JOSEPH N. AKROTIRIANAKIS (Bar No. 197971)
jakro@kslaw.com
AARON S. CRAIG (Bar No. 204741)
acraig@kslaw.com
KING & SPALDING LLP
633 West Fifth Street, Suite 1700
Los Angeles, CA 90071
Telephone: (213) 443-4355
Facsimile: (213) 443-4310
Attorneys for Defendants NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CARLOS DADA, *et al.*,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LTD. and Q CYBER TECHNOLOGIES LTD.,

Defendants.

Case No. 3:22-cv-07513-JD
[*Honorable James Donato*]

DECLARATION OF YARON SHOHAT IN SUPPORT OF MOTION TO DISMISS OF DEFENDANTS NSO GROUP TECHNOLOGIES LIMITED AND Q CYBER TECHNOLOGIES [FED. R. CIV. P. 12(B)(2), (B)(6), FORUM NON CONVENIENS]

[Filed Concurrently with Notice of Motion and Motion to Dismiss and [Proposed] Order]

Date: May 25, 2023
Time: 10:00 a.m.
Ctrm: 11

Action Filed: 11/30/2022

I, Yaron Shohat, declare as follows:

1. I am a citizen and resident of Israel. I am currently the Chief Executive Officer of Defendant NSO Group Technologies Limited ("NSO") and I was the Chief Operating Officer of NSO at all times relevant to this case, including from February to November 2021. Defendant Q Cyber Technologies Limited ("Q Cyber" and, collectively with NSO, "Defendants") is NSO's sole director and majority shareholder.

2. I have personal knowledge of the facts set forth herein and, except as otherwise stated, could testify competently to each fact averred herein.

3. NSO is a technology company that designs and licenses technology to governments and government agencies for national security and law enforcement purposes.

4. Defendants are incorporated and have their principal places of business in Israel. As Israeli corporations, Defendants are subject to service of process in Israel. Defendants have no presence in any other country. Defendants do no business in California and have no offices or employees in California or elsewhere in the United States. Defendants have not performed any actions relevant to Plaintiff's lawsuit in California, and they have not targeted any activities relevant to the lawsuit at California. All of Defendants' employees with knowledge relevant to this lawsuit reside in Israel, and any documentary evidence relevant to the case is located in Israel.

5. Sales of NSO's Pegasus technology are strictly monitored and regulated by the Government of Israel. The export of NSO's Pegasus technology is regulated under Israel's Defense Export Control Law ("DECL"), with which I was very familiar as NSO's COO during all times relevant to this case. A copy of the DECL is attached as **Exhibit A**.

6. To export its Pegasus technology, NSO is required to register with the Israeli Ministry of Defense ("MoD"). Under the DECL, the MoD is empowered to investigate NSO and its business, refuse or cancel NSO's registration, or deny NSO's license, taking into account several factors, including the intended use of NSO's Pegasus technology and the identity of NSO's customers. The MoD can and does ask NSO to provide documentation about its customers and prospective customers and the intended uses of NSO's Pegasus technology by NSO's customers and potential customers. The MoD requires this documentation from NSO for each export of

NSO's Pegasus technology.

7. NSO's contracts require Pegasus end-user customers to demonstrate that they are a government or an authorized agency for national security and law enforcement purposes of a government and to provide any other necessary documentation for approval by the MoD.

8. The MoD requires the NSO provide it with signed certificates from the end-users of NSO's Pegasus technology in which the end-users declare that NSO's Pegasus technology will be used only for prevention and investigation of terrorism and criminal activity.

9. NSO markets and licenses its Pegasus technology exclusively to sovereign governments and authorized agencies for national security and law enforcement purposes of governments and does so only after receiving the necessary export control licenses from the MoD. NSO does not market or sell its Pegasus technology for use by any private entities, and any allegation made to the contrary is false.

10. Contrary to Plaintiff's false allegations, at all times relevant to this case, including from February to November 2021, Defendants did not operate NSO's Pegasus technology. Instead, NSO marketed and licensed the Pegasus technology to its sovereign government customers, which then operated the Pegasus technology themselves, to advance their own sovereign interests of fighting terrorism and serious crime. Defendants' role was limited to NSO providing advice and technical support to assist customers in setting up—not operating—the Pegasus technology.[1] When Defendants provided those support services, they did so entirely at the direction of their government customers, and Defendants followed those directions completely. Defendants' operation of the Pegasus technology NSO has licensed to sovereign governments and agencies for national security and law enforcement purposes is also prohibited under each export control license NSO has been granted. Each of the licenses NSO has been granted provides that operational use or ongoing operation of Pegasus by NSO employees (or their subcontractors) is prohibited, and that operation of Pegasus by NSO employees (or their subcontractors) is permitted only for demonstration purposes and on devices owned by NSO. Each export control license NSO

[1] Defendants do not participate in any NSO customer's installation of the Pegasus technology on any device.

has been granted further requires that NSO's remote access to Pegasus technology licensed to a customer is permitted solely for purposes of maintenance (which is not related to operation of Pegasus).

11. Plaintiff alleges that Defendants used Pegasus to monitor journalists, human rights activists, political dissidents, diplomats, and other senior government officials. That is false. At all times relevant to this case, including from February to November 2021, Defendants did not monitor anyone, and Defendants prohibited their customers from using the technology for purposes other than fighting terrorism and serious crime, by contractual prohibitions against such behavior and required end-user certificates signed by the customer. If a government ever misused NSO's Pegasus technology to monitor Apple users for purposes other than fighting terrorism and serious crime, Defendants have no knowledge of that misuse, which would be a violation of that government's contract with NSO. If Defendants suspected any improper use of Defendants' Pegasus technology outside these parameters, service to that customer would be suspended pending investigation. If investigation revealed such ongoing misuse, that customer would be terminated. NSO does not collect or store any information collected by its customers.

12. At all times relevant to this case, including from February to November 2021, because NSO's government customers used Defendants' technology to investigate and prevent terrorism and crime, discovery into Defendants' customers' use of the technology would require sovereign governments to reveal sensitive information about their national-security, intelligence, and law enforcement operations.

13. At all times relevant to this case, including from February to November 2021, all of NSO's customers are located outside of the United States. If any of NSO's government customers have witnesses or evidence relevant to this lawsuit, those witnesses and that evidence would be located outside of the United States.

14. Defendants have no control over, or knowledge of, where Apple chooses to install and maintain any of its servers, which Apple server(s) would be used to transmit any communications with Apple, or where those servers are located.

I declare under the penalty of perjury and the laws of the United States that the foregoing is true and correct this 9 day of March 2023, at Tel Aviv, Israel.



YARON SHOHAT