil society actors.
h. Establish community public oversight boards to oversee and approve the acquisition or use of new surveillance technologies, with powers to approve or reject based on the states' human rights obligations, provisions for public notice and reporting.
i. Reform existing laws that pose barriers to remedy for victims of unlawful surveillance and ensure that both judicial and non-judicial paths to remedy are available in practice.
j. Furthermore, states must, at a minimum, implement the below recommendations if the moratorium on the sale and transfer of surveillance equipment is to be lifted:

    - Implement domestic legislation that imposes safeguards against human rights violations and abuses through digital surveillance and establishes accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy.
    - Implement procurement standards restricting government contracts for surveillance technology and services to only those companies which demonstrate that they respect human rights in line with the UN Guiding Principles and have not serviced clients engaging in surveillance abuses.

- Participate in key multilateral efforts to develop robust human rights standards that govern the development, sale and transfer of surveillance equipment, and identify impermissible targets of digital surveillance

k. Inform securities exchanges and financial regulators of the harms associated with private surveillance technology companies, and require strict, regular scrutiny in law and regulation of disclosures and applications by those companies and their owners, including before any major events (public listings, mergers, acquisitions, etc.)
l. Protect and promote strong encryption, one of the best defences against invasive surveillance.

We urge Israel, Bulgaria, Cyprus and any other states in which NSO has corporate presence:

a. Exporting States, including Israel, Bulgaria and Cyprus, must immediately revoke all marketing and export licenses issued to NSO Group and its entities, and conduct an independent, impartial, transparent investigation to determine the extent of unlawful targeting, to culminate in a public statement on results of efforts and steps to prevent future harm.

Signatories

Civil Society Organizations

#SeguridadDigital
Access Now
Advocacy for Principled Action in Government
Africa Open Data and Internet Research Foundation (AODIRF)
African Freedom of Expression Exchange (AFEX)
Al-Haq
ALQST for Human Rights
Amman Center for Human Rights Studies (ACHRS)
Amnesty International
ARTICLE 19: Global Campaign for Free Expression
Asian Forum for Human Rights and Development (FORUM-ASIA)
Asociación por los Derechos Civiles (ADC)
Association for Progressive Communications (APC)
Barracón Digital
Bits of Freedom
Bloggers of Zambia
BlueLink Foundation
Body & Data, Nepal

Brazilian Association of Investigative Journalism (Abraji)
Brazilian Institute of Consumer Protection (Idec)
Breakpointing Bad
Business & Human Rights Resource Centre
Center for Democracy & Technology
Center for Civil Liberties (Ukraine)
Centro de Análisis Forense y Ciencia Aplicadas -CAFCA-
Centro de Documentación en Derechos Humanos “Segundo Montes Mozo S.J.” (CSMM)
Citizen D | Državljan D
Civic Assistance Committee, Russia
CIVICUS: World Alliance for Citizen Participation
Civil Rights Defenders
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Comisión Ecuménica de Derechos Humanos, Ecuador
Comisión Intereclesial de Justicia y Paz
Comisión Intereclesial de Justicia y Paz
Comisión Mexicana de Defensa y Promoción de los Derechos Humanos
Committee to Protect Journalists (CPJ)
Conectas Direitos Humanos
Conectas Human Rights
Conexo
Cooperativa Tierra Común - México
CyberPeace Institute
Data Privacy Brasil Research Association
Datysoc
Deache
Defend the Defenders
Defense for Children International - Palestine
Derechos Digitales · América Latina
Digitalcourage
Digital Defenders Partnership
Digital Empowerment Foundation
Digital Rights Foundation
Digital Rights Kashmir
Digital Security Lab Ukraine
DPLF - Due Process of Law Foundation/Fundación para el Debido Proceso
Egyptian Initiative for Personal Rights (EIPR)
Electronic Frontier Foundation (EFF)
Electronic Privacy Information Center (EPIC)

ELSAM
epicenter.works
Equipo de Reflexión, Investigación y Comunicación de la Compañía de Jesús en Honduras
Equipo Jurídico por los Derechos Humanos (Honduras)
Ethics in Technology a 501c3
European Center for Not-for-Profit Law (ECNL)
European Digital Rights (EDRi)
FIDH - International Federation for Human Rights
Fitug e.V.
Franciscans International
Free Expression Myanmar (FEM)
Fundació.Cat
Fundación Acceso (Central America)
Fundación Datos Protegidos
Fundación InternetBolivia.org
Fundación Karisma (Colombia)
Global Partners Digital
Global Voices
Global Witness
GlobaLeaks
Guardian Project
Gulf Centre for Human Rights (GCHR)
Health, Ethics and Law Institute of Forum for Medical Ethics Society, India
Heartland Initiative
Hermes Center
Hiperderecho (Perú)
Hivos
Homo Digitalis
Horizontal
Human Rights Commission of Pakistan
Human Rights First
Human Rights House Foundation (HRHF)
IFEX
IFEX-ALC
Iniciativa Mesoamericana de Mujeres Defensoras de Derechos Humanos (IM-Defensoras)
INSM Network (Iraq)
Institute for Policy Research and Advocacy (ELSAM), Indonesia
Instituto para la Sociedad de la Información y 4ta Revolución Industrial (ISICRI) de Perú

International Commission of Jurists (ICJ)
International Corporate Accountability Roundtable
International Legal Initiative
International Service for Human Rights
Internet Freedom Foundation, India
Internet Protection Society (Russia)
IPANDETEC Centroamérica
Jordan Open Source Association (JOSA)
Justice for Iran
Kijiji Yeetu, Kenya
Liga voor de Rechten van de Mens (LvRM), The Netherlands
Ligue des droits humains, Belgium
Masaar -Technology and Law Community
Media Foundation for West Africa (MFWA)
MediaNama, India
Meedan
Mnemonic
Nothing2Hide
ONG Acción Constitucional
OpenArchive
Ordem dos Advogados do Brasil (OAB)
Panoptikon Foundation
Paradigm Initiative (PIN)
PDX Privacy
PEN America
PEN International
PEN Iraq
Planet Ally
Privacy International (PI)
Protection International (PI)
Punjab Women Collective
Ranking Digital Rights (RDR)
Red de Desarrollo Sostenible Honduras
Red en Defensa de los Derechos Digitales (R3D)
Reporters Sans Frontières / Reporters Without Borders (RSF)
Rethink Aadhaar
Robert F. Kennedy Human Rights
Roskomsvoboda (Russia)
S.T.O.P. - The Surveillance Technology Oversight Project

Security First
Seguridad en Democracia (SEDEM)
Sin Olvido
Sin Olvido Verde
SMEX
Southeast Asia Freedom of Expression Network (SAFENet)
Statewatch
Sursiendo, Comunicación y Cultura Digital
TEDIC NGO
Tejiendo Redes Infancia en América Latina y el Caribe
Terra-1530
The Bachchao Project (TBP)
The Humanism Project
The London Story, The Netherlands
Ubunteam
Universidad de Paz
Ura Design
Urgent Action Fund for Women's Human Rights (UAF)
Wikimedia France
Women's International League for Peace and Freedom (WILPF)
World Organisation Against Torture (OMCT)
Xnet

Independent Experts

Alex Orué, LGBTQ+ & digital activist, Mexico
Alex Raufoglu, Washington D.C, USA
Alexandra Argüelles (Mozilla Fellow)
Arzu Geybulla (Azerbaijan Internet Watch)
Chip Pitts, Independent Expert
David Kaye, Clinical Professor of Law, UC Irvine School of Law, and former United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
Douwe Korff, Emeritus Professor of International Law, London Metropolitan University
Dr. Courtney Radsch
Dr. Koldo Casla, Lecturer, University of Essex School of Law and Human Rights Centre
Dr. Tara Van Ho, Lecturer, University of Essex School of Law and Human Rights Centre
Elies Campo, Telegram Messenger
Elio Qoshi (Ura Design)

Giorgio Maone (NoScript)
Hannah R. Garry, Clinical Professor of Law, Director, USC International Human Rights Clinic
Jennifer Green, Clinical Professor of Law, University of Minnesota Law School
John Scott-Railton, Senior Researcher, the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy
Kenneth Harrow, Rwanda country specialist, Amnesty International USA
Kiran Jonnalagadda, Hasgeek
Kushal Das, Public Interest Technologist, Freedom of the Press Foundation, Director at Python Software Foundation
Marietje Schaake, President, CyberPeace Institute
Nikhil Pahwa, MediaNama
Rebecca MacKinnon, co-founder, Global Voices
Ritumbra Manuvie, University of Groningen
Ron Deibert, Professor of Political Science and Director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy
Susan Farrell (OTF AC)
Tarcizio Silva (Mozilla Fellow)