UNITED NATIONS
HUMAN RIGHTS
SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS

PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9543 / +41 22 917 9738 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

REFERENCE:
OL OTH 52/2019

18 October 2019

Dear Mr. Hulio,

I am writing to provide preliminary reactions to the Human Rights[1] and Whistleblower policies[2] that NSO Group Technologies (NSO Group) published in September 2019. I welcome any genuine efforts to enhance human rights accountability and oversight in the private surveillance industry and I am happy to gain a better understanding as to how NSO Group plans to implement its human rights responsibilities.

For background, it is my responsibility as the United Nations Special Rapporteur on freedom of opinion and expression to evaluate how governments, non-state actors and companies protect and promote everyone's right to seek, receive and impart information and ideas worldwide. The UN Human Rights Council appointed me to the position in 2014, and I report to the Council and the General Assembly. I also conduct official country missions and communicate regularly with governments, civil society and private industry. Digital rights has been at the center of my work, and I have focused on the obligations of governments and the concomitant responsibilities of companies to ensure protection of freedom of expression and privacy in digital space. My most recent report to the Human Rights Council is of definite relevance to your industry and NSO Group in particular. In it, I highlighted the near total lack of both accountability for abuses of surveillance technologies and legal or political constraints on their global transfer.[3]

I was glad to learn of NSO Group's effort to develop a Human Rights and Whistleblower Policies. The Human Rights Policy explicitly states that NSO Group is "committed to respecting human rights as enshrined in the International Bill of Human Rights [...]" Your Policy also noted that the United Nations Guiding Principles on

[1] NSO Group, Human Rights Policy, https://www.nsogroup.com/governance/human-rights-policy/.
[2] NSO Group, Whistleblower Policies, https://www.nsogroup.com/governance/whistleblower-policies/.
[3] *See generally* David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/41/35 (May 28, 2019), https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/35

Business and Human Rights guide you in fulfilling "our obligation to respect human rights throughout our business activities." This is an important recognition and, taking you and your company at your word, I will also frame my comments around those same standards of international human rights law.

The NSO Group's new policies come in the wake of significantly troubling information about the sale, transfer and use of your company's technologies and their impact on human rights, especially but not limited to freedom of expression and the right to privacy. That context is critical to my understanding of the nature and impact of your new policies. Thus, I will first reference some of the most worrying information I have received on the use of NSO Group's technologies, and then I will share a non-exhaustive assessment of a number of areas where the policies may undermine the overall object and purpose of the UN Guiding Principles and the broader corpus of human rights law.

Information Received Concerning Use of NSO Group Technologies

According to information I have received, all of which is in the public record, the NSO Group's Pegasus technology has been used by governments to track civil society, journalists, political dissidents, and others across the world. Pegasus offers authorities the capability of hacking directly into mobile devices and gaining access to calls, messages, and other data stored on the device and other locations. Most commonly, the target of a surveillance operation receives a message containing a specific link, which installs the Pegasus software on the device when the target clicks on the link. Once activated, Pegasus gives full access to the phone's data including communications and location information. A Canadian research and advocacy organization, Citizen Lab, has found indications of "possible political themes within targeting materials in several countries, casting doubt on whether the technology is being used as part of 'legitimate' criminal investigations".[4] Among the victims allegedly targeted by the use of Pegasus spyware are journalists, politicians, United Nations investigators, human rights defenders and others in dozens of countries worldwide. In addition, the NSO Group is reportedly funding

[4] *See* Bill Marczak, *Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries*, Citizen Lab, (Sept. 18, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/. On specific examples, see Bill Marczak, The Million Dollar Dissident: NSO Group's Iphone Zero-Days used against a UAE Human Rights Defender, Citizen Lab (Aug. 24, 2016), (https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/) and VOA News, Khashoggi Friend Says Israeli Spyware Played Role in His Killing (Dec. 3, 2018), https://www.voanews.com/world-news/middle-east-dont-use/khashoggi-friend-says-israeli-spyware-played-role-his-killing, David D. Kirkpatrick & Azam Ahmed, *Hacking a Prince, an Emir and a Journalist to Impress a Client*, N.Y. Times (Aug. 31, 2018), https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html, Bill Marczak, *Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries*, Citizen Lab, (Sept. 18, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/, John Scott-Railton et al., *Reckless VI: Mexican Journalists Investigating Cartels Targeted With NSO Spyware Following Assassination of Colleague*, Citizen Lab (Nov. 27, 2018), https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/, John Scott-Railton et al., *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted with NSO Exploit Links*, Citizen Lab (Feb. 11, 2017), https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/, Amnesty International, Amnesty International Among Targets of NSO-Powered Campaign (2018), https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.

startup companies selling similar technologies that enable hacking into WIFI routers, home speakers, and other devices.[5]

Special Procedures mandate holders have addressed the use contrary to human rights law of surveillance technology developed by the NSO Group on several occasions. The most recent examples include the 2019 report to the Human Rights Council of Special Rapporteur on extrajudicial, summary or arbitrary executions, Agnes Callamard, on the Investigation into the unlawful death of Mr. Jamal Khashoggi,[6] and my own 2019 report to the Human Rights Council on the private surveillance industry.[7] In addition, the use of the Pegasus technology has been subject of several communications by Special Procedures mandate holders.[8]

International Human Rights Framework

Your Human Rights Policy identifies the International Bill of Rights as a standard of importance. The central international human rights treaty is the International Covenant on Civil and Political Rights (ICCPR), concluded in 1966, which involves binding obligations on States to promote and protect a range of rights including rights to privacy, opinion and expression. The ICCPR largely echoes the 1948 Universal Declaration of Human Rights. Article 19 of both instruments protects everyone's right to hold opinions without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media. Article 17 (1) of the Covenant, echoing article 12 of the Declaration, provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence" (A/HRC/41/35, para. 23). It has become customary to emphasize that individuals enjoy the same rights online as they do offline, as numerous resolutions of the UN General Assembly and Human Rights Council make clear.

Privacy and expression are intertwined in the digital age, with online privacy serving as a gateway to secure exercise of the freedom of opinion and expression (A/HRC/41/35, para 24; A/HRC/29/32; and A/HRC/23/40, para. 24). The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and

---

[5] Becky Peterson, Inside the Secretive Israeli Spyware Startup Scene, Where the Notorious NSO Group Has Spawned a Web of Companies that Hack Into Devices, Business Insider (Sep. 6, 2019), https://www.businessinsider.com/israel-offensive-cybersecurity-world-funded-by-nso-group-2019-9.

[6] *See* Agnes Callamard (Special Rapporteur on extrajudicial, summary or arbitrary executions). Report on Investigation into the unlawful death of Mr. Jamal Khashoggi. U.N. Doc A/HRC/41/CRP.1, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session41/Documents/A_HRC_41_CRP.1.docx. See also David Ignatius, How a Chilling Saudi Cyberwar Ensnared Jamal Khashoggi, Wash. Post (Dec. 7, 2018), https://www.washingtonpost.com/opinions/global-opinions/how-a-chilling-saudi-cyberwar-ensnared-jamal-khashoggi/2018/12/07/f5f048fe-f975-11e8-8c9a-860ce2a8148f_story.html.

[7] See David Kaye (Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression). On the Private *Surveillance Industry*. U.N. Doc A/HRC/41/35.

8 See e.g. AL SAU 10/2019 and AL MEX 4/2017, available at https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization (A/HRC/23/40, para. 24). Article 17 of the ICCPR permits interference with the right to privacy only where it is "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant", is in pursuit of "a legitimate aim" and "meet[s] the tests of necessity and proportionality" (A/69/397, para. 30). Article 19 articulates a three-part test requiring that restrictions be "provided by law" and be "necessary" to protect the "rights or reputations of others", "national security or public order (*ordre public*), or public health or morals."[9]

Human rights law does not, as a general matter, directly govern the activities or responsibilities of private business, and international human rights treaties generally do not impose direct legal obligations on business enterprises. However, the actions of business enterprises can affect the enjoyment of human rights by others.[10] A variety of initiatives provide guidance to enterprises to ensure compliance with fundamental rights. The Human Rights Council endorsed the UN Guiding Principles on Business and Human Rights in 2011. The Guiding Principles recognize the responsibility of business enterprises to respect human rights, independent of State obligations or the implementation of those obligations (see A/HRC/17/31, annex; and A/HRC/32/38, paras. 9- 10). They provide a minimum baseline for corporate human rights accountability, urging companies to adopt public statements of commitment to respect human rights endorsed by senior or executive-level management; conduct due diligence processes that meaningfully "identify, prevent, mitigate and account for" actual and potential human rights impacts throughout the company's operations; and provide for or cooperate in the remediation of adverse human rights impacts (see A/HRC/17/31, annex, principles 16-24).

Concerns Relating to Human Rights Policies

In my May 2019 report to the Human Rights Council, I describe how surveillance companies should meet their human rights responsibilities.[11] The report emphasized that private companies are creating, transferring and servicing surveillance technologies in troubling ways. Credible allegations have shown that companies are selling their tools to Governments that use them to target journalists, activists, opposition figures and others who play critical roles in democratic society. Some of these companies have objected to the findings of journalists and human rights organizations, arguing that they do not permit the use of their products for illicit purposes, they have mechanisms to evaluate sales to "sensitive" end users and they abide by national laws on the control of exports. It is possible that some companies are making genuine attempts to address the charges of

[9] Detailed explication of the three-part test under article 19 may be found in Human Rights Committee, general comment No. 34 (2011) on the freedoms of opinion and expression, paras. 5–9 and 22–36; and A/HRC/38/35.
[10] See generally, UN OHCHR, The Corporate Responsibility to respect Human Rights: An Interpretative Guide. HR/PUB/12/02. https://www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf
[11] See footnote 3.

complicity in surveillance-based repression and abuses. There are, however, virtually no *public disclosure* and *accountability* processes to verify such claims.

The gravity of the allegations, the report found, demands transparency in companies' relationships and processes, the integration of human rights due diligence throughout the companies' supply chain and servicing. These processes should establish human rights by design, regular consultations with civil society (particularly groups at risk of surveillance), and robust transparency reporting on business activities that have an impact on human rights. Companies should also put in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards. These safeguards include contractual clauses that prohibit the customization, targeting, servicing or other use that violates international human rights law, technical design features to flag, prevent or mitigate misuse, and human rights audits and verification processes. The report also recommended that when companies detect misuses of their products and services to commit human rights abuses, they should promptly report them to relevant domestic, regional or international oversight bodies. They should also establish effective grievance and remedial mechanisms that enable victims of surveillance-related human rights abuses to submit complaints and seek redress.

I concluded in the report that, given the extraordinary evidence and risk of abuse of surveillance technologies, it is essential that companies immediately cease the sale and transfer of and support for such technologies, until they have provided convincing evidence that they have adopted sufficient measures concerning due diligence, transparency and accountability to prevent or mitigate the use of these technologies to commit human rights abuses.

Particularly given the abuses and opacity of the private surveillance industry, NSO Group's development of a Human Rights Policy itself deserves comment and oversight, and I encourage NSO Group -- and all businesses in the sector -- to engage with human rights experts and have regular consultations with civil society. Generally, my conclusion concerning the Policy, on the merits, is that it neither references the legacy of harm perpetuated as a result of NSO Group's failure to ensure that its technology is used responsibly nor articulates why its new policy will necessarily lead to improved outcomes for victims of surveillance harassment.

The Human Rights Policy raises many questions about how NSO Group plans to prevent or mitigate human rights abuses committed with the technology it makes available to governments worldwide. I would be pleased if you would respond to the following questions:

1. How will NSO Group confirm that its clients are complying with human rights law? In part IV of the Human Rights Policy, NSO Group claims that it requires States to agree to abide by human rights standards, but gives no indication that it has a reliable way to verify if States are complying with those standards. The last section of the human rights policy rightly states

that countries bear responsibility for enforcing human rights and providing remedies when they occur, but this fact does not exculpate NSO Group from human rights abuses committed by States who use its technology. Please describe, in detail, what new policies have been put in place at NSO Group that will ensure previous errors in identifying ongoing human rights abuse will not be repeated.

2. How does NSO Group's new due diligence policy differ from the previous policies that allowed for its product to be sold to States with bad human rights records? According to publicly available information,[12] an NSO Group employee described a process of balancing the State's interest in thwarting threats against the potential for human rights violations. Do NSO Group's due diligence procedures currently engage in this sort of balancing?

3. What internal safeguards does NSO Group have in place that ensure design and engineering choices incorporate human rights safeguards? There is no mention of NSO Group's incorporation of internal flagging systems or 'kill switches' that detect misuse. While your Policy states that the NSO Group designs its "products to support effective governance of use and to prevent unauthorized or accidental misuse," and that you have an "escalating set of remedies culminating in the termination of use of [y]our products after a substantiated case of severe misuse," this mechanism seems to rely heavily on customers notifying you of their knowledge of the misuse. Furthermore, your Policy states that you "never use or participate in the use of [y]our products" and "have no access to personal data used in or generated from their use [...] We do not operate our products ourselves or on behalf of our customers; our role is limited to the provision of technical support and maintenance services to our customers." This raises a fundamental question: how can NSO Group genuinely uphold the Guiding Principles on Business and Human Rights when it has no direct way to monitor how its products are being used?

4. How will NSO Group ensure full transparency on the principles and effectiveness of its human rights policy? Section X of the Human Rights Policy states that NSO Group will take into consideration various constraints, including commercial restraints, which may limit its ability to disclose specific information about the effectiveness of its policy. Given the NSO Group's previous intransigence on the subject of transparency, this language reads as a broad justification to restrict any information related to its Human Rights Policy that reflects poorly on NSO Group or its clients.

[12] https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/

5. The Human Rights Policy makes no mention of reporting misuse of NSO Group's tools to national human rights institutions or intergovernmental bodies in the Human Rights Policy. How does NSO Group intend to inform national and international bodies about abuses?

6. It is imperative that certain details about NSO Group's operations be disclosed to the public, including the potential uses and capabilities of its products, the types of after-sales support provided to clients, a record of incidents of misuse of NSO Group's products, and an accounting of types of sales to law enforcement, intelligence or other government agencies or their agents. NSO Group indicates at various points in its policy that it compiles this kind of information, but at no point indicates a willingness to disclose it to anyone outside the universe of NSO Group's business partners and customers. How does NSO Group plan on making this data available?

7. NSO Group should commit to holding regular consultations with affected rights holders, civil society groups and digital rights organizations. The policy states NSO Group's commitment to "ongoing dialogue with all relevant stakeholders," but the policy description suggests this does not include victims of civil rights abuses. While we applaud NSO Group's acknowledgment that digital surveillance has a disproportionate impact on vulnerable communities, how does NSO Group intend to bring those unreasonably targeted by NSO Group technology into regular consultation?

8. When a party believes it or its members are victims of human rights abuses facilitated by NSO Group's products and submits a complaint to NSO Group, how will you provide for an independent assessment of that claim? The policy makes no mention of independent follow-ups to complaints, something crucial to ensuring that reports of abuse are met with meaningful follow up. There is also no mention of effective means of redress for victims of misuse of NSO Group technology including compensation. How will NSO create a path for victims to have their concerns addressed directly by the company?

Concerns Relating to Whistleblower Policies

Whistleblower protections rest upon a core right to freedom of expression, guaranteed under international law, in particular the International Covenant on Civil and Political Rights (ICCPR). In 2015, I reported to the UN General Assembly on the topic of protection of whistleblowers under international human rights law (A/70/361). Whistleblowers enjoy the right to impart information, but their legal protection when publicly disclosing information rests especially on the public's right to receive it.

States and organizations have responded to the problem of hidden wrongdoing with laws and policies to protect those who take steps to report it. However, individuals who report alleged wrongdoing are still subjected to harassment, intimidation, investigation, prosecution and other forms of retaliation. All too often, States and organizations implement the protections only in part or fail to hold accountable those who retaliate against whistle-blowers. Moreover, beyond law, the right to information also requires a bedrock of social and organizational norms that promote the reporting of wrongdoing or other information in the public interest. The strengthening of such norms requires training at all levels of organizations, supportive policies and statements from political and corporate leaders, international civil servants, the courts and others, and accountability in cases of reprisals.

I am mindful of the challenges that NSO Group and other private surveillance corporations face in protecting their businesses with legal and confidentiality standards while also adhering to human rights. In your press release you stated that "this new policy publicly affirms [y]our unequivocal respect for human rights and [y]our commitment to mitigate the risk of misuse." Your stated commitment to freedom of expression and human rights policy brings NSO Group a step closer towards upholding the appropriate privacy and freedom of expression standards.

I welcome efforts to include a broad scope of individuals and bodies covered by your Policy. According to the document available online, the Policy covers "all employees, contractors, partners, officers, and directors of the NSO Group, as well as any external person or body who wishes to express a grievance". By keeping a broader terminology to include employees and non-employees the focus remains on the alleged wrongdoing rather than the individual imparting the information.

However, the whistleblower policy does raise some serious concerns about the actual protection of whistleblowers and the consequential chilling effect that could arise from your investigation scheme. In particular, I would be pleased if you would respond to the following questions:

1. What is the scope of protected disclosures? The scope of protected disclosures included in your Policy is not easily understandable by potential whistleblowers. Your Policy states that

   > "[w]histleblowing is the reporting of suspected wrongdoing or dangers in relation to NSO Group's activities or products. This may include, for example, bribery and corruption misconduct; the inappropriate use/misuse of the NSO Group's products and/or services and resulting adverse human rights impact by any person, including employees, officers, directors, consultants, contractors, customers, or other NSO Group representatives or partners".

While you include very brief examples of what might constitute "wrongdoing," whistleblowing does not always involve specific individual wrongdoing, but it may uncover hidden information that the public has a legitimate interest in knowing. International authorities and States often provide a general protection for the disclosure of information in the public interest, or disclosure of specific categories of information, or both. While the term "public interest" may appear capacious as a basis for whistleblower protection, a State or Organization might define "public interest" as involving information that contributes to public debate, promotes public participation, exposes serious wrongdoing, improves accountability or benefits public safety (A/70/361). In order to encourage and protect whistleblowers, please clarify what the NSO Group understands as an "inappropriate" use or a "misuse" of its technology.

2. What are the specific confidentiality guarantees for whistleblowers? Whistleblower policies should protect strongly against the risk that persons who disclose facts that indicate wrongdoing may be subject to personal attack and other forms of retaliation. Guarantees and mechanisms of confidentiality provide important protection against retaliation. Whistleblowing mechanisms should provide for secure submissions and take other steps to ensure the confidentiality of disclosures, including by defining intentional or negligent breaches of confidentiality as a form of retaliation subject to penalty. While your Policy expressly accepts "anonymously raised concerns" and allows whistleblowers to "raise confidential concerns", it lacks clarity on the mechanism in place that will be in charge of receiving the "suspected wrongdoing or dangers". For example, the policy does not clearly establish who reads the complaint-email sent by the whistleblower[13] and who follows up. The Policy also states that a meeting may be arranged with the whistleblower. However, it does not clarify how NSO Group will guarantee anonymity in this process, who would be present in this meeting, what confidentiality and unbiased measures are taken to ensure that the employees who are a part of follow-up process do not retaliate or release the identity of the whistleblower.

3. Your policy states that once the whistleblower has raised a concern an "initial assessment will be carried out to determine whether it should result in an investigation", and its potential scope. If the case warrants it, "NSO Group may appoint an investigator or a team of investigators". However, the Policy does not clearly state who will carry out the initial assessment, how the investigator or team of investigators are appointed, or the nature of their independence from the company. As drafted, the investigation appears to be limited to company internal mechanisms.

   When working properly, internal mechanisms provide a way for someone who perceives wrongdoing to seek a competent authority's investigation. They allow

[13] The Policy does state that the General Counsel of NSO Group has access to the email account.

for timely attention by those who may be in the best position to address problems, while also providing a basis for balancing legitimate interests in secrecy and the redress of wrongdoing. However, the policy's internal mechanism presents potential whistleblowers with serious risks that may be fatal to the purpose of whistleblowing. The Policy lacks strong measures of confidentiality and the proposed mechanism for reporting lacks independence from the organization in which it is embedded, putting whistle-blowers at risk of retaliation.
As long as internal reporting channels require implementing actions by various individuals in the organization's management, they will fail to enjoy the credibility that comes with independent review.

4. Your Policy states that NSO Group "will support whistleblowers who raise *genuine* concerns[...] even if they turn out to be mistaken" (emphasis added) and later adds that NSO Group "may take legal action against a whistleblower that has made false allegations maliciously or with a view to personal gain." What is considered a *genuine* concern? What classifies as malicious allegations? The whistleblower's motivations at the time of the disclosure should be immaterial to an assessment of their protected status. Variations of a "good faith" requirement for reporting, could be misinterpreted to focus on the motivation of the whistle-blower rather than the veracity and relevance of the information reported. It should not matter why the whistleblower brought the information to attention if he or she believed it to be true[14] ().Upon disclosure, authorities should investigate and redress the alleged wrongdoing without any exception based on the presumed motivations or "good faith" of the person who disclosed the information.

   Protection mechanisms should promote disclosure and not require potential whistleblowers to undertake precise analyses of whether perceived wrongdoing could be considered as "malicious" (especially without giving a clear and precise definition of the term). Otherwise, the protection itself would be hollow, encouraging disclosure and signaling potential retaliation at the same time.

5. Your Policy also lacks strong and clear punishments to those who retaliate against whistleblowers. The Policy states that "it is strict NSO Group policy that employees, contractors, officers, directors and consultants must not threaten or retaliate against whistleblowers in any way." However, the policy should include that the punishment of those who retaliate will be serious, not merely disciplinary, and including the possibility of removal from their post and personal liability.

Thank you for your engagement on this critical issue. I would appreciate a response to my questions and concerns. I am happy to discuss these issues further with you or your representatives.

---

[14] David Kaye, Report of the of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/70/361 (Sept 8, 2015), para. 31 https://undocs.org/A/70/361