From: [redacted]

To: European Data Protection Supervisor <EDPS@edps.europa.eu>

Sent at: 01/03/22 00:53:36

Subject: Letter from NSO

Dear Sirs,

Please find attached NSO's letter to Mr. Wiewiorowski.

Best regards,

[redacted] **| Legal & Compliance Department| NSO Group**

NSO GROUP

February 28, 2022

Wojciech Wiewiorowski
European Data Protection Supervisor
60, Rue Wiertz /Wiertzstraat
1047 Brussels, Belgium

Dear Mr. Wiewiorowski,

NSO Group Technology ("NSO") has read with great interest, and with an increased level of disappointment, your "Preliminary Remarks on Modern Spyware" Report ("report"), dated February 15, 2022.

Given that the report is very much, if not exclusively, focused on one of our technologies known as "Pegasus" we would greatly welcome the opportunity to provide our subject matter expertise and insights to your collective efforts to craft polices that incorporate our shared commitment to defend the rights to privacy and data protection of the EU citizens while ensuring the public safety of such EU citizens.

In the last few months, NSO has been featured prominently recently in the media, primarily as a result of reports compiled by advocacy organizations that rely on allegations and "evidence" that we were never provided with and which we at NSO could easily verify and/or refute. Consequently, these reports, based on assumptions and premises that have not been properly assessed by and verified with us, have been used to construct a narrative that presents the public with what we consider to be a distorted view of NSO, Pegasus and cyber intelligence industry.

We have repeatedly cooperated with governmental investigations, as these are the legitimate fora to determine misuse (if any) and it is in that spirit that we write to you to clarify a number of misrepresentations contained in your report.

Background

NSO's mission is to save lives and create a safe public space for civilians, a mission that has been successful in the past decade, preventing dozens of terror attacks, aiding in the apprehension of pedophiles, human traffickers and drug lords, many of them across the European Union by government agencies of EU members. Our technologies were developed as response to a critical need by law enforcement and intelligence agencies, as they struggled to monitor the activities of terrorists, drug cartels and other criminals, who are communicating via off-the-shelf mobile applications utilizing end-to-end encryptions offered by various communications platforms, allowing them to "go dark". Traditional investigative techniques,

such as wiretapping, are becoming irrelevant. Instead, Pegasus allows the investigators to operate on a hard-wired, pre-identified small set of numbers, one at a time, instead of the previously common mass-surveillance methods.

Importantly, NSO does not operate Pegasus and is not privy to the data collected. We provide the system to our customers, law enforcement and intelligence agencies of states and government agencies, and they use our technologies subject to Israeli government export authorizations and our own human rights governance program, which will be detailed below, as well as the respective local judicial systems.

The Report

Based on our review of your report, we note with regrets that it contains several assertions based on a misunderstanding of the technology:

1. On the report's page 4, section 2, the report states "one cannot exclude the possibility of using Pegasus beyond mere interception capabilities". - Pegasus software is an intelligence gathering tool solely, and cannot be used for any other purposes based on contracts, technological capabilities provided with the system, and the End User Certificate issued to the customer by the Israeli Ministry of Defense.

2. On the report's page 4, section 2, the report states that it (Pegasus?) could impersonate the victim" – Pegasus is unable to manipulate data on a target's phone (like sending messages on their behalf). Pegasus is designed with surveillance and data gathering capabilities and it is incapable of impersonating a victim.

3. On page 5, section 2, the report states that "all traces of the software vanishes" - while turning down the phone, and that "the attack infrastructure is in the cloud" - While Pegasus is indeed hard to detect on a target's phone, it has a built-in investigative capability, in case a misuse is suspected, that making it impossible to erase and/or manipulate. Those capabilities cannot be completely vanished, and an "audit trail log" exists permanently, with the ability to retroactively check whether or not a certain phone number was hacked. NSO has been granted access by its customers to performed this type of investigation many times in the past, when an allegation of misuse arose, leading to shut down of systems and termination of seven contracts to date. Without this consent we are not privy to the phone numbers that are the subject of our customers' investigations.

4. On page 6, section 2, the report states that Pegasus creates "permanent and strong risk of massive security breaches…, comparable in a way to encryption backdoors". This statement is incorrect : the data collected by the customers is NOT stored in the cloud,

any cloud, and there are no backdoors to the system. There is no shared data base of NSO's customers, contrary to some media reports, and the logs securely exists only on the servers of the customers, for the sole purpose of investigation of improper use. The Pegasus system allows for targeted surveillance only, with customers receiving license for a limited number of concurrent targets and is therefore inherently less intrusive then a backdoor. In this light we refer you to the recent interview of the Belgian Minister of Digitalisation and Privacy Mr. Mathieu. On that occasion Minister Mathieu stated he did "not agree with lowering the level of security and privacy of all Belgians' messages in order to conduct investigations from time to time. It's as if, because the police and the justice system do searches from time to time, everyone should leave their back door open". In this context Minister Mathieu further argued that "today we have technological means to access tapping other than by degrading the level of security of all Belgians. Look at the Pegasus software"[1].

5. On page 6, section 3, the report states that you are basing your claims for misuse of our products on "worldwide media investigations." As stated earlier in this submission, these "worldwide media investigations" contain a number of assumptions and premises that are wrong. Most recently, the Israeli news outlet Calcalist published a story dubbed "The Pegasus Affair" claiming that the Israeli police used Pegasus to infiltrate phones without a warrant, essentially conducting mass-surveillance of high-profile politicians, opposition leaders and activists, without the proper legal authority. The Deputy Attorney General along with representatives of the Mossad and the Shin Bet announced the findings of their investigation into the allegations. Their report found no evidence of wrongdoing. Shortly thereafter, Calcalist announced an investigation into their reporting to determine what went wrong. Unfortunately this scenario has repeated itself throughout the past several years. We have patiently responded to hundreds of media inquiries, walking reporters through our due diligence program, pointing to the release of our Transparency and Responsibility Report and stating that while we are restricted in what we can say due to confidentiality and national security issues, many of these allegations are wrong and, in some cases, they were contractually and technologically impossible. For example, the allegation which claimed that our products were misused on President Emmanuel Macron, Jeff Bezos, and Jamal Kashoggi is not true; they were never targeted by NSO's products.

Human Rights and Compliance Programs

[1] https://www.rtl.be/info/belgique/politique/mathieu-michel-s-oppose-a-vincent-van-quickenborne-et-veut-s-en-prendre-a-tik-tok-1332188.aspx. Listen in particular to the extract from 5m and 30 sec to 7 m.

NSO Group is acutely aware of the inherent human rights challenges and potential for misuse and the need for such tools to be used responsibly and for the purpose they were designed. To combat potential misuse, the Company has developed a thorough governance framework and has publicly committed to adhering to the UN Guiding Principles on Business and Human Rights ("UNGPs") and the OECD Guidelines for Multinational Enterprises ("OECD Guidelines"). These commitments are reflected in the Company's Human Rights Policy ("HR Policy").

We conduct rigorous due diligence on all of our prospective clients. No sale of NSO's Pegasus cyber intelligence tool can or will occur unless and until the following multiple conditions have been met:

- The potential customer is a government law enforcement or intelligence agency (e.g., Pegasus is not available for sale to, or use by, individuals or private companies);
- NSO has been granted a marketing license by the Israeli government to speak with that specific potential customer;
- We have completed an internal review of the potential customer concluding that the government and its specific agency users do not present a significant risk of using Pegasus in a manner that would violate United Nations-defined human rights standards;
- All sales of Pegasus are subject to requesting a license from the Israeli and them approving it following a rigorous review process ;
- The customer signs an End User Agreement with the Israeli government requiring immediate revocation of the export license if the Pegasus tool is used for any purposes other than lawful counter-terrorism, or other specified lawful purposes;
- The Company incorporates human rights compliance clauses in all customer agreements, requiring additional human rights-related assurances based on identified risks or mitigation measures;
- NSO's licenses limit the maximum number of devices that can be monitored, which also reduces the risk it will be used for reasons other than legitimate law enforcement or for mass surveillance; and
- Where a customer is accused of misusing technology, the Company investigates immediately and takes prompt remedial action, including termination where appropriate.

We deeply abhor any alleged or actual misuse of our products and, while we maintain our position that a number of media reports were not accurate we ,are especially troubled by credible allegations that our products may have been, or actually were, used in a manner that could have enabled improper or otherwise abusive surveillance of journalists, human rights advocates, and others. Any customer using Pegasus in this manner is in clear and egregious violation of all commitments and agreements they have made with us. Limiting the possibility of product misuse is a core value of NSO and we are undertaking several investigations to assess the reality of certain allegations.

The need for a global standard

NSO's standards are higher than the export controls of most States including those of the European Union, but the same cannot be said of a number of other companies operating in our area of business. The company has been advocating for a international regulation for responsible use of such technologies for some time. This is why NSO has repeatedly expressed its strong support for such international sector-specific standards and regulation, and we hope a dialogue aimed at delivering effective regulation can now be reinvigorated. Given this leadership and our practical experience establishing and working to continually improve our Human Rights Program, we believe NSO can bring a useful perspective and a valuable contribution, we are committed to doing so. We appreciate that such a dialogue with international bodies like the EDPS regarding sector standards and regulations may be a longer-term objective but we are ready to enter into such a dialogue in good faith.

EDPS Meeting Request

We recognize that cyber intelligence is a complicated and sensitive issue, which is why it is critical, and incumbent for a company as NSO to serve as a necessary resource to detail how Pegasus operates and the compliance processes NSO implements to ensure proper use of its products. We would therefore appreciate the opportunity to further expand on any of the points raised in this letter and answer any questions in a meeting (be it virtual or face to face) with EDPS as well as other interested stakeholders.

We look forward to your response.

Sincerely,

[redacted]

NSO Group Technologies Ltd.

NSO Group Technologies LTD I22 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