AMNESTY INTERNATIONAL

ANNEX 2

NSO GROUP TECHNOLOGIES LTD. RESPONSE TO AMNESTY INTERNATIONAL LETTER RE: NSO GROUP INTERNAL INVESTIGATIONS

4 OCTOBER 2020

Index number: DOC 10/4187/2021

October 4th, 2020

VIA ELECTRONIC MAIL

Ms. Danna Ingleton
Acting Co-Director - Amnesty Tech
Amnesty International UK

Dear Ms. Ingleton:

We are in receipt of your letter of September 25, 2020, seeking information with regard to NSO Group's grievance and investigation process. We welcome a continued dialogue with Amnesty International and are pleased to be able to provide further information about our processes and approach.

As you are aware, we develop technologies used by government agencies to thwart terrorist plots, violent crimes, trafficking rings, and other major threats to safety and welfare. We understand that, in the vast majority of instances, our technologies are used lawfully, as intended, and without complaint. However, because of the risk of misuse of our products by third parties, we are committed to the establishment of a human rights program that aligns with the UN Guiding Principles on Business and Human Rights (UNGPs). That includes alignment with UNGP 31, regarding operational level grievance mechanisms.

We also note that no other company in our sector has sought to align its processes with the UNGPs, much less developed a human rights program. As a result, we have limited models from which to draw insights in areas that pose particular challenges and no best practices have been established. Nevertheless, we have and will continue to develop and improve our policies and procedures as our experience unfolds. We believe that our commitment and program is, in fact, best in class and it generally aligns with the newly released U.S. State Department Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities. We appreciate our continued engagement with Amnesty International UK, along with any constructive recommendations you may be able to offer regarding our approach.

In response to your questions about our whistleblower processes, under NSO's written procedures, when a concern is lodged, we immediately initiate a preliminary investigation. The preliminary investigation process is overseen by an internal committee comprised of the Chief Executive Officer ("CEO"), Chief Product Officer ("CPO"), and General Counsel. This preliminary inquiry is conducted by our Head of Compliance, typically in consultation with independent outside counsel. As part of this process, at the outset, when the circumstances warrant, we will suspend the customer's ability to use our products until the investigation is

concluded. We then seek to determine whether a full investigation is appropriate, which includes an evaluation of whether the concern raised is technically not possible, there is sufficient information to conduct an investigation, or it is otherwise clear that there was no misuse of our System.

Where the allegation appears credible, we launch a full investigation which shall include all or most of the following steps (as the circumstances warrant), engaging with the customer, commissioning reports from third party due diligence providers, performing technical assessments to the extent possible, analyzing relevant domestic legal requirements, and preparing a written summary of the evidence. This process is overseen by a board-level committee, the Governance, Risk and Compliance Committee ("GRCC"), comprised of one independent Director, the Group CEO, the General Counsel and at least two additional directors. Although discretion in appointing the investigative team rests with the GRCC, investigations generally are handled by our internal compliance team in conjunction with independent external counsel, who provides impartial and objective advice and analysis. The internal team typically is led by the Head of Compliance, who reports to the General Counsel, who also reports to NSO's Board of Directors thus ensuring a level of independence when conducting investigations. Where we determine that a customer has misused our system – whether because they have failed to adhere to procedural protections aligned with interpretations of Articles 17 and 19 or the International Covenant on Civil and Political Rights (as construed by the Office of the High Commissioner on Human Rights, the European Court of Human Rights, and others), or appear to have targeted individuals for reasons inconsistent with legitimate aims under those same Articles or under the terms of our agreement – we take immediate remedial action. Such action can range from termination of the agreement, instituting additional protections, and other steps. Indeed, we have terminated agreements and/or or instituted enhanced remedial protections on previous occasions.

We take this process seriously. Every concern that is raised is subjected to it. We neither presuppose the System has been used appropriately or inappropriately, regardless of past allegations or news reports about the customer, or our past relationship. No restrictions are imposed on individuals who submit grievances, including seeking a waiver of rights, confidentiality as to the concern being raised, or to constrain remediation through alternative processes. While our investigations require engagement with our customers and individuals assisting in our investigation process, our investigations are conducted under legal privilege, and we can and do keep the sources of any concerns and materials generated during the investigation strictly confidential. We take all reasonable steps to prevent retaliation against and preserve the rights of privacy of those who report potential misuse of NSO products, although certain identifying information about the alleged target or device must be disclosed in order to conduct an investigation. We also maintain a strict non-retaliation policy embedded in our Whistleblowing Policy and Investigations Procedure. In terms of anticipated timelines, we respond immediately when concerns are raised, and the process normally is completed within 60 days from initiation.

Through this process, we believe that many of the components of UNGP 31 are met. However, because our System is used by authorized governmental parties to thwart major criminal threats and support covert investigations, our engagements – similar to others throughout our sector - are highly confidential. State agencies view that confidentiality as critical to preventing terrorists, criminals and criminal organizations from taking active measures to avoid detection, and thus part of their mission to protect their citizenries from physical harms and material risks.

Accordingly, we can only confirm to submitting parties that their concern is being actively pursued and when it has concluded. Needless to say, the actual government users of our technologies may choose to comment on allegations that are raised, which we often encourage given their greater access to facts, their duty to protect human rights, and their fundamental obligation to ensure that "those affected" by human rights abuses "have access to effective remedy" (UNGP 25). For these reasons, we cannot confirm that any specific concern warranted a thorough investigation or remediation, or whether a user targeted a specific device, which would necessarily confirm the existence of a customer relationship.

We also are conscious that Amnesty International is sensitive to our constraints, as its chapters face similar questions about how much they can keep individuals who lodge concerns apprised of the progress of an investigation, and thus would appreciate any constructive insights you might be willing to share. *See, e.g., Whistleblower Policy*, Amnesty International Australia, Sec. 3.1 (23 July 2019), at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-n--Zu4TsAhWJBhAIHdsCA6cQFjABegQICxAD&url=https%3A%2F%2Fwww.amnesty.org.au%2Fwp-content%2Fuploads%2F2019%2F08%2FBP02-AIA-Policy-Whistleblower.pdf&usg=AOvVaw2QvAofMWQS2W-79Xoam61W).

For the confidentiality, privacy and privilege concerns we have identified, we cannot comment on the substance of the concerns Amnesty International UK raised in October 2019 and June 2020 regarding alleged activities involving the Moroccan government. We can confirm that the information Amnesty International UK provided was taken extremely seriously, subjected to the process identified above, and that our inquiries have concluded. Of course, we cannot confirm who is or is not a customer or whether our products were or were not used in specific circumstances.

Nevertheless, since you requested information in relation to allegations involving the Moroccan government, and while we cannot comment on whether the Moroccan government is a customer or whether our System has been used in any specific circumstance, the Moroccan government itself appears to have responded to allegations Amnesty International has made, at least as reported by the press. Those press reports indicate that the relevant individuals mentioned by Amnesty International in its reports may have engaged in conduct that, it would seem, a state might legitimately investigate

Of course, we welcome any suggestions or insights you have as to how we might provide further details without betraying the customer confidentiality that is absolutely required in our engagements and our sector more generally, and we continue to look for ways to provide greater transparency despite these constraints. We likewise have begun to assess the extent to which we might be able to prevent customers from using our System in relation to certain classes of individuals or entities. We again would welcome any suggestions as to how individuals might practically be identified by name, device or position, and how we might avoid creating an "immunity" for certain individuals that inappropriately exempts them from legitimate government investigations of criminal activity.

We thank you again for your letter, reiterate our desire to engage constructively on these important issues, including about our investigations process and balancing the need for governments to protect their citizens and individual rights to privacy, and look forward to further dialogue.

Sincerely,

Shalev Hulio,
Chief Executive Officer
For NSO Technologies Ltd.