November 5, 2021

The Honorable Antony Blinken  
Secretary of State  
U.S. Department of State  
2201 C Street, NW  
Washington, DC 20520

Secretary Blinken:

We write to urge you to use the resources of the State Department to further expose the direct link between advanced surveillance technologies and human rights abuse around the world, most recently highlighted by the revelations surrounding NSO Group’s Pegasus software and the Commerce Department’s entity listing of NSO Group and other companies. This bold step by the Biden administration highlights the risks from proliferation of off-the-shelf products marketed by foreign companies that facilitate gross human rights abuses. However, we write to urge further action to deter the growing proliferation of such products and services.

As members of Congress deeply concerned with the rising tides of authoritarianism around the world, we have closely tracked the parallel and reinforcing proliferation of commercially distributed surveillance and cyber-intrusion tools. These are extremely sensitive and powerful technologies used by foreign governments against Americans, as well as against journalists and civic activists. As noted by the Commerce Department, this week’s entity listing of NSO Group was based on evidence that the company “supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers.”

The proliferation of these tools represents a threat to U.S. national security interests, undermining strategic U.S policy objectives linked to good governance, democracy, free speech, and rule of law reforms. Globally, we have seen thousands of incidents of spyware use to track dissidents extraterritorially, intimidate civil society, track journalists and activists, and undermine democracy. While recent reporting confirmed that NSO Group’s Pegasus software was used against journalists, human rights activists, and opposition politicians, many others are profiting from this new arms market. Hacking tools sold by companies like China Electronics Technology Group and FinFisher have been linked to tracking minorities and hacking democracy activists, and Circles is selling its software to countries with a history of targeting journalists and activists with spyware.

These tools have become lynchpin drivers of survivability and reinforcement for authoritarian regimes. The proliferation of these tools provides a cheaper and less resource-intensive way for such regimes to police dissent, along with plausible deniability. Where dictators previously had to physically tail, detain, and interrogate sympathizers to track down critics, they can now do this dirty work behind the scenes with commercially supplied and easily available tools that hack into cell phones and computers of activists and opponents. Making matters worse, the market for such tools is “shrouded in secrecy.”

U.S. law explicitly asserts that defending human rights in other countries is in our interests: “A principal goal of the foreign policy of the United States shall be to promote the increased observance of internationally recognized human rights by all countries.” Further, as a signatory to both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, the U.S. has committed to the principle that “[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.” The UN Special Rapporteur on the promotion and
protection of the right to freedom of opinion and expression has called for “an immediate moratorium on
the sale and transfer of the tools of the private surveillance industry” xv until safeguards can be
established, noting that “Privacy and expression are intertwined in the digital age, with online privacy
serving as a gateway to secure exercise of the freedom of opinion and expression.”xvi

As a frontline weapon of authoritarians, digital surveillance tools represent a fundamental threat to U.S.
interests. As such, we urge you to take the following steps:

1. Consider the abusive clients of NSO Group and other such problematic companies for sanction
under the Global Magnitsky Act and consider the establishment of a targeted sanctions regime to
hold accountable individuals and companies that sell these tools to authoritarian states.

2. Coordinate with the Commerce Department to develop and regularly update a list of countries
likely to use products and services with surveillance capabilities in violation of basic human
rights, xvii including to silence dissent, sanction criticism, punish independent reporting (and
sources for that reporting), manipulate or interfere with democratic or electoral processes,
persecute minorities or vulnerable groups, or target advocates of human and democratic rights
(including activists, journalists, artists, minority communities, or opposition politicians).

3. Initiate a requirement for the State Department to produce a regular report to be shared with the
Commerce Department’s Bureau of Industry & Security, the Treasury Department’s Office of
Foreign Assets Control), the President, and Congress that lists foreign companies engaged in a
pattern of providing items and services with surveillance capabilities to countries or entities that
results in their use in violation of fundamental human rights.

4. Use all available diplomatic tools to shine a spotlight on and deter the sale of surveillance tools to
regimes with a history of human rights abuse and political repression, coordinating development
and distribution of such statements with likeminded allies (including co-signatories of the
Wassenaar Arrangement and members of the Freedom Online Coalition).

5. Consider using the State Department’s “Guidance on Implementing the UN Guiding Principles
for Transactions Linked to Foreign Government End-Users for Products or Services with
Surveillance Capabilities”xviii as the basis for a multilateral voluntary agreement or framework on
corporate best practices.

Again, we commend the Department for boldly recognizing the threats from 21st century surveillance to
human rights and US national security interests. We would welcome the opportunity to engage with you
on this urgent follow-on request.

Respectfully,

Tom Malinowski     Anna G. Eshoo
Member of Congress     Member of Congress

Katie Porter      Joaquin Castro
Member of Congress     Member of Congress
cc: The Honorable Gina Raimondo, Secretary of Commerce, U.S. Department of Commerce

1 U.S. Department of Commerce: Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (November 3, 2021)
2 Fast Company: Israeli cyberweapon targeted the widow of a slain Mexican journalist
3 Washington Post: Private Israeli spyware used to hack cellphones of journalists, activists worldwide
4 Reuters: WhatsApp sues Israel’s NSO for allegedly helping spies hack phones around the world
5 Forbes: Xinjiang: How China Uses A Spying Smartphone App To Automate Citizen Oppression
6 Privacy International: Surveillance follows Ethiopian political refugee to the UK
7 CitizenLab: From Bahrain With Love - FinFisher’s Spy Kit Exposed?
8 Amnesty International: German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed
9 AccessNow Alert: FinFisher Changes Tactics to Hook Critics
10 CitizenLab: Running in Circles - Uncovering the Clients of Cyberespionage Firm Circles
14 “International Covenant on Civil and Political Rights,” UN General Assembly (December 16, 1966), Art. 17(1); “Universal Declaration of Human Rights,” UN General Assembly (December 10, 1948), Art. 12; see also “Resolution adopted by the General Assembly on 16 December 2020” (Resolution 75/176), UN General Assembly, §1.
16 Id, ¶24.
17 We recommend starting with the definition of “Product or Service with Intended or Unintended Surveillance Capabilities” in the “Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities,” U.S. Department of State (September 30, 2020) at p. 5: (“Product or Service with Intended or Unintended Surveillance Capabilities: “product or service with intended or unintended surveillance capabilities” is defined as a product or service marketed for or that can be used (with or without the authorization of the business) to detect, monitor, intercept, collect, exploit, preserve, protect, transmit, and/or retain sensitive data, identifying information, or communications concerning individuals or groups.”)
18 Id.