

Dipanjan (DJ) Deb
Co-Founder and Chief Executive Officer
Francisco Partners
One Letterman Drive
Building C - Suite 410
San Francisco, CA 94129
Via e-mail: deb@franciscopartners.com

November 1, 2018

Dear Mr. Deb,

We are writing to you with new findings on NSO Group, a company in which we believe Francisco Partners has a [majority stake](#). In light of these additional findings, which detail with high confidence how NSO Group's Pegasus spyware is being used to spy on civil society activists in Canada and elsewhere, we hope that Francisco Partners will engage in a constructive dialogue with Citizen Lab regarding Francisco Partners' human rights due diligence processes and compliance with the [UN Guiding Principles on Business and Human Rights](#).

New Findings on NSO Group

As you may be aware, Citizen Lab recently released two reports concerning your portfolio company NSO Group: "[Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries](#)" ("*Hide and Seek Report*" published on September 18, 2018) and "[The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil](#)" ("*The Kingdom Came to Canada Report*" published on October 1, 2018).

The *Hide and Seek Report* describes new Internet scanning techniques that identified likely NSO Group Pegasus spyware infections in 45 countries, with 36 probable government operators. Pegasus appears to be in use by multiple countries with dubious human rights

munkschool.utoronto.ca



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 0A7
T: 416.946.8929 F: 416.946.8877

At the Canadiana Gallery
14 Queen's Park Crescent West
Toronto, ON
Canada M5S 3K9
T: 416.978.5120 F: 416.978.5079

records and histories of abusive behaviour by state security services. Moreover, pertinent to the question of NSO Group's responsibilities in addressing and preventing abuses of its product, at least six countries identified in the report as suspected Pegasus operators are known to have used spyware to target civil society in the past: Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates.

The *Kingdom Came to Canada* report assesses with high confidence that the phone of Omar Abdulaziz, a Saudi activist, university student, and Canadian permanent resident located in Quebec, was infected with Pegasus spyware. Based on the evidence gathered through our research, it is probable that the operator of the spyware is linked to Saudi Arabia's government and security services. In addition, [the same Pegasus operator](#) has been linked to the targeting of an Amnesty International researcher and a Saudi blogger.

The apparent sale by NSO Group of Pegasus spyware to Saudi Arabian government entities is alarming: while Saudi Arabia's human rights record has long been abysmal, the Saudi government has taken increasingly aggressive action demonstrating a blatant rejection of human rights obligations in the face of international criticism. Such action includes the [premeditated murder](#) of Saudi dissident journalist Jamal Khashoggi inside the Saudi consulate in Istanbul, Turkey. Notably, Omar Abdulaziz and Jamal Khashoggi [were in contact](#), working together on projects concerning human rights and democracy in Saudi Arabia.

Human Rights Due Diligence and Compliance with the UN Guiding Principles on Business and Human Rights

In a letter dated [February 20, 2018](#) to the Citizen Lab, Francisco Partners explained that it was "very much willing to engage in a constructive dialogue with Citizen Lab on the topic of enhanced corporate governance and social responsibility". In light of the *Hide and Seek* and *Kingdom Came to Canada* reports, and the growing body of evidence that NSO Group's Pegasus spyware is being used for illegal purposes, we are asking Francisco Partners to honour this statement and engage in such a constructive dialogue.

In particular, we ask that Francisco Partners begin this dialogue by describing any measures it has taken to ensure compliance with the UN Guiding Principles on Business and Human

Rights. While we appreciate that Francisco Partners [has stated](#) that it “mandates the adoption of compliant business ethics policies and processes” and works with company management teams on social responsibility policies and processes, these statements were vague, unsubstantiated, and provided no actual insight into Francisco Partners’ compliance practices. We believe that detailed and transparent answers to the following questions could be a useful starting point for this dialogue and would be welcomed by those who invest through Francisco Partners, civil society, and the broader public:

1. What efforts has Francisco Partners made to remedy the apparent failures of oversight in the sales of NSO Group’s spyware to authoritarian regimes like Saudi Arabia?
2. Who at Francisco Partners advises NSO Group on human rights due diligence issues and what advice has been provided?
3. What efforts has Francisco Partners made to ensure that [legitimate users of NSO Group spyware \(or other spyware\) are not also engaging in illegitimate uses](#) of that spyware?
4. What efforts has Francisco Partners made to ensure transparency with regards to its investments in NSO Group, particularly to limited partners investing in this fund?
5. What efforts has Francisco Partners made to ensure that Francisco Partners does not make further investments in companies that produce spyware used for illegal purposes?
6. What efforts has Francisco Partners made to audit its existing investments and ensure that these companies are operating in compliance with international human rights law?
7. Does Francisco Partners solicit external ethics reviews and oversight of its business practices and its portfolio companies?

In addition to the tragic human rights consequences of illegal and abusive uses of spyware, there are significant business risks for Francisco Partners that should further motivate a comprehensive review of the company’s human rights due diligence processes and compliance with the UN Guiding Principles on Business and Human Rights. [Investigations](#) into and [litigation](#) against NSO Group is exposing [indicators and details](#) of the company’s technology that may lead to additional discoveries pertaining to the spyware’s operation and deployment and that ultimately affect the company’s bottom line. Further, from an investment perspective, it is difficult to envision a situation where the value of a company is being enhanced after its products are discovered to have been grossly abused, particularly if the company appears to have taken little action to prevent such abuses.

Conclusion

In the spirit of engaging in a constructive dialogue, as expressed in your letter of [February 20, 2018](#), we hope that Francisco Partners will begin by answering the questions we have asked in this letter. As we noted in our correspondence to you dated [May 29, 2018](#) (which remains unanswered), unsubstantiated references to business ethics and social responsibility do not address the serious human rights impacts of your portfolio companies. In light of the gravity of the situation in Saudi Arabia and NSO Group's links to that authoritarian regime, we hope that detailed, transparent, and substantiated answers will be forthcoming shortly.

Sincerely,



Ronald J. Deibert, OOnt

Professor, Political Science Department, University of Toronto

Director, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto