NSO GROUP

August 20, 2023

VIA E-MAIL

To: Beatriz Balbin
Chief
Special Procedures Branch
OHCHR

Cc: Mary Lawlor, Special Rapporteur on the situation of human rights defenders

Pichamon Yeophantong, Chair-Rapporteur of the Working Group on the issue of human rights and transnational corporations and other business enterprises

Irene Khan, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Clement Nyaletsossi Voule, Special Rapporteur on the rights to freedom of peaceful assembly and of association

Ana Brian Nougrères, Special Rapporteur on the right to privacy

Office of the United Nations High Commissioner for Human Rights
Palais des Nations
CH-1211 Geneva 10, Switzerland

Ref: AL OTH 62/2023

Re: **Joint Communication from Special Procedures**

Dear Ms. Balbin,

I am writing on behalf of NSO Group Technologies ("NSO" or the "Company") in response to your joint letter dated July 3, 2023. We welcome the opportunity to build upon our previous dialogues with Special Procedures, the Office of the United Nations High

NSO Group Technologies LTD 122 Galgalei HaPlada St. P.O.B 4166, Herzliya, 4672222, Israel
Telephone: +972.77.4341292 | Fax: +972.77.4253513 | | Email: office@nsogroup.com

NSO GROUP

Commissioner for Human Rights ("OHCHR"), and respond to the points raised in your most recent joint letter.

As a company, NSO remains dedicated to assisting government authorities conducting lawful investigations to protect the security and safety of citizens against terrorism and major crimes. NSO's products are licensed only to legitimate intelligence and law enforcement agencies of sovereign states after receiving requisite export licenses from the relevant export authorities. These government agencies operate our systems solely in accordance with their sovereign authorities under domestic laws, after agreeing to NSO's contractual requirements, which include human rights requirements consistent with international norms. In particular, our products help government authorities address the misuse of end-to-end encryption applications by terrorist and criminal groups to secretly plan, plot, and conspire to commit unlawful activities. Our technology has been used by states to prevent serious crimes and save lives on a massive scale. With our technology, states and state agencies have thwarted numerous major terrorist attacks, captured and brought many pedophiles to justice, broken up criminal organizations and drug trafficking rings and freed kidnapping and human trafficking victims. When used as designed and in accordance with NSO's contracts, our technology has protected the non-derogable rights to life, freedom from physical harm, freedom from arbitrary detention, freedom from torture, and freedom from cruel, inhuman or degrading treatment or punishment of countless individuals worldwide.

At the same time, NSO is fully aware of and committed to addressing the impact and potential risk of misuse of our products by the Company's customers. Indeed, NSO is proud to be the first and to its best knowledge the only company in the cyber surveillance technology sector to have implemented policies and procedures towards alignment with the United Nations Guiding Principles on Business and Human Rights. NSO has also continued to advocate for the development of a robust international framework for regulating the use of cyber surveillance technology, and has called for collaboration and dialogue among leaders from government, industry, civil society, and academia. NSO stands ready to engage constructively in this process as well as any other global initiatives.

With that context, we provide the following information to address the questions raised in your joint letter. We have grouped our responses thematically for ease of review.

Allegations Concerning Human Rights Defenders in Mexico (Questions 1–4)

As with any report of potential misuse of NSO's products, we remain seriously concerned about the allegations of misuse of Pegasus against members of Mexico's civil society, including Mr. Jorge Santiago Aguirre Espinosa ("Espinosa") and Ms. María Luisa Aguilar Rodríguez ("Rodríguez"), allegedly by one or more of the Company's customers. NSO learned of these allegations from the New York Times when contacted for comment and through monitoring publicly reported information on alleged instances of misuse of Pegasus, a practice established as part of NSO's ongoing efforts and commitment to address human rights risks. NSO identified

reports about these allegations in March and April 2023, including [redacted] a series of articles published by the New York Times.[1]

Promptly upon learning about the allegations in these reports, including related to Espinosa and Rodríguez, and consistent with the Company's Potential Product Misuse Investigations Procedure, NSO conducted a preliminary review of the allegations. This included determining whether there is sufficient information to facilitate a full investigation, such as phone numbers or Mobile Station International Subscriber Directory Numbers ("MSISDNs"), whether the reported conduct is technologically feasible using NSO's technology to which the alleged customer had access, and whether the alleged conduct actually involved potential product misuse. We were provided with an MSISDN for one of the alleged targets described in the media reports and, through open source research, NSO was able to identify additional numbers that the Company believes are related to other alleged targets. However, we do not have MSISDNs or phone numbers conclusively linked to Espinosa or Rodríguez. We welcome any additional phone numbers, MSISDNs, or other specific information that the UN Special Procedures Branch, Espinosa, or Rodríguez is able to provide, which NSO will incorporate into our investigation.

Our investigative efforts remain ongoing, and we are continuing to pursue all available means to bring our review to conclusion. NSO's efforts to engage with relevant agencies that have the potential authority to engage in the alleged conduct have required the Company to navigate national security concerns, obtain high-level clearances and authorizations, and address geographic and language challenges. NSO also has worked with an independent third party to collect, examine, and verify system information potentially relevant to the alleged conduct described in the media reports.

Contractual Safeguards (Questions 3–5)

Due to contractual obligations and national security considerations, NSO cannot confirm or deny the identity of our customers or share details regarding specific contracts. However, NSO's standard end-user agreements strictly require that our customers respect internationally recognized human rights, including the rights to privacy and freedom of expression as contained in the International Covenant of Political and Civil Rights Articles 17 and 19, and use the Company's products only for legitimate intelligence and law enforcement purposes. Where not clearly defined under domestic law, or where domestic law is not fully aligned with international

[1] Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, and Ron Deibert, *Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains*, The Citizen Lab (April 18, 2023), https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022; *See also* Natalie Kitroeff and Ronen Bergman, *Spying by Mexico's Armed Forces Brings Fears of a 'Military State,'* New York Times (March 7, 2023), https://www.nytimes.com/2023/03/07/world/americas/mexico-military-surveillance.html; *How Mexico Became the Biggest User of the World's Most Notorious Spy Tool*, New York Times (April 18, 2023), https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html; *He Was Investigating Mexico's Military. Then the Spying Began*, New York Times (May 22, 2023), https://www.nytimes.com/2023/05/22/world/americas/mexico-spying-pegasus-israel.html.

norms, NSO includes contractual provisions defining specific crimes and terrorism-related activities in respect of which our products may be used to prevent or investigate. We further limit the geographic territories in which customers are able to use our products, as well as the duration of the licenses extended to customers.

Moreover, our customers are contractually required to fully comply with all applicable domestic laws and regulations related to surveillance activities, including obligations to obtain judicial warrants, consents, approvals, or the like. In addition, following a due diligence review, if NSO determines that there is an elevated risk that a customer's existing processes for evaluating the appropriateness of surveilling a particular target with NSO's technology may not be consistent with international norms, NSO contractually requires the customer to formulate and strictly abide by an internal procedure or protocol that is consistent with international principles. Customers are further contractually obligated to review NSO's Human Rights Policy, provide immediate notice to NSO of any knowledge they may have regarding suspected misuse of the Company's products that could result in human rights violations, and cooperate with NSO's investigations regarding allegations of product misuse. We also reserve the contractual right to suspend or terminate a customer's access to our products for human rights-related misuse, including while an investigation is ongoing, which we have done numerous times in the past when we believed that there was a misuse of our system.

Human Rights Due Diligence (Questions 3–8)

As noted above, NSO cannot confirm or deny the identity of our customers or provide details of any specific due diligence review. Nevertheless, customer due diligence remains a vital part of NSO's human rights compliance program. For each new sales opportunity, NSO conducts a thorough human rights-focused due diligence review in accordance with the Company's Human Rights Due Diligence Procedure. NSO also conducts periodic due diligence reviews of the Company's existing customers. While NSO cannot ultimately prevent every customer misuse of the Company's technology, we can and do attempt to identify those that have a heightened risk.

As part of the due diligence review process, NSO conducts a human rights-focused country-level assessment. This includes an evaluation of the prospective country's human rights record, as well as its perceived respect for the rule of law, freedom of speech and freedom of the press, political stability, and level of corruption. NSO also considers the nature of the product at issue, the potential customer's profile, defined mission, and credibility, the duration of the anticipated contract, and other factors that could increase or decrease human rights risks. Depending on the level of potential human rights-related risk, NSO may further assess adverse public information, analyze the domestic legal framework and, where appropriate, require a review by an external risk and investigation firm. Once compiled, the Company evaluates the information and determines the appropriate course of action, which includes potential measures that may reasonably be employed to mitigate risks of misuse if the engagement proceeds. In

many instances, NSO declined to license the Company's technology to potential customers following our due diligence review.

Over the past several years, NSO has sought to continuously improve the Company's human rights program, including its due diligence process. NSO's Compliance team has progressively and significantly increased its engagement with potential customers as part of the due diligence process. This engagement continues over the duration of the relationship and allows NSO to collect additional information, provide human rights-focused training and education, and better evaluate an actual or potential end-user's commitment to human rights. For example, NSO's Vice President for Compliance has conducted more frequent in-person site visits to customer locations to gain a better understanding of end-user organizations and processes, and provide enhanced guidance on the Company's human rights requirements.

NSO also expanded the scope of publicly available data that we use to derive an objective score for a potential customer's country as part of evaluating new opportunities. This score helps determine the level of due diligence that will be conducted and is used to evaluate the relative strength of the rule of law and protection of human rights in a prospective customer country. [redacted] In addition, following evaluation of the potential human rights impacts of our products on journalists, NSO added subjective factors to our due diligence review, as discussed further below. These measures are designed to help us identify—and avoid where possible—customers that we think might misuse our technology.

We are committed to consistently enhancing our due diligence endeavors and refining our compliance program, ensuring an ongoing process of learning. This dedication aims to guarantee that our systems are operated by our customers in alignment with Human Rights to the utmost degree.

Additional Measures to Address Potential Human Rights Impacts (Questions 4–8)

Impact Assessment Related to Journalists

In an ongoing effort to address potential human rights impacts from the use of our products, NSO has been assessing the potential impacts of its technology on journalists and the media. As part of the assessment, NSO researched and collected publicly available data points on reported instances of potential misuse of Pegasus against journalists, and analyzed key information about the reported targets, including their country of residence, demographic information, journalistic reporting activities, and prior interactions with governments. NSO identified several salient trends with respect to these allegations as a result of our analysis of the potential impacts of NSO's activities on rights-holders. We modified our due diligence review

process to address these trends.[2] NSO is continuing to evaluate the potential impact of our products on journalists and other vulnerable populations.

Detailed Guidelines for End-Users

To further mitigate the risk of misuse of our products, NSO created a detailed Standard Operating Procedure ("SOP") for certain end-users of NSO technology where, following a due diligence review, NSO determines that there is an elevated risk that a customer's existing processes for evaluating the appropriateness of surveilling a particular target with NSO's technology may not be (i) consistent with international norms or (ii) fully visible to NSO. This SOP enumerates a step-by-step process that customers' employees are required to follow in the course of operating NSO technology. The SOP specifically instructs end-users to consider whether a target is a human rights defender, a journalist, a lawyer, or a political dissident, and if so, to exercise heightened care. Another key aspect of the SOP is that it requires end-users to create a record that NSO—or an agreed independent third party—can access with customer consent and review if allegations of misuse subsequently arise.[3] The SOP is designed to help customers operate NSO technology in accordance with established international human rights standards, including by following internal processes that address substantive and procedural considerations.

Continued Engagement with Stakeholders

NSO continues to engage with stakeholders to work towards an international framework for regulating the use of cyber surveillance technology. Over the past several years, NSO has engaged and sought to engage with numerous stakeholders—ranging from government entities, parliamentary or congressional committees, and international organizations, including the United Nations, to academics, civil society organizations, and professional associations—regarding the need for a robust international regulatory framework governing the use of cyber surveillance technology and the responsibilities of States and private entities.

While NSO has undertaken and continues to undertake appropriate steps to mitigate risks of misuse of our products, there are obvious limits as to what a private company can do to monitor the actions of customers, particularly when those customers are intelligence and law enforcement agencies of sovereign governments engaged in highly sensitive and confidential

---

[2] NSO's impact assessment focused on identifying the potential human rights impacts of our products, not on determining whether each identified allegation was true. NSO investigates all credible allegations that its products have been misused through a separate investigation process governed by our Potential Product Misuse Investigation Procedure.

[3] This record is in addition to the existing "indelible, permanent, and uneditable auditable record" as called for in the April 2023 report prepared by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. United Nations Human Rights Special Procedures, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, April 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf.

investigations. Similarly, while NSO is committed to transparency and continues to be one of the most forthcoming companies in the cyber surveillance technology sector, we are under strict regulatory and confidentiality restraints that significantly limit our ability to share customer information publicly.

Continuing dialogue, including multi-stakeholder exchanges and multilateral efforts that encompass governments, industry, academic communities, and civil society, therefore remains key to appropriately regulating this industry and protecting the rights of individuals. NSO remains committed to that open dialogue and establishing an international framework for the responsible use of cyber surveillance technology with guidelines and criteria for legitimate use commensurate with globally accepted human rights standards. Such an international framework would also need to address when the obligation of private companies to disclose information about a customer relationship or activity—for example, when there are credible allegations of misuse—outweighs the desires of State authority customers to maintain confidentiality related to their purchase and operation of a product, as well as the States' own obligations for transparency against their need to conduct covert opperations. We welcome the opportunity and stand ready to further engage with the UN Special Procedures Branch to help develop this framework as well as related guidelines and criteria.

Ongoing Commitment to Respecting Human Rights (Questions 4–8)

As we have always made clear, NSO is committed to respecting human rights. NSO has voluntarily implemented an industry-leading human rights due diligence process that goes beyond legal and regulatory requirements, and the Company investigates all credible allegations that its products have been misused to wrongly target anyone, including human rights defenders, journalists, political dissidents, and other vulnerable individuals.

We have undertaken serious and appropriate steps to address instances of potential product misuse. For example, in recent instances in which the Company received concerns or complaints regarding alleged product misuse, NSO suspended customers' use of its technology, conducted a detailed review of customer compliance, reviewed the relevant contracts, and interviewed customer representatives to understand their processes and perspectives. In particular, NSO evaluated whether customers had a factual basis to conduct surveillance under the relevant domestic legal framework and whether that domestic legal framework is consistent with the requirements under international law. NSO has reinstated customer access to its system only where it gained comfort that its technology was not misused. In a number of instances, NSO terminated contracts and severed relationships with customers after misuses were identified.

It is worth noting, however, that the rapid development and widespread use of end-to-end encryption has profoundly changed the ability of states to prevent and investigate terrorism and other serious crimes. The use of new and advanced technologies by terrorists and criminals to further their unlawful activities has, in turn, required intelligence and law enforcement agencies

NSO GROUP

across the globe to search for and embrace new technologies to combat terrorism and other serious crimes. NSO's mission is to assist lawful investigations by state authorities to protect the security and safety of citizens against terrorism and major crimes, which in themselves are an important contribution towards the enjoyment of human rights. Inevitably, when determining whether to terminate a customer's license to use the Company's technology, NSO has to consider the customer's reduced capability to prevent or tackle terrorism and other serious crimes, and the potential adverse human rights impacts that may result from such circumstances.

We hope this response, together with our previous communications with Special Procedures, can help shed light on NSO's human rights program and its ongoing efforts to further improve the processes that are already in place.

Sincerely,

[redacted]

Yaron Shohat
Chief Executive Officer
NSO Group Technologies

NSO Group Technologies LTD 122 Galgalei HaPlada St. P.O.B 4166, Hertsliya, 4672222, Israel I
Telephone: +972.77.4341292 I Fax: +972.77.4253513 I I Email: office@nsogroup.com