NSO GROUP

December 10, 2019

VIA ELECTRONIC MAIL
ATTN: MR. DAVID KAYE
Special Rapporteur

Mr. David Kaye
UN Special Rapporteur
United Nations Human Rights Office of the High Commission
Palais des Nations
CH-1211 Geneva 10, Switzerland

Re: **NSO Human Rights and Whistleblower Policies**

Dear Mr. Kaye:

NSO Group Technology ("NSO") writes in response to your letter of October 18, 2019, requesting information related to its Human Rights and Whistleblower Policies. NSO develops and licenses to States and State agencies technologies that are intended to prevent acts of terrorism, large-scale drug trafficking, pedophile networks, and other serious criminal acts that threaten life, liberty, safety, and personal security. In so doing, NSO assists States in meeting the expectations of the first Principle of the UNGPs: "States must protect against human rights abuse within territory and/or jurisdiction by third parties." We further strive to respect human rights by our own conduct, and through customer vetting, diligence, and monitoring, seek to mitigate the risk of misuse of NSO products by customers in our value chain as contemplated by *UNGP*s 17-19.

We also are committed to being transparent in our approach. In this vein, we welcome the opportunity, as you requested, to provide further details in relation to our Human Rights Program and Whistleblower Policy.

By way of background, NSO has worked, and continues to work, with its advisors, including human rights, legal, and intelligence experts, to develop an approach to protecting human rights tailored to the specifics of technology suppliers to the lawful interception industry. We adopted a number of new corporate policies in September 2019, including our Human Rights Policy and Whistleblower policies. We are now designing and implementing enhanced procedures and governance structures to ensure full adherence to such policies. We will publish summaries of these procedures along with further policies over the coming months. While our

efforts are very much ongoing, we value your recognition of the steps we are taking and welcome your input.

At the core of our human rights governance is a detailed customer due diligence process building on existing procedures required by our Business Ethics Committee. At the outset of any potential relationship with a customer, we undertake diligence to identify the likelihood of potential human rights risks arising from the misuse of our products. *See UNGP 17*. While we continue to refine our approach, our review includes requests for information to the potential customer, open source research, engagement with relevant experts to assess the reputation and past history of the customer related to human rights and the rule of law, the proposed use of our products, relevant governance standards, and other factors. Our processes are risk-tiered, such that we conduct a more thorough review and require an enhanced level of internal approvals in instances where we believe risks of misuse may be greater. In situations where our review reveals that the risks may be unduly high, we do not pursue the engagement. Further, NSO is subject to Israel's legal limitations on the relationships that we may pursue, which include its own set of human rights protections, providing further restrictions.

When Israeli law permits us to pursue a relationship with a customer and we do not believe the potential for misuse is unduly high, we seek to mitigate relevant risks through a variety of differing steps. *See UNGP 19*. For instance, our licenses are limited in volume, geography, and duration as a means of mitigating risks. Further, our contracts specifically demand that customers utilize our technologies as intended – to investigate and prevent crimes and terrorism – and not to commit human rights violations. Our contracts require that customers immediately notify us of any potential misuse that may result in human rights violations. Our contracts and product design prevent customers from modifying our products in any way or transferring products to another user. Also, a customer's use of our products may be terminated by NSO for any material breach of the contract terms. In fact, NSO has terminated relationships of significant value when we have concluded that customers have failed to abide by our contract. We are presently considering other potential approaches, such as enhanced training, to further mitigate risks to stakeholders.

In addition, we are working diligently with outside experts to identify enhanced approaches for ensuring the appropriate use of our products, despite clear and substantial challenges. Specifically, we are limited by the technological and commercial boundaries of our products to track each specific usage of our products by our customers. Our customers are government security agencies pursuing highly sensitive criminal and national security-related investigations, where operational visibility is simply not permitted. Despite these limitations, we are pursuing other potential approaches, such as certifications of usage that may provide additional confidence that our products are being used as intended in the appropriate circumstances.

Another pillar of our human rights governance is our grievance and investigation policies and procedures. When NSO receives credible information that our products may have been

misused by our customers, we act swiftly. Specifically, we may (and we have in the past) suspend use of the technology, demand responses from customers, engage independent investigators, and/or consult with human rights experts. Where credible evidence of misuse has been found or suspected, we will terminate the relationship and/or undertake other appropriate steps. We also fully cooperate with investigations that may be undertaken by home and host legal authorities. In this vein, as part of remediating potential negative impacts and enhancing our program more generally, you correctly cite our commitment to engaging with "all relevant stakeholders". As our Human Rights Policy indicates, this includes engagement with civil society organizations and vulnerable populations who may be disproportionately affected by our products, including on the basis of "race, color, sex, language, religion, political or other opinions, national or social origin, property, birth or other status or their exercise of human rights". The Policy further references engagement "directly with the individuals affected" in specific instances that may involve a customer's misuse, which may be relevant to remediation efforts and program improvements more generally.

As with other businesses striving to act consistently with the UNGPs, and as indicated in our Human Rights Policy, we will undertake auditing and assessment activities to identify the extent to which we are complying with our own internal policies and procedures, our impacts, and how our program can be improved. While our approach to publishing data related to our operations is still under development, we are guided by *UNGP 21*, and will seek to identify appropriate means of providing public details regarding our assessments, operations, grievances, and other activities, along with a summary of our supporting operational and governance procedures, whilst complying with our contractual and legal restrictions on disclosure.

Specific to our Whistleblower Policy, we are open to receive any information – internal or external – that employees or third parties may wish to provide in relation to our products or their use. Complaints are reviewed by our General Counsel and compliance team for further appropriate action, including the need for independent external investigators, or further details before an investigation can effectively be launched. We specifically prohibit retaliation for reporting concerns in good faith – e.g., concerns that the reporter believes are legitimate. Penalties for retaliation can include discipline up to and including termination. We also take active measures to avoid disclosing the identities of individuals who report anonymously or seek to remain anonymous, to assist in avoiding retaliation by third parties.

We agree, as you indicate, that legitimate concerns can be raised for many reasons. We further agree that the motive of the individual for making a report is distinct from whether the concern itself should be addressed.

We do hope this helps clarify our current approach. As noted, we are continuing to develop our program and processes. Given the span of programs that you observe, we welcome any further constructive guidance your office might be willing to offer. To this end, I would like to extend a personal invitation to you to visit Israel during the month of January 2020 to meet with our management and engage in an open discussion regarding challenges at the nexus of technology and human rights and attendant best practices. Please let us know your availability for such a trip, and thank you again for your letter.

Sincerely,

Shaley Hulio,
Chief Executive Officer
for NSO GROUP TECHNOLOGIES

cc: Beatriz Balbin
Chief
Special Procedures Branch
OHCR