

February 18, 2021

Dear Professor Deibert:

We received your letter of January 11, sent in response to our December correspondence. Though your letter does not express any interest on your side to enter any real dialogue to further the important idea of proper use of cyber intelligence tools, nor any willingness to provide information which can assist in our investigating this matter, we have provide below a detailed explanation of our activities in this regard to refute your unfounded claims as to the seriousness of our actions.

### *Background*

By way of background, NSO Group was founded in 2010 with a simple mission: to make the world a safer place by developing technologies that lawful governments can use to investigate and prevent major crimes and terrorism. In a perfect world, tools such as those developed by NSO would not be needed. The world we live in, however, has terror organizations, drug cartels, human traffickers, pedophilia rings and criminal syndicates who aggressively exploit off-the-shelf encryption capabilities offered by mobile messaging and communications applications. These technologies provide dangerous criminals and their networks a safe haven, allowing them to “go dark” and avoid detection, communicating through otherwise impenetrable mobile messaging systems. As a result of such criminal behavior, law enforcement and counterterrorism government agencies around the world are often unable to stop dangerous criminals as they plot and execute their nefarious plans against innocent civilians.

To counter this threat, NSO Group has developed a technology that it licenses to law enforcement and intelligence agencies to collect target-centric data from the mobile devices of suspected major criminals. These government agencies use the technology to monitor the messaging systems that suspected terrorists and criminals use. This technology has been used by governments to prevent serious crimes and save lives on a massive scale. With the technology, government agencies have thwarted terrorist attacks, captured and brought pedophiles to justice, broken up criminal organizations and drug trafficking rings and freed kidnaping victims.

The technology, however, is highly limited in scope. It may be used by our customers only with specific, pre-identified phone numbers when the law enforcement or intelligence agency has a specific target of interest and the technology is aimed directly at them. In many ways, the technology is similar in concept to a traditional wiretap. Instead of listening to specific telephone conversations, it helps law enforcement monitor mobile messaging, offering legitimate law enforcement and intelligence operations personnel a window into the activities of previously identified and targeted criminal actors on an individual basis. The technology cannot be used to gather information broadly in the manner of mass surveillance and does not penetrate computer networks, desktop or laptop operating systems, or data networks.

The technology is overwhelmingly used by governments as intended, and we work hard as a company to conduct our business ethically and responsibly and take active steps to prevent its

misuse. We are committed to the UN Guiding Principles on Business and Human Rights, and have implemented a robust governance framework. That framework codifies NSO's commitment to ethical business, and integrates human rights safeguards into all aspects of our work – from the design to the licensing for the use of our products. While other surveillance technologies have been developed by governments and companies in China, Russia, Italy, and elsewhere, we are perhaps the only company in the surveillance industry to have such a thorough governance framework, or even to commit to the UNGPs.

Of course, we are aware that, as with wiretaps, messaging intercepts can be inappropriately used, and our governance framework will not prevent all abuses by our customers. We can and do put in place technological limitations that limit any customers' ability to alter the intended use of the system and the customer has no ability to extract the technology to be used for other purposes or to transfer the system to another user. We also are aware that since NSO does not operate the system, but only licenses the technology to governments to use, those risks are higher. Nor does NSO know which specific suspected criminals are targeted after it has been licensed by government customers.

To mitigate those risks, as part of our governance framework, we take concrete and specific steps, consistent with international standards, to address those risks. We license the technology only to select, approved, verified and authorized government agencies, specifically to be used in national security and major law enforcement-driven investigations. We conduct due diligence on those users to assess the risks of misuse, do not license technologies to customers where the risk of misuse is too high, and have expansive contract terms to mitigate potential misuse. We actively investigate all concerns that arise, utilizing independent resources, and take action depending on the results.

In addition, we operate under close regulatory scrutiny. The Defence Export Controls Agency (DECA) of the Israeli Ministry of Defense sharply restricts the licensing of our technologies, mandating that NSO Group follow the principles in our governance framework. While we acknowledge that even with our framework and DECA's regulatory oversight risks of misuse remain, we believe our approach is thorough, strong and best practice in our industry.

#### *Citizen Lab's Assertions*

Citizen Lab asserted that it does not believe that we take our responsibility to respect human rights seriously, citing in part statements made by Professor David Kaye, and that it does not believe we will undertake a thorough investigation into allegations that a customer has misused our technology to target journalist Rania Dridi and journalists from *Al Jazeera*. This is completely, baseless and untrue.

We are disappointed with the unfounded lack of confidence that Citizen Lab has expressed in our compliance efforts. We reached out to you in a sincere effort to fully conduct an investigation of the allegation raised in your report. As you know, we have repeatedly expressed our desire to work collaboratively with you towards our mutual goal of assuring that these types of systems are not misused to violate human rights. We would have expected that an organization that has so clearly expressed a desire to conduct unbiased research, and strategic policy and legal engagement at the intersection of communication technologies, human rights, and global

security, would be interested in a dialogue with the leading company in this sphere both from the technical aspect and that of being a leader in its unprecedented compliance policies and efforts. I hope we are not mistaken.

Over the past 15 months, NSO Group has taken significant steps to increase the robustness of its human rights framework. Consistent with the U.S. 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," NSO has specifically integrated human rights elements into its business processes to help identify, prevent, and mitigate risks of misuse of its products. As the Guidance recommends, before any sale takes place, we consider the nature of our products and the likelihood that they may be misused by a customer in a manner that violates human rights. We review the human rights record of our potential customers, relying on a variety of external data sources focused on rule of law, political stability and corruption for the country in question. All of our customers have many legitimate needs for the use of the systems in fighting terror and serious criminal activity and are part of the international community's coalitions to achieve these goals. We also consider the laws and regulations of the countries where our products are licensed. As a result of these steps, we have declined numerous opportunities where we determined the inherent risk of misuse was unduly high. My confidence in the integrity of these processes is high, since – as head of compliance – they are my responsibility. Moreover, when I benchmark our efforts against others in this arena, I came to realize that we are much more advanced in our process than any other company in the intelligence world.

Also consistent with the Guidance, in connection with sales, we have expansive contractual provisions designed to help prevent misuses. Specifically, we require the technology to be used only where there is a legitimate law enforcement or intelligence-driven reason connected to that specific number. All customers must agree to respect human rights and adhere to human rights norms. Use of our technology against law-abiding citizens is prohibited, and customers certify that they will use our products responsibly. Our contracts make clear that we may suspend or terminate customers who fail to fully comply with applicable domestic laws and regulations or fail to respect human rights, including the rights to privacy and freedom of expression. We also limit the number of instances in which the technology can be used, which also reduces the risk it will be used for reasons other than legitimate enforcement of significant criminal conduct.

After a sale is completed, also consistent with the Guidance, we closely monitor various forms of media and seek continuous feedback on the use of our products. We conduct periodic reviews that include open-source intelligence gathering, periodic meetings between compliance and business team members, and in-country visits by NSO Group compliance personnel with customer personnel. NSO also has internal and external whistleblower processes that allow for anonymous reports of violations both within the company and by its customers. Where credible concerns arise that our products might have been misused, we have developed a detailed investigative protocol, requiring that we investigate concerns, seek outside assistance as appropriate, and report to the Governance, Risk and Compliance Committee of our board. We have used that protocol repeatedly, conducting investigations around the world into allegations that government agencies have used the technology for reasons other than to investigate serious potential crimes. Again, as responsibility for investigations fall within my remit, I can attest to the seriousness with which they are taken.

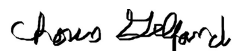
Following investigations, we have terminated customers and barred their future use, restricted the use of others, and instituted additional mitigating measures regarding others. We actively seek to learn from these matters, continually looking for ways to improve our framework, policies and procedures to prevent future misuses. As an example, through this process, we have begun implementing human rights training that end-users must complete in certain circumstances to ensure that our customers understand our human rights-related expectations.

*Further Engagement*

We recognize, that despite our best efforts, there is no foolproof mechanism to assure that customers do not violate their obligations and misuse our products, and thus improperly invade the privacy and chill the free expression. However, the goal of our human rights framework is to do the maximum that we can to mitigate those misuses, and ensure that our products are used consistent with their intent: to prevent terrorists and violent criminals from succeeding in their plots. To that end, we regret that Citizen Lab declined to provide even the most basic cooperation to assist our investigation of this matter and repeatedly has declined to meet with us to discuss these issues. Nevertheless, we are always open to engage in a constructive discussion about our program, discuss our approach, and, frankly, consistently improve our compliance program. If your agenda is legitimately geared towards protection of Human Rights, we would expect that you support these efforts.

As Citizen Lab's has claimed confidentiality obligations as a reason for declining to cooperate, we also have confidentiality obligations of our own, particularly as our customers use our products in the course of sensitive undercover investigations. We shall continue conducting a thorough and fulsome investigation, as we do in all matters of this sort, irrespective of whether or not you shall decide to cooperate.

Best Regards,



Chaim Gelfand