Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Working Group on the issue of human rights and transnational corporations and other business enterprises; the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on the situation of human rights defenders

REFERENCE:
AL OTH 211/2021

4 August 2021

Mr. Hulio,

We have the honour to address you in our capacities as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Working Group on the issue of human rights and transnational corporations and other business enterprises; Special Rapporteur on the rights to freedom of peaceful assembly and of association and Special Rapporteur on the situation of human rights defenders, pursuant to Human Rights Council resolutions 43/4, 44/15, 41/12 and 43/16.

We are independent human rights experts appointed and mandated by the United Nations Human Rights Council to report and advise on human rights issues from a thematic or country-specific perspective. We are sending this letter under the communications procedure of the Special Procedures of the United Nations Human Rights Council to seek clarification on information we have received. Special Procedures mechanisms can intervene directly with Governments and other stakeholders (including companies) on allegations of abuses of human rights that come within their mandates by means of letters, which include urgent appeals, allegation letters, and other communications, as well as issue public statements and undertake other forms of advocacy. The intervention may relate to a human rights violation that has already occurred, is ongoing, or which has a high risk of occurring. The process involves communicating in writing with the concerned actors identifying the facts of the allegation, applicable international human rights norms and standards, raise the concerns and questions of the mandate-holder(s), and seek clarification and request corrective action. Communications may deal with individual cases, general patterns and trends of human rights violations, cases affecting a particular group or community, or the content of draft or existing legislation, policy or practice considered not to be fully compatible with international human rights standards.

In this connection, we are writing to convey our serious concerns with regards to **the reported use of the Pegasus spyware developed by NSO Group Technologies (the NSO Group) to surveil hundreds of journalists, human rights defenders and political leaders in various countries**.

The United Nations Special Procedures have previously raised human rights concerns about the Human Rights and Whistleblower policies developed by the NSO Group in September 2019 (OL OTH 52/2019 and OL OTH 2/2020), and about the use of the Pegasus spyware in July 2019 (AL SAU 10/2019). We thank your company for its response dated 10 December 2019, but we remain seriously concerned, especially in light of the information we recently received.

On 18 July 2021, an international investigation exposing widespread global surveillance of the mobile devices of hundreds of journalists, human rights defenders and political leaders, through the use of the NSO Group's Pegasus spyware, was made public. As a result, access to calls, messages, and other data stored on the device of those affected was reportedly hacked. It is reported that at least 180 journalists from about 20 countries were targeted, including countries where our mandates have previously raised serious human rights concerns about the state of media freedom and the rights to freedom of expression and freedom of peaceful assembly.

On the day after this information was made public, the NSO Group released a statement[1] in which it made the following remarks: "We would like to emphasize that NSO sells it technologies solely to law enforcement and intelligence agencies of vetted governments for the sole purpose of saving lives through preventing crime and terror acts […]. Our technologies are being used every day to break up pedophilia rings, sex and drug-trafficking rings, locate missing and kidnapped children, locate survivors trapped under collapsed buildings, and protect airspace against disruptive penetration by dangerous drones." In the same statement, the NSO Group claimed that the report published on international media was "full of wrong assumptions and uncorroborated theories that raise serious doubts about the reliability and interests of the sources".

We are troubled that your company rejected vehemently the information that had been made public, but chose not to disclose the results of any internal probe into potential human rights harms that may have been caused by your company, or to which it may have contributed, or which were directly linked to your products or services through business relationships. Under human rights law and the United Nations Guiding Principles on Business and Human Rights[2], companies have a responsibility to respect all internationally recognized human rights throughout their activities and operations. In order to identify, prevent, mitigate and account for how they address their human rights impacts, companies are expected to conduct regular and ongoing human rights due diligence in consultation with relevant stakeholders. In this context, we urge your company to make public the results of any human rights due diligence your company may have recently conducted, including in relation to the information that has now been made public. In accordance with Guiding Principle 21, in order "to account for how they address their human rights impacts, business enterprises should be prepared to communicate this externally, particularly when concerns are raised by or on behalf of affected stakeholders".

We are alarmed that the surveillance operations that were recently exposed reportedly used technology developed by your company to surveil hundreds of journalists, human rights defenders and political leaders, whose roles are critical in a democratic society. We are deeply concerned by the allegations that the Pegasus spyware was supplied to and used by State agencies or by entities that do not have a track record of respecting international human rights. We fear that the Pegasus spyware may have been planted onto the devices of journalists, human rights defenders and political leaders with the goal of monitoring, intimidating and possibly silencing them. If such an intrusive interference was carried out in contravention of human rights laws and norms, your company may have legal responsibility to those persons who were harmed as a result of such interference.

---

1 www.nsogroup.com/Newses/following-the-publication-of-the-recent-article-by-forbidden-stories-we-wanted-to-directly-address-the-false-accusations-and-misleading-allegations-presented-there/

2 A/HRC/RES/17/31, Annex, referred to hereinafter as the "Guiding Principles".

We are further deeply concerned that the apparent disregard for the right to be free from any unlawful and arbitrary interference in one's private life may have not only affected concerned journalists, human rights defenders and political leaders, but also those with whom these individuals have been in contact. If the allegations are confirmed, the unlawful hacking of numerous cell phones may have contributed to infringing the rights to privacy, liberty and security, and possibly to life, of an extremely high number of individuals, in numerous countries.

In light of these major human rights risks, we would like to remind your company about its responsibility to respect human rights norms, especially the rights to privacy, freedom of expression, association, assembly, security and liberty, and the right to life. In its resolution 34/7, the United Nations Human Rights Council noted "with deep concern that, in many countries, individuals and organizations engaged in promoting and defending human rights and fundamental freedoms are frequently subject to threats, harassment and insecurity as well as to unlawful or arbitrary interference with their right to privacy, as a result of their activities". Likewise, the United Nations General Assembly has repeatedly "condemned unlawful or arbitrary surveillance and interception of communications as 'highly intrusive acts' that interfere with fundamental human rights" (A/68/167 and A/71/199).

Under Article 17 of the International Covenant on Civil and Political Rights (ICCPR), everyone has the right to be protected against "arbitrary or unlawful interference with his privacy, family, home or correspondence". Further, Article 19 of the ICCPR protects the right of everyone to freedom of expression, including the 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 one's choice. As is well documented, Articles 17 and 19 of the ICCPR are closely connected, as the right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression (see A/HRC/23/40 and A/HRC/29/32). Surveillance measures can only be justified when it is prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued. Surveillance, in addition to interfering with the private life of individuals, also interferes directly with the privacy and security necessary for freedom of opinion and expression, and always requires evaluation under articles 12 and 19 of the Universal Declaration of Human Rights (A/71/373).

If allegations that journalists were targetted are confirmed, it would be a serious violation of State obligations to media freedom under international human rights law. Furthermore, if human rights lawyers had their communications compromised, this may have violated their right "to carry out their functions in private and to communicate in conditions that fully respect the confidentiality of their communications, without influence or interference of any kind" (CCPR/C/GC/32, para. 34). The failure of NSO to conduct human rights due diligence on these mattters could amount to corporate complicity.

We would like to recall the recommendations made by the previous Special Rapporteur on freedom of opinion and expression in his 2019 report for a suitable legal and policy framework for regulation, accountability and transparency within the private surveillance industry (see A/HRC/41/35, para. 60). In particular, the Special Rapporteur called on companies to undertake human rights due diligence, regular audits of programmes, remedial mechanisms, enhanced transparency and cooperation with human rights experts and regular consultations with civil society. We reiterate his call "for a moratorium on the global sale and transfer of private surveillance

technology until rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways" (Ibid. para. 66).

Finally, we are deeply troubled by your statement of 19 July 2021 indicating that "NSO is considering a defamation lawsuit" against the authors of the investigative report. We have time and again called for effective measures to protect those who expose alleged wrongdoings by States or corporations from what are commonly known as strategic lawsuits against public participation or "SLAPPs". In its recent guidance on ensuring respect for human rights defenders (A/HRC/47/39/Add.2), the Working Group on Business and Human Rights underlined that SLAPPs are not only incompatible with responsible business, but engaging in them reflects poor strategic sense, as they destroy any credibility of the corporate commitment to respect human rights. We reiterate that such civil and criminal legal lawsuits have a devastating chilling effect on the legitimate work carried out by human rights defenders, journalists and civil society actors, and we would thus urge your company to refrain from such actions.

Given the serious allegations and in keeping with our responsibility, under the mandates provided to us by the Human Rights Council to seek to clarify all cases brought to our attention, we would be grateful for your response on the following matters:

1. Please provide any additional information and comment(s) which you may have on the above-mentioned allegations.

2. Please provide detailed information as to the measures, including human rights due diligence, that your company has taken in line with the Guiding Principles to identify, prevent, mitigate and account for adverse human rights impacts caused by your company's products and services, or to which they may have contributed or be directly linked.

3. Please provide information as to the process adopted and criteria applied by your company in vetting governments' law enforcement and intelligence agencies prior to the sale or supply of technology, and what ongoing measures you have in place to ensure their compliance with human rights obligations in the deployment of such technologies.

4. Please provide information as to the steps that your company has taken, or is considering to take, in line with your responsibility under the Guiding Principles, to ensure that Pegasus spyware is not sold to, or used by, States or State agencies that may violate international human rights norms and standards.

5. In your first annual transparency and responsibility report (June 2021, page 5), you note that you "plan to focus in particular on assessments of the impact of potential misuse of our products in connection with the media and journalists". Please provide any further information about such assessments that you may have undertaken since the report was published, or that you plan to undertake in the near future.

6. If you consider the allegations above to be accurate, please provide information on any action taken to halt the human rights violations identified and to provide remedies for victims, including, where possible, an ex post notification that they were placed under surveillance or that their data was hacked. Please also identify any grievance mechanisms or channels that your company has for victims or other individuals to report alleged misuse of your technology, and how your company responds to allegations received via this channel.

7. Please provide detailed information on any measures your company has taken to identify, prevent and mitigate any allegations of surveillance, intimidation and harassment of journalists, human rights defenders and politicians.

This communication and any response received from your company will be made public on the communications reporting website within 60 days. They will also subsequently be made available in our regular report to the Human Rights Council.

While awaiting a reply, we urge you to take all necessary interim measures to halt the alleged violations and prevent their re-occurrence and in the event that the investigations support or suggest the allegations to be correct, to ensure the accountability of any person(s) responsible for the alleged violations.

We may publicly express our concerns in the near future as, in our view, they are a matter of public interest. The press release will indicate that we have been in contact with your company to clarify the issues in question.

A letter raising these issues has been sent to the Government of Israel.

Please accept, Mr. Hulio, the assurances of our highest consideration.

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

Surya Deva
Chair-Rapporteur of the Working Group on the issue of human rights and transnational corporations and other business enterprises

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

Mary Lawlor
Special Rapporteur on the situation of human rights defenders