

Congress of the United States

Washington, DC 20515

December 15, 2021

The Honorable Janet Yellen
Secretary
Department of Treasury
1500 Pennsylvania Ave NW
Washington, DC 20220

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

Dear Secretary Yellen and Secretary Blinken:

We write to urge you to implement Global Magnitsky sanctions for technology companies that have enabled human rights abuses, including the arrests, disappearance, torture and murder of human rights activists and journalists, such as Jamal Khashoggi, by selling powerful surveillance technology to authoritarian governments. This would build on the Administration's recent addition of several technology companies to the Entities List for surveillance-enabled human rights violations.

Journalists and civil society organizations have for years documented the direct link between the sale and export of surveillance technologies and human rights abuses by authoritarian governments. Commercially available surveillance technologies like malware, location tracking services and bulk intercept technology have directly contributed to those abuses. For example, according to Bloomberg, Bahraini activists were arrested and tortured, during which they were shown transcripts of text messages and phone calls intercepted using Western-supplied surveillance technology. As the Washington Post has reported, these surveillance products have also enabled dictators to reach beyond their own borders to hack the phones of activists and dissidents living in exile overseas, including in the United States. Furthermore, this technology also poses a serious threat to U.S. national security, as it has been used against U.S. government officials, as Reuters recently reported.

The Biden-Harris Administration has made a public commitment to "put human rights at the center of U.S. foreign policy, including by working to stem the proliferation of digital tools used for repression." The Secretary of Commerce followed through on that commitment when she recently added several surveillance companies to the Entities List, which will restrict the export by U.S. companies of technology to these foreign firms. While this bold action by the Administration is certainly worthy of praise, export controls alone are unlikely to effectively deter these foreign firms. Their developers are located overseas, and they can certainly find foreign sources for the hardware and software on which they rely to develop and sell their products.

However, these surveillance companies do depend on the U.S. financial system and U.S.-based investors, particularly when they eventually wish to raise billions by listing on the stock market.

To meaningfully punish them and send a clear signal to the surveillance technology industry, the U.S. government should deploy financial sanctions.

In 2016, Congress enacted the Global Magnitsky Human Rights Accountability Act, which gave the President the authority to sanction individuals responsible for gross violations of internationally recognized human rights. Executive Order 13818, which builds upon and implements the law, provides you with additional authority to also sanction individuals who provide technological support that enables human rights abuses. To that end, we urge you to add the following surveillance companies, their chief executive officers, senior executives, and other agents as appropriate, to the Specially Designated Nationals list published by the Office of Foreign Assets Control. Each of these companies are complicit in human rights abuses enabled through the surveillance technologies and services they sold to their authoritarian foreign government customers:

- DarkMatter, which according to an investigation by Reuters, hacked into the devices and accounts of human rights activists and journalists, including Americans, on behalf of the United Arab Emirates. According to cyber researchers at the Citizen Lab at the University of Toronto, several of the activists targeted by DarkMatter were subsequently arrested and imprisoned, or convicted in absentia by the UAE Government.
- Nexa Technology (formerly known as Amesys), which, according to an investigation by the French news organization Mediapart, sold bulk internet monitoring technology to the governments of Egypt and Libya, resulting in the arrest and torture of human rights activists who were identified via their intercepted electronic communications.
- NSO Group, which, according to investigations by the Citizen Lab and Amnesty International, provided hacking software to Saudi Arabia, the United Arab Emirates, Mexico, Morocco, Bahrain, and other governments, resulting in those countries hacking into the devices of journalists and human rights activists. These researchers revealed that U.S.-based journalist Jamal Khashoggi's associate Omar Abdulaziz, as well as Khashoggi's wife, fiancée, and son, were targeted with NSO's software both before and after his murder.
- Trovicor, which provided bulk internet monitoring technology to Bahrain. According to Bloomberg, this was used to intercept communications of activists who were then jailed and tortured.

Thank you for your attention to this serious matter. We look forward to your timely response.

Sincerely,



Ron Wyden
Chairman
Senate Committee on Finance



Adam B. Schiff
Chairman
House Permanent Select Committee
on Intelligence

Christopher S. Murphy
United States Senator

Gregory W. Meeks
Chairman
House Foreign Affairs Committee

Brian Schatz
United States Senator

Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform

Chris Van Hollen
United States Senator

Tom Malinowski
Member of Congress

Edward J. Markey
United States Senator

Anna G. Eshoo
Member of Congress

Gerald E. Connolly
Member of Congress

Jamie Raskin
Member of Congress

Joaquin Castro
Member of Congress

Sara Jacobs
Member of Congress

Katie Porter
Member of Congress

Ro Khanna
Member of Congress

Stephen F. Lynch
Member of Congress

Ted W. Lieu
Member of Congress