29 July 2021

Hon. Karen Andrews MP
Minister for Home Affairs
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

Cc: Parliamentary Joint Committee on Intelligence and security

Dear Minister Andrews,

The Pegasus Project: Massive data leak reveals Israeli NSO Group’s spyware used to target activists, journalists, and political leaders globally.

The Pegasus Project is a ground-breaking collaboration by more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories, a Paris-based media non-profit, with the technical support of Amnesty International, who conducted cutting-edge forensic tests on mobile phones to identify traces of the NSO Group’s spyware.

NSO Group Technologies is an Israeli technology firm whose spyware ‘Pegasus’ enables the remote surveillance of smartphones. Yet Amnesty’s most recent research highlights that the NSO Group’s spyware has been used to facilitate human rights violations around the world on a massive scale. These include heads of state, activists and journalists.

The investigation has uncovered that the NSO Group’s ‘Pegasus’ spyware which, when surreptitiously installed on victims’ phones, allows an attacker complete access to the device’s messages, emails, media, microphone, camera, calls and contacts.

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 Group has not taken adequate action to stop the use of its tools for unlawful targeted surveillance of activists and journalists, despite the fact that it either knew, or arguably ought to have known, that this was taking place.

The investigation has so far identified at least 180 journalists in 20 countries who were selected for potential targeting with NSO spyware between 2016 to June 2021, including in Azerbaijan, Hungary, India and Morocco, countries where crackdowns against independent media have intensified.
Amnesty International has released the full technical details of its Security Lab’s in-depth forensic investigations as part of the Pegasus Project.¹ The Lab’s methodology report documents the evolution of Pegasus spyware attacks since 2018, with details on the spyware’s infrastructure, including more than 700 Pegasus-related domains.

There is nothing to suggest that NSO’s customers did not also use Pegasus in terrorism and crime investigations, and the consortium also found numbers in the data belonging to suspected criminals.

**These revelations must act as a catalyst for change.** The surveillance industry must no longer be afforded a laissez-faire approach from governments with a vested interest in using this technology to commit human rights violations.

For these reasons, I ask that you

1. Conduct an audit of current security contracts to ensure Australia is meeting its own human rights obligations, and ensure that these tools are not used to unlawfully target human rights defenders and civil society
2. Disclose information about all previous, current, or future contracts with private surveillance companies by making proactive disclosures
3. Ensure surveillance is only against specified persons, authorized by a competent, independent and impartial judicial body with limitations on time, manner, place and scope of surveillance
4. Support the call for the global sale and transfer of surveillance technology to be temporarily paused.

For further information, or to discuss and organise a meeting, please contact Ry Atkinson at ry.atkinson@amnesty.org.au or 0423 270 124.

Yours sincerely,

Tim O’Connor
Campaigns Manager
Amnesty International Australia

---