June 1, 2020

VIA ELECTRONIC MAIL
ATTN: MR. DAVID KAYE
Special Rapporteur

Mr. David Kaye
UN Special Rapporteur On the Promotion and Protection of the Right to Freedom of Opinion and Expression
United Nations Human Rights Office of the High Commission
Palais des Nations
CH-1211 Geneva 10, Switzerland

Re: **NSO Human Rights and Whistleblower Policies Response to February 20, 2020 Letter**

Dear Mr. Kaye:

NSO Group Technology ("NSO") writes in response to your letter dated February 20, 2020, requesting additional clarification regarding its Human Rights and Whistleblower Policies. Of course, as you are aware, the obligation to combat terrorism and other serious crimes, and protect human rights, rests with States. As we explained in our original letter to you of December 10, 2019, NSO develops and licenses to States and State agencies technologies intended to allow States to meet those obligations. NSO thus is in many respects similar to a traditional defense contractor, while also assisting states in their efforts to "protect against human rights abuse within their territory and/or jurisdiction by third parties," as provided by Principle 1 of the UN Guiding Principles on Business and Human Rights (UNGPs).

NSO is committed to being transparent in its approach, particularly given the absence of best practices that appropriately balance critical government crime prevention efforts that protect human rights, with our industry's responsibility respect for privacy and other human rights. NSO thus welcomes the opportunity to provide further details about how it strives to strike that balance.

As we made clear in our prior correspondence, NSO continues to develop, tailor, and refine its Human Rights Program, receiving advice and input from a variety of experts in differing disciplines. The policies and procedures that help shape the program are designed to maximize the likelihood that NSO's products are used consistent with their intent – to prevent dangerous and life-threatening criminal activity – while mitigating the risk that users engage in unlawful and arbitrary interference with rights to privacy, or infringements of freedom of expression. Of course, unlike a state, we cannot as a private actor monitor the real-time usage of government law enforcement and intelligence agencies. Thus, our focus is on pre-contracting due diligence, risk identification and mitigation, investigation of alleged misuses, and post-engagement scrutiny to gain a level of comfort surrounding the proper use of our products. As our prior letter further made clear, NSO also is subject to Israel's export control and other legal requirements, which provide further restrictions on potential customers and engagements, as well as permitted uses.

Due Diligence Process

Most notably since our last letter, we have adopted a human rights due diligence procedure that applies to all future engagements and renewals, and we would be glad to consider further improvements in light of any insights you might be able to provide. In this context, in our desire to continually improve our program, we would greatly appreciate any insights into other programs that in your view have addressed some of the points you mention in your correspondence. For instance, we would be grateful if you could point us to corporate due diligence frameworks that you believe could serve as a model for industry standards; where we might look to identify aspects that could strengthen our approach; or examples of contractual provisions that you believe are sound, or where other companies have determined that end-users committed material breaches such that we might consider adjusting the standards and definitions in our processes and contract terms. Similarly, are there specific limitations or controls that you consider effective or promising? While we likewise seek to be as transparent as feasible with all stakeholders, we would appreciate any specific thoughts you might have regarding how the disclosure of information you request should be balanced against state confidentiality concerns, government efforts to prevent threats to national security, or legitimate law enforcement efforts. We gladly would consider any details into good practice that you might be able to provide.

At the moment, our human rights due diligence consists of a multi-step process. *See generally* UNGP 19. As you are aware, NSO's customers are States and governmental agencies. Under the procedure, when a new opportunity arises, which can range from a general possibility

to engage with a State or State agency, NSO conducts a human rights-focused country-level assessment. This includes the prospective country's human rights record, as well as its perceived respect for the rule of law and freedom of speech, political stability, and level of corruption. That analysis relies on a number of authoritative public indicators, such as the World Bank Worldwide Governance Indicators and the Transparency International Corruption Perception Index. At this initial stage of review, NSO also considers the nature of its product and its potential for misuse – as NSO has a wide portfolio of products with varying potential risks of misuse – NSO's prior relationship with the entity that will use its products, the credibility of that entity and its defined mission, the duration of potential use, and other factors which could potentially increase or decrease human rights risks.

At the conclusion of this initial stage of review, NSO's compliance team categorizes the opportunity according to the risks of potential negative human rights impacts. As a rule, NSO does not pursue opportunities where the human rights risks are unduly high, and thus the process could stop here. If the process does proceed, NSO conducts additional diligence steps. The specific steps taken differ depending on the level and nature of potential risk, but they generally include a review by an external risk and investigation firm, an assessment of adverse public information, and a detailed analysis of the domestic legal framework. Among the legal issues analyzed are whether domestic standards and protections are consistent with International Covenant on Civil and Political Rights Articles 17 and 19,[1] including the accessibility of the law, the clarity of the law, the foreseeability of the impact, and other essential factors identified by human rights courts and tribunals. That includes, for instance, an examination of the definition of the nature of offenses giving rise to secret surveillance and categories of people susceptible; any limits on the duration of surveillance; procedures to be followed when examining and using the data; precautions taken when communicating the gathered intelligence to other parties; circumstances in which data may be destroyed; and whether surveillance requests must be approved by an independent authority with relevant standards guiding his or her decision-making. *See Zakharov v. Russia*, App. No. 47143/06 (ECHR Dec. 4, 2015); *Case of Big Brother Watch and Others v. the United Kingdom*, Applications Nos. 58017/13, 62322/14, 24960/15 (ECHR April 2, 2019).

[1] ICCPR Article 17 provides: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; 2. Everyone has the right to the protection of the law against such interference or attacks." ICCPR Article 19 states: ". . . 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary … (b) For the protection of national security or of public order (ordre public), or of public health or morals."

In addition, at this point of the process, further information might be obtained directly from the anticipated user, depending on the nature of the situation and the potential risks identified. When that information has been accumulated, NSO may consult with external experts and advisors to determine the appropriate course of action. That includes potential measures that reasonably may be employed to prevent and mitigate the risks of misuse and negative impacts if the engagement proceeds. If the risks, even with mitigating measures, are deemed unduly high, NSO will terminate discussions and the engagement will not proceed.

If the engagement proceeds, NSO's contracts will include, at a minimum, detailed Human Rights provisions that are consistent with NSO's Human Rights Policy, an ability to suspend NSO's systems upon suspected misuse, and an agreement to cooperate in any investigation into potential misuse. These provisions help provide confidence that, regardless of the domestic framework, users are abiding by our standards, which are consistent with human rights norms. NSO also may seek additional remediation measures, such as representations and warranties from users, insist on a shortened contract duration, request that users undergo human rights training, and other steps. *See* OHCHR Response to Request from BankTrack for Advice Regarding the Application of the UN Guiding Principles on Business and Human Rights in the Context of the Banking Sector, June 12, 2017, at 9 ("Carrying out due diligence appropriate to the scope and complexity of a [company's] portfolio and risk picture should help it effectively identify risks and prevent them from occurring" and it should "clearly communicate their human rights expectations to clients and other business partners.")

Furthermore, our systems are configured in a manner that limits the use by our customers, to a specified duration, to a limited number of concurrent targets, and in specific regions, to minimize risks of misuse.

Finally, NSO monitors and reviews the due diligence of all entities that use its technologies both on an ongoing and periodic basis. *See* OHCHR Response to Request from BankTrack, at 9 ("due diligence in the UNGPs is a continuous, ongoing, iterative process") This may include engagement with NSO's customer or user representatives, media searches for adverse information, updated reviews of due diligence reports, meetings with the end-user personnel, and in-country visits by NSO's legal and compliance team.

NSO takes several steps in instances where NSO's technologies as suspected of being used in a manner inconsistent with domestic law, international norms, or the contract. NSO generally suspends use of the technology and investigates the potential misuse. It also may obtain further legal advice, consult with external experts, and pursue additional efforts.

Where misuse is identified, NSO generally suspends use of the technology and investigates the misuse. It also generally will seek to use the leverage it might possess – consistent with the UNGPs 13, 19 and 22 – to take appropriate action to prevent or mitigate any

adverse human rights impacts. That may include insisting on periodic certifications and declarations prior to maintenance renewals, instituting further product restrictions based on volume and geographic coverage, conducting a review of operational security, requiring End-Users to participate in enhanced training, and other tailored measures. For instance, in recent instances in which NSO has received concerns or complaints regarding alleged misuse, it has immediately stopped the customer's use of the system, conducted a detailed review of the domestic legal frameworks, reviewed the relevant contracts and agreements, and interviewed the users and their legal representatives to understand their processes, protections and perspectives. NSO has reinstated the system only after gaining comfort that the system was not misused. In contrast, in a small number of instances, NSO has terminated contracts and severed relationships with customers after misuses were identified, and will terminate agreements if the user does not cooperate in our inquiries - but this is another area where your insights on sound industry practice would be most appreciated. *See* OHCHR Response to Request from BankTrack, at 8 (a company "may facilitate a client or other entity to cause harm, if it knows or should have known that there is human rights risk associated with a particular client or project, but it omits to take any action to require, encourage or support the client to prevent or mitigate these risks. The [company's failure to act upon information that was or should have been available to it may create a facilitating environment for a client to more easily take actions that result in abuses. Conversely, if the [company] knows about a human rights risk associated with a particular project and takes reasonable steps to prevent and mitigate these risks, the situation would instead in principle be one of 'linkage'.")

It is important to understand, however, that NSO's ability to assess the use of its technologies through System-based inquiries depends on the cooperation of the user, consistent with the quotation from the article you include on page 3 of your letter. Absent customer cooperation, we are limited to reviewing available metadata, which fails to provide detailed insights and does not provide sufficient data to allow one to determine if there was any misuse. When we do receive cooperation from a customer, which is a condition of continued usage of the System, we then can review customer-generated data maintained on the customers system, and try to inspect the usage with information that is highly reliable – consistent with the quoted language. Because certain allegations do not make it clear which user might have improperly targeted a particular person, we may end up contacting multiple customers, and undertaking multiple inspections, in any given inquiry. Reconstructing potential usage of the System after the fact thus can be demanding, and sometimes leads to limited conclusions and less than a full picture. These are all issues that NSO must take into account when reaching a conclusion and final determination regarding any potential misuse.

Whistleblowing Policy

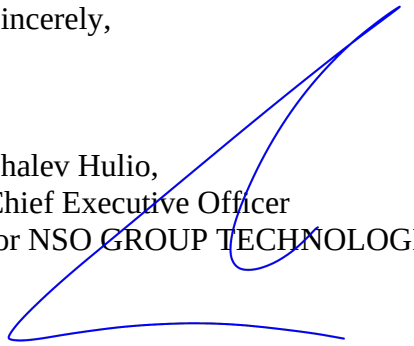
With respect to our Whistleblowing Policy, NSO encourages all employees, business partners, and external stakeholders to report any suspected misuse of NSO's technologies. NSO's Whistleblowing Policy specifically applies to "the inappropriate use/misuse of the NSO Group's products and/or services and resulting human rights impacts by any person, including ... customers...." NSO has a clear and strong non-retaliation policy, and handles each investigation in a manner that tries to preserve the confidentiality of all reporters, witnesses, and other stakeholders. NSO has zero tolerance for any suspected misuses by any of its employees, subcontractors, resellers, or customers.

NSO's Head of Compliance receives, reviews and responds to every report from a whistleblower, and takes steps to prevent the unfair or detrimental treatment of every reporter. The Head of Compliance initiates the preliminary evaluation of the information received, and will attempt to contact the reporter in order to obtain sufficiently specific information to conduct an investigation. The Head of Compliance also will review NSO's existing documentation relevant to the allegation. Once all of this information is analyzed, the Head of Compliance, General Counsel, and other high-level Company personnel will evaluate the report and existing information, and determine whether to proceed with a full investigation, as described above, seek additional information, or stop the review, typically because there is not enough information to proceed.

Conclusion

We hope this clarification helps shed light on our evolving program. As we have noted, we are continuing to refine our approach, and given the span of the programs, we would welcome further constructive guidance you may be willing to offer. Indeed, if you could provide us with an update on any steps to explore industry standards within the industry following your June 2019 report to the Human Rights Council, that would be appreciated. We are disappointed you did not accept our prior invitation to meet at our offices during the month of January, but do reiterate our offer to engage in an open discussion regarding challenges at the nexus of technology and human rights and attendant best practices, including as part of any sector-wide dialogue that you might initiate.

Sincerely,



Shalev Hulio,
Chief Executive Officer
for NSO GROUP TECHNOLOGIES

cc: Beatriz Balbin
Chief

Special Procedures Branch
OHCR

NSO Group Technologies LTD |22 Galgalei HaPlada St. P.O.B 4166, Hertsliya, 4672222, Israel |
Telephone: +972.77.4341292 | Fax: +972.77.4253513 | | Email: office@nsogroup.com