UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

To the Attention of the Blackstone Group L.P. Board of Directors:

Mr. Stephen A. Schwarzman
Mr. Hamilton ("Tony") E. James
Mr. Jonathan D. Gray
Mr. J. Tomilson Hill
Mr. Bennett J. Goodman
Mr. James W. Breyer
Mr. Peter T. Grauer
Mr. Richard Jenrette
Ms. Rochelle B. Lazarus
Mr. Jay Light
The Right Honorable Brian Mulroney
Mr. William G. Parrett

July 25, 2017

I am writing regarding recent reports that Blackstone Group is in talks to acquire a $400 million, 40% stake in the Israel-based firm NSO Group Technologies. Spyware designed, marketed and sold by NSO Group is used by government customers to remotely exploit, infect, and monitor phones running Apple iOS and Google's Android operating systems.

The purpose of this letter is to alert you to investigations conducted by the research group I direct, the Citizen Lab, as well as by respected news organizations and civil society groups in several countries. The results suggest a lack of due diligence by NSO Group concerning the sale of their spyware, and widespread misuse of NSO's spyware by several of its government clients. We outline these concerns below.

These findings include reported cases of misuse and abuse of NSOs' spyware by customers, including cross-border targeting within the United States, the targeting of at least one American citizen, impersonation of the United States government, and the targeting of a minor. Moreover, NSO's exploit infrastructure includes domains that spoof a wide range of international bodies and companies, ranging from the International Committee of the Red Cross, to Google Inc., and the UK Government's visa application portal.

Civil society organizations and others have called into question whether some of these activities were in violation of United States and Mexican law, as well as international human rights law. Reports on the misuse of NSO spyware have triggered at least one formal government investigation, which is ongoing, and calls for further investigation internationally.

We urge you to carefully consider the human rights and ethical implications of an investment in a spyware company such as NSO Group, the products and services of which have turned up in numerous high-profile instances of politically-motivated digital targeting. We also raise questions regarding the due diligence conducted by Blackstone concerning NSO Group, to which we would appreciate your timely response.

At Trinity College
1 Devonshire Place, Toronto, ON
Canada M5S 3K7
T: 416-946-8900 F: 416-946-8915

At the Observatory
315 Bloor Street West, Toronto, ON
Canada M5S 0A3
T: 416-946-8929 F: 416-946-8877

www.munkschool.utoronto.ca

Use of NSO Group's Spyware to Target Civil Society

The Citizen Lab, an interdisciplinary research laboratory based at the University of Toronto's Munk School of Global Affairs, has published a total of five reports since 2016 on NSO Group's spyware. Our organization's research outlines strong evidence that NSO Group's spyware was sold to customers with a known history of abuse of spyware, and subsequently used by those actors in apparent violation of international human rights law and applicable national laws. The reports include the following findings (each with the corresponding report date):

Targeting of an Award-Winning Human Rights Activist

- On **August 24, 2016**, Citizen Lab demonstrated that NSO Group's spyware had been used by one of its customers in the United Arab Emirates to target Ahmed Mansoor, an award-winning human rights defender (Citizen Lab, New York Times). Mr. Mansoor, currently imprisoned in the UAE, is identified as a prisoner of conscience by Amnesty International.
- Prior to the sale of spyware by NSO Group to the UAE customer, the UAE had gained international notoriety for using spyware made by two other foreign companies to target Mr. Mansoor in 2011 and 2012, such that its ongoing misuse of commercial spyware was wholly foreseeable.
- NSO Group's "exploit infrastructure," named "Pegasus," included domains spoofing a wide range of legitimate entities. NSO has never publicly clarified its role in registering and maintaining these domains (Citizen Lab, New York Times). Such domains attempt to spoof, among others:
    - The International Committee of the Red Cross
    - Government service portals, such as the United Kingdom's visa application portal
    - Facebook Inc., Google Inc., Federal Express Inc., and Turkish Airlines
    - News organizations such as CNN, The BBC, Al Jazeera, and Univision

Targeting of Public Health Campaigners and a Federal Scientist

- On **February 11, 2017,** Citizen Lab researched showed that NSO Group's spyware was used to target public health campaigners and a federal scientist in Mexico (Citizen Lab, New York Times).

Targeting of Journalists, Families, and Anti-Corruption Advocates

- On **June 19, 2017,** Citizen Lab investigations showed that journalists, lawyers representing families of missing students, and anti-corruption advocates in Mexico were targeted with NSO Group spyware (Citizen Lab, New York Times).
- Targets included at least one US citizen, as well as a minor child located in the United States.
- Targeting activities included impersonating the United States government, including to target an individual located within the United States. Targeting using NSO Group's spyware also included impersonating alerts from the AMBER alert system, a service designed for the protection, location, and rescue of kidnapped children.

Targeting of Political Leadership

- On **June 29, 2017,** Citizen Lab demonstrated that prominent Mexican politicians, including the president of Mexico's Senate and the president of the PAN political party, were targeted using NSO Group's spyware (Citizen Lab, The Guardian).

Targeting of Forensic Investigators

- On **July 10, 2017,** Citizen Lab verified that NSO Group's spyware was used to target the Interdisciplinary Group of Independent Experts (GIEI), an international body of forensic investigators under the Organization of American States with diplomatic status investigating a mass disappearance in Mexico (Citizen Lab, NY Times Report).

Reporting and investigation by organizations including R3D, SocialTic, Article 19, and Privacy International—as well as dozens of media outlets internationally—have uncovered additional details that suggest a lack of due diligence and/or a failure of know-your-customer policies on the part of NSO Group, and possible legal violations by NSO Group's customers.

Collection and Sale of Known Software Vulnerabilities and a Failure to Responsibly Disclose

Services provided by NSO Group include the sale of so-called "zero day" exploits, which enable the remote infection of commercially available electronic devices. These exploits make use of undocumented vulnerabilities in commercial software and operating systems developed by companies that serve consumers worldwide, such as Apple Inc.. Instead of responsibly disclosing information about these vulnerabilities to software companies, however, NSO Group sells solutions which exploit them to customers in United Arab Emirates and elsewhere. These zero-day exploits were used to target the abovementioned individuals, and failure to disclose their existence may have left upwards of hundreds of millions of users at risk.

When researchers at Citizen Lab, in collaboration with security firm, Lookout Inc, discovered a set of three zero-day exploits used by NSO Group, Apple Inc. was forced to urgently develop and deploy a security update for the approximately one billion users of Apple iOS and OS X operating systems. Google Inc. has conducted its its own investigation into this issue, referring to NSO Group's Android technology as both "malware" and "spyware." Lookout Inc. has also separately investigated NSO Group's technology targeting Android devices.

Investigations and Calls for Investigation

In light of the serious human rights concerns raised by the use of NSO Group technology, a number of international bodies have called for investigation, and at least one investigation is presently ongoing:

- The Mexican Government's Office of the Prosecutor (PGR) is currently conducting an investigation into the abuse of NSO Group's spyware in Mexico;
- Independent United Nations experts have issued a joint statement calling for a full and impartial investigation into the abuse of NSO Group's spyware and calling for an immediate end to the surveillance of civil society actors;
- UNESCO's World Association of Newspapers and News Publishers (WAN-IFRA) has called for an investigation into the abuse of NSO Group's spyware;
- European Members of Parliament have called for an international commission to investigate the abuse of NSO's spyware.

Blackstone's Commitment to Responsible Investment

Blackstone Group has made public commitments to a range of corporate social responsibility, ethics, transparency, and responsible investing principles. For example, Blackstone Group has highlighted its collaboration with the Private Equity Growth Capital Council (PEGCC), whose Guidelines for Responsible Investment require the consideration of social issues, compliance with local law, and respect for human rights.

Blackstone Group also states that the firm performs an analysis that includes the relevant "social issues" for all investments throughout the engagement period.

Questions about the Potential NSO Group Acquisition

In the spirit of Blackstone's commitment to transparency and principles of responsible investment, and given the serious human rights implications of the products and services offered by NSO Group, we respectfully request clarification on whether Blackstone has:

- Conducted due diligence into NSO Group's human rights-related policies, if any, including its know-your-customer policies;
- Conducted due diligence into the human rights impact of NSO Group's products and services;
- Requested and received a full list of NSO Group's government customers, including customers in countries where a high risk for human rights abuse is present;
- Requested and received information about NSO Group's compliance with export regulations covering their spyware;
- Requested and received sufficient clarification related to the widely-reported cases described above in which NSO Group spyware was abused;
- Requested and received sufficient clarification about what steps, if any, NSO Group has taken to address these reported cases;
- Requested and received clarification about NSO's potential exposure to criminal and civil liability in the jurisdictions in which it operates, given these reported cases.

Questions concerning Risks and Commitments to Investors

Several of the reported abuses described above have called into question whether the activities of NSO Group and its customers are in compliance with domestic and international law. A potential investment in NSO Group also raises serious issues related to the commitments Blackstone Group has made regarding responsible investing to its shareholders.

- Has Blackstone Group conducted an analysis of the potential risks associated with investing in a company whose spyware has been used to target human rights defenders, journalists, and other civil society actors, as well as to impersonate internationally-recognized companies and other entities?
- Has Blackstone Group evaluated the potential risks associated with the sale of exploits related to consumer software and operating systems?
- Does Blackstone intend to disclose their assessment of such risks, if any are found, to its shareholders?
- What steps will Blackstone take to ensure that this acquisition will not violate the principles of corporate social responsibility, responsible investment, ethics, and transparency to which Blackstone subscribes?
- Does Blackstone intend to disclose information about the abuses involving NSO Group spyware, as described above, to its investors?
- Given Blackstone's commitments to corporate social responsibility, does Blackstone have any specific policies or ethical guidelines concerning investments in firms such as NSO Group that sell zero-day exploits and surveillance technology?

Should an Investment Take Place

What steps does Blackstone plan to take, should an acquisition go forward, to ensure that NSO Group meets Blackstone's high standards for corporate social responsibility? For example, does Blackstone intend to place an individual on the board of NSO Group?

Thank you in advance for your attention to this matter.

Sincerely,

Ronald J. Deibert
Director of Citizen Lab
Professor of Political Science
Munk School of Global Affairs
University of Toronto