

Congress of the United States

Washington, DC 20515

September 29, 2022

The Honorable Antony Blinken
Secretary
Department of State
2201 C Street NW
Washington D.C. 20500

The Honorable Gina M. Raimondo
Secretary
Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

Dear Secretary Blinken and Secretary Raimondo,

In July, the House Permanent Select Committee on Intelligence (HPSCI) held an open hearing on the substantial national security risks and civil liberties challenges posed by foreign commercial cyber surveillance technology (commonly referred to as spyware). We heard testimony from three witnesses, including Carine Kanimba, a U.S. citizen and daughter of Rwandan activist Paul Rusesabagina, who was a target of foreign commercial spyware that was able to track her movements, correspondence, and even likely record her private conversations with U.S. and foreign officials. Forensic analysis has also revealed that the family members and friends of journalist Jamal Khashoggi were targeted with spyware in the months leading up to his brutal murder. We are deeply concerned by the unethical uses of this technology, particularly when it targets U.S. citizens and residents. As part of our continuing oversight, we request that you provide specific details as to the steps the State and Commerce Departments are taking not only to protect U.S. citizens and residents, but also to hold accountable companies that proliferate this malicious weapon and foreign governments that are misusing it.

The *Fiscal Year 2023 Intelligence Authorization Act* (IAA), passed out of our committee on a unanimous bipartisan basis. The bill includes a major new provision to address the threat of commercial spyware. In addition to directing classified reporting requirements and additional resources to the Intelligence Community, the bill would provide authority for the Director of National Intelligence to bar any IC contract with foreign spyware companies and authorizes the President to put in place sanctions on foreign commercial spyware firms that target the IC.

We need to prevent foreign governments, that now have the ability to access information on an individual's phone, tablet, or computer, undetected, from misusing this tool and violating the privacy of U.S. citizens. Toward that end, we strongly urge you to take steps to protect our citizens from becoming targets of this easily exploited technology including by monitoring the activities of spyware companies added to the Commerce Department's Entity List, as well as adding other companies that abuse this technology to this list, suspending U.S. foreign assistance to foreign governments that target Americans with foreign commercial spyware, and working with democratic countries to ban the import and use of such spyware. We request that you take necessary steps and provide us with timely updates on how the Department of State is addressing these threats.

Although some foreign governments have used commercial spyware within the bounds of their constitutions and rule of law, over the past year there have been numerous reports that many governments are exploiting this technology to target opposition leaders, activists and human rights defenders, journalists, civil society leaders, businesspeople, academics, and foreign leaders. As a consortium of researchers recently highlighted in a public letter to you and other Cabinet officials, some of these abuses appear to have occurred even after the Commerce Department added several spyware companies, including NSO Group, to its Entity List. State and Commerce must be vigilant in monitoring the abuses of companies on the Entity List, ensuring they are not evading the bans, and work together to add other spyware companies to the list if they meet the criteria.


However, the Entity List designation is not enough. We recognize that spyware is not going away; it will almost inevitably evolve and become more readily available, cheaper, and more widely used. We are gravely concerned that this technology will become accessible to non-state actors, such as terrorist groups, criminal cartels, or paramilitary groups and militias. A whole of government response is necessary to combat this rapidly emerging threat to the privacy of everyday Americans. We encourage you to apply pressure, particularly on those foreign governments that are recipients of U.S. assistance and continue to abuse this technology or use it to target U.S. citizens and residents. The American people's tax dollars should not be going to foreign governments that target our own people.

We also are gravely concerned by public reports that foreign commercial spyware has been used against U.S. diplomats overseas. This attack may have put at risk individuals who engage with our diplomats on a regular basis and underscores the counterintelligence threat to U.S. government personnel and systems posed by this weapon. We request that you detail publicly any instance in which foreign spyware has been used against our diplomats, and what steps State is taking to confront these unacceptable abuses, including by imposing costs on foreign governments or persons that targeted our personnel.


Even as the threat posed by spyware is rapidly evolving, we believe there is a window of opportunity to prevent its further spread and misuse. Consistent with State's efforts to counter transnational repression, we encourage you to bring together democratic countries on the margins of other international convenings, including the United Nations General Assembly this month and the Biden Administration's second Summit for Democracy later this year, to reach an understanding to ban the use of foreign commercial spyware. Such a strong message would dissuade investors from backing spyware companies and complement efforts by U.S. technology companies to protect the privacy of billions of people. We look forward to receiving more information on what steps are being taken on this line of effort.

Clear and determined action needs to be taken to send the unequivocal message to foreign governments who have acquired commercial spyware that the targeting of Americans and exploitation of this technology will not be tolerated. We appreciate your attention to the pressing and sensitive matter of protecting U.S. citizens and defending our national security interests.


Sincerely,




James A. Himes
Member of Congress




Jackie Speier
Member of Congress




Val Butler Demings
Member of Congress



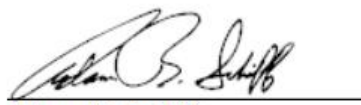
Jason Crow
Member of Congress




Brian Fitzpatrick
Member of Congress




Mike Quigley
Member of Congress




Adam B. Schiff
Member of Congress




Joaquin Castro
Member of Congress




Peter Welch
Member of Congress




Eric Swalwell
Member of Congress




Sean Patrick Maloney
Member of Congress




Jim Cooper
Member of Congress



Raja Krishnamoorthi
Member of Congress



André Carson
Member of Congress



Chris Stewart
Member of Congress