

14 08 2019



**Ivan Penchev**

Director of the International Controlled Trade and Security Directorate  
International Trade Control  
Department Ministry of Economy  
Sofia, 8 Slavianska Str.

C/C

Ms Maya Manolova, Ombudsman of the Republic of Bulgaria

**Subject: Re: Investigation into export licenses to the NSO Group**

Dear Mr. Penchev,

We write to you to follow up on our [14 May letter](#) requesting an investigation into export licenses for NSO Group's surveillance technology. Since our last letter, several developments have taken place regarding NSO Group and the surveillance technology sector broadly. We would like to take this opportunity to draw your attention to these developments, and to reiterate our previous request for information regarding NSO Group export licenses.

The new [thematic report](#) to the UN Human Rights Council issued this June by the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, focuses on the human rights obligations imposed by law on States and the related responsibilities of companies. The Special Rapporteur **recommends a moratorium on the export and use of targeted surveillance technology such as NSO Group's Pegasus spyware** until an appropriate legal framework is agreed upon. We remain concerned that [Bulgarian authorities have issued](#) export licenses to NSO Group, whose tools have contributed to human rights abuses and heavily contributed to the need for an international moratorium on their trade and use.

The Special Rapporteur cites the surveillance technology sector's unwillingness to comply with human rights law and the consequent difficulty of current export controls to adequately compensate for this irresponsible and unacceptable practice. Kaye writes that "[surveillance technology] companies have not disclosed instances of meaningful action, such as putting in place due diligence processes that identify and avoid causing or contributing to adverse human rights impacts through their own activities and that prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships".

Responding to this continued lack of action in the wake of numerous purported human rights abuses tied to NSO Group, the Special Rapporteur suggests an immediate moratorium on the export and use of its spyware and similar technologies everywhere. He further suggests that states work to establish mechanisms to ensure they only grant export licences if a company “regularly demonstrates that it has rigorously implemented its responsibilities under the Guiding Principles with respect to the design, sale, transfer or support of such technologies.” Kaye emphasizes throughout the report that existing dual-use technology export standards have not sufficiently accounted for human rights. Thus, it is imperative that States establish mechanisms to engage all stakeholders in the decisions of their export controls regimes and develop a “framework by which the licensing of any technology would be conditional upon a national human rights review and companies’ compliance with the Guiding Principles on Business and Human Rights”.

Meanwhile, further reports [confirm the role](#) that NSO Group products played in the attacks on human rights lawyers via messaging application WhatsApp. The United States Department of Justice has commented that it is aware of this attack facilitated by NSO Group’s spyware. Additionally, Omar Abdulaziz, a Saudi dissident living in Montreal, [has alleged](#) that Saudi government officials used NSO Group’s spyware to track communications with Jamal Khashoggi, a journalist who was killed in October of last year. UN Special Rapporteur Agnes Cammallard [reports](#) that there is “credible evidence” that Saudi Prince Mohammed bin Salman was involved in Khashoggi’s murder. These reported attacks are not in isolation and NSO Group is not alone; [dozens of spyware firms offer technologies](#) with similar capacities to NSO Group’s Pegasus spyware. The threat that these tools pose to civil society, activists, journalists, and dissidents, is only further compounded by the legal uncertainty regarding the abuses tied to the sector and continued lack of scrutiny by export regimes on the matter. Now, more than ever, it is necessary for export control authorities to increase scrutiny of not only NSO Group, but of similar products and services.

When we last wrote, we sent a similar letter to the Cypriot export authorities, as [findings tell us](#) that licenses have been issued through these two countries. This past week, Cyprus responded to our first inquiry. Bulgaria therefore remains the only actor who has not provided us with answers and transparency; we implore you to clarify your role in exporting and trading NSO Group Products in the EU.

It is our understanding that the Bulgarian authorities have issued export licenses for NSO Group in the past and are likely to be approached for similar efforts in the future. Given the information we have presented, we reiterate the suggestions we offered in our 14 May

14 08 2019



letter to start working to resolve this issue and continue to stress the rising urgency of this matter:

**Recommendations:**

---

1. Clarify whether you require NSO Group or similar surveillance technology exporters to obtain a license for intra-EU exports, and whether such export licenses have been granted, to your knowledge, in the past 5 years;
  2. Disclose details of any instances where, after consultation with NSO Group or internal deliberation, your authorities decided an export license was not necessary under local or EU law;
  3. Review surveillance technology licenses which have been issued in the past 5 years, with attention to the procedures followed, and to the actual or potential human rights impacts of any licenses granted;
  4. Share results of any investigation regarding NSO Group, to the extent legally permissible, including information on classification, capabilities, and intended end uses of the controlled technology, and parties to the export;
  5. Clarify whether and under what circumstances you require assessment of the potential human rights impacts of exports, and if so, how such assessments generally impact license determinations; and clarify, specifically, whether your authorities have undertaken or otherwise obtained a human rights impact assessment involving NSO Group, at any point, and how the assessment was used;
  6. Take further positive action in promoting human rights by carefully scrutinizing any further or renewed technology exports or transfers from NSO Group, its affiliates, or similar surveillance technology exporters to ensure their potential human rights impacts are evaluated and steps are taken to prevent adverse impacts.
- 

We remain at your disposal for any further information we might provide to aid your efforts, as well as to organise a meeting or conference call if that would be helpful.

Thank you in advance for your response and best regards,

Guillermo Beltrà

14 08 2019



**Access Now (<https://www.accessnow.org>)** defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For More Information, please contact:

**Peter Micek** | General Counsel | [peter@accessnow.org](mailto:peter@accessnow.org) | +1-888-414-0100 x709

**Guillermo Beltrà** | Policy Director | [guillermo@accessnow.org](mailto:guillermo@accessnow.org)