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

REFERENCE:
OL OTH 2/2020

20 February 2020

Dear Mr. Hulio,

Thank you for your letter of 10 December 2019, in which you responded to my letter of 18 October 2019. I appreciate your stated commitment to the UN Guiding Principles on Business and Human Rights, which distinguishes NSO Group from other companies in the private surveillance industry. You also indicated that NSO Group is "now designing and implementing enhanced procedures and governance structures to ensure full adherence" to human rights and whistleblower protections policies. I look forward to learning details of that design and implementation.

Notwithstanding your responsiveness, I remain concerned that your articulation of commitment to the Guiding Principles does not ensure protection and remedy for those unlawfully targeted by governments using your company's technology. The prevention of acts of terrorism and other serious crimes is undeniably a legitimate, even essential, aim of law enforcement and security agencies, and I understand that such use is what NSO Group aims to facilitate. Yet my question remains: given the extensive and credible allegations of abuse of human rights using NSO Group technologies, what are you doing to identify, rectify and prevent abuse and remedy violations? What are you doing to ensure not only that your technology is not subject to misuse but also that NSO Group employees do not engage in any facilitation of such human rights violations?

NSO Group is not alone in the industry, of course, and I hope that our exchange is understood in global and industry-wide context, in which governments are abusing surveillance technologies to interfere with human rights and there is an extremely limited global framework to ensure the use of such technologies in accordance with human rights law. As you know, my report on the subject to the UN Human Rights Council in May 2019 (A/HRC/41/35) highlighted the limitations of the current framework at global and national levels and urged a moratorium on the sale and transfer of such surveillance technologies until legal mechanisms to govern their export and use are in place.

Many of the specific questions I raised in my initial letter remain unanswered, and I hope that you are in a position to respond to them. Rather than review those questions in detail, I would simply like to seek clarification concerning several points raised in your letter. The questions that follow are rooted in my effort to understand how exactly NSO Group implements a human rights policy assertedly grounded in the UN Guiding Principles.

Human rights due diligence

Your December letter begins by noting that you aim to "develop an approach to protecting human rights tailored to the specifics of technology suppliers to the lawful interception industry." Your use of the term "lawful" to modify "interception" is instructive. Because of its interference with privacy and the freedom of expression, among other rights, surveillance of any kind must satisfy the conditions of human rights law. (See, e.g., UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age (A/HRC/27/37), 30 June 2014; UN Special Rapporteur on freedom of opinion and expression, Report of the Special Rapporteur on the implications of States' surveillance of communications (A/HRC/23/40), 17 April 2013.) Under Article 17 of the International Covenant on Civil and Political Rights ("ICCPR"), individuals must be protected against "arbitrary and unlawful interference" with their privacy, family, home, or correspondence. Under Article 19 of the ICCPR, any restriction on freedom of expression – such as the use of surveillance technology against journalists, human rights defenders, and others – must be provided by law and necessary and proportionate to protect a legitimate objective.

Given this legal framework, what specific due diligence does NSO Group undertake to determine whether the end-user actually uses the technology consistent with human rights standards? You mention that you seek to identify "risks of misuse" of your technology that "may be unduly high" and that you "do not pursue the engagement" in such circumstances. How and by what standards do you determine whether a risk is "unduly high"? Does your assessment include an evaluation of whether the State deploys the technology in accordance with Articles 17 and 19 of the ICCPR? Since you do not define "risks of misuse," I would like to know whether you consider it to be a misuse if a State fails to provide basic legal safeguards, consistent with international human rights law, on the deployment of your technology. Moreover, do you reconsider, and have you reconsidered, relationships with end-user States that fail to meet fundamental rule of law standards? Would you please provide examples of implementation of such an approach?

Presumably in keeping with the UN Guiding Principles norm of ongoing evaluation and due diligence (Principle 17), your letter also notes that the use of your technology may be terminated for material breach of contract, and that you have "terminated relationships" when you have "concluded that customers have failed to abide by our contract." I would be interested to know more about this assertion, which echoes your Human Rights Policy. Would you please provide examples where NSO Group determined that the conduct by an end-user client constituted a material breach? Do your contracts include human rights provisions, and did the material breach involve interference with an individual's human rights? If so, what specific rights were involved and who was the end-user responsible? Was the human rights violation the basis for asserting the material breach? Did your termination of relationships end all engagement with the end-user State, or only the specific end-user agency? Did you take action to report such breaches to law enforcement authorities, to Israeli export authorities, or to a victim of abuse?

Operational visibility and monitoring

You assert in your letter that NSO Group is "limited by the technological and commercial boundaries of our products to track each specific usage" and that, given the nature of government security investigations, "operational visibility is simply not permitted." I would like to understand the scope of this assertion. Such a claim appears to be at odds with an interview that you gave to Ynet Media journalist Ronen Bergman last year (*Weaving a cyber web*, Ynet, 1 November 2019). Bergman asked, "Were you involved in the Khashoggi murder?" The interview quoted you as saying the following:

> "We conducted a thorough inspection of all of our clients, not just the one client who could perhaps be a potential suspect for involvement in the affair, but also other customers who may for some reason have had an interest in monitoring him. We also checked whether maybe someone went to a certain other country and asked their intelligence services 'to do him a favor.' We checked all of our clients, both through conversations with them and through technological testing that cannot be forged. The systems have records and it is impossible to act against a target such as this without us being able to check it."
>
> After all these tests, I can tell you, in an attributed quote, that Khashoggi was not targeted by any NSO product or technology, including listening, monitoring, location tracking and intelligence collection."

Could you please explain what constituted a "thorough inspection" of your clients? Could you please identify the process by which you identified the relevant clients and "other customers"? Could you also please explain what you meant by "technological testing that cannot be forged" and "[t]he systems have records and it is impossible to act against a target such as this without us being able to check it"? Does this indicate that NSO Group does in fact have the ability to achieve some measure of "operational visibility"? If you do enjoy this visibility, would you please explain further how and under what circumstances you exploit this technological advantage? If you do not have such visibility, how do you undertake appropriate human rights monitoring and due diligence in accordance with your stated policy?

Licensing practices

You write that your "licenses are limited in volume, geography, and duration". Would this mean that you license the technology for a specific number of usages, against a certain number of targets located in specific areas, or does it indicate some other kind of limitation? Does your transfer of technology entail that you receive information from the end-user of the specific intended usage of the NSO Group product? Or does it involve a generic assertion of use, as an example, for "counter-terrorism purposes"? What kind of due diligence do you undertake to be certain that such a legitimate use will be made?

Whistleblower policy

Your December letter briefly addressed whistleblowing in a reiteration of your published whistleblower policy, and thus my concerns and questions remain the same.

1. What is the scope of protected disclosures?

2. What are the specific confidentiality guarantees for whistleblowers?

3. How are the investigators or team of investigators appointed? How is their independence and impartiality ensured? There does not seem to be an independent nature of this process and an internal investigative team is counterintuitive to whistleblowing as a principle.

4. What classifies as a malicious allegation? What is considered a genuine concern?

In keeping with my own commitment to transparency in the work of my mandate, I will be making a copy of this letter available to the public and posting it on the website page for the mandate of the Special Rapporteur on the right to freedom of expression. A copy of this letter is sent also to the Government of the State of Israel. This communication, as well as any response received, will also be made available in the communications reporting website of the OHCHR within two working days. It will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Sincerely,

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