JOSEPH N. AKROTIRIANAKIS (Bar No. 197971)
jakro@kslaw.com
ZACHARY W. BYER (Bar No. 301382)
zbyer@kslaw.com
MATTHEW NOLLER (Bar No. 325180)
mnoller@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

APPLE INC.,

Plaintiff,

v.

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No. 3:21-cv-09078-JD

DECLARATION OF SHALEV HULIO IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

Action Filed: 11/23/2021

I, Shalev Hulio, declare as follows:

1. I am a citizen and resident of Israel. I am the Chief Executive Officer and a co-founder of Defendant NSO Group Technologies Limited ("NSO"). 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 their authorized 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 the United States. 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, not California, and any documentary evidence relevant to the case is located in Israel.

5. Sales of Defendants' Pegasus technology are strictly monitored and regulated by the Government of Israel. The export of the technology is regulated under Israel's Defense Export Control Law ("ECL"), with which I am very familiar as NSO's CEO. The ECL imposes strict limits on the information covered parties may disclose outside of Israel. A copy of the ECL is attached as **Exhibit A**.

6. To export its technology, including NSO's Pegasus software, NSO is required to register with the Israeli Ministry of Defense ("MoD"). Under the ECL, 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 technology and the identity of its customers. The MoD can and does ask NSO to provide documentation about its customers and prospective customers and the intended uses of NSO's technology by NSO's

customers and potential customers. The MoD requires this documentation from NSO for each intended use of NSO's technology.

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

8. The MoD requires the end-users of NSO's Pegasus technology to sign end-use certificates declaring that NSO's technology will be used only to investigate terrorism and serious crime.

9. NSO markets and licenses its technology exclusively to governments and their authorized agencies for national security and law enforcement purposes and does so only after receiving the necessary licenses from the MoD. NSO does not market or sell its technology for use by any private entities.

10. NSO takes into account U.S. and European Union export control restrictions. NSO conducts due diligence of potential customers, including examining publicly available information, evaluating questionnaires, and considering the potential customer's record of respecting rule-of-law concerns. Government customers must provide due diligence materials before receiving NSO's technology.

11. NSO requires, as a condition of use, that its government customers agree that they (1) will use NSO technology only for the prevention or investigation of serious crimes and terrorism and ensure that it will not be used for human rights violations and (2) will immediately notify NSO of any potential misuse. NSO contractually can suspend or terminate service to customers engaged in any improper use of its products outside these parameters and NSO has done so in the past when improper use has been uncovered. Moreover, the State of Israel may deny or revoke export licenses if it becomes aware the terms of the export license have been violated, including, for example, that the technology is being used to violate human rights.

12. NSO's technology also has technical safeguards, such as general and customer-specific geographic limitations. One of the limitations relevant to this case is that NSO's Pegasus technology cannot be used against U.S. mobile phone numbers. Another such limitation is that

the Pegasus technology cannot be used against a device within the geographic bounds of the United States.

13. Contrary to Plaintiff's false allegations, Defendants do not operate any of their technologies. Instead, Defendants market and license the technologies to their customers, which then operate the technologies themselves, to advance their own interests of fighting terrorism and serious crime. Defendants' role is limited to providing advice and technical support to assist customers in setting up—not operating—the technologies.[1] When Defendants provide those support services, they do so entirely at the direction of their government customers, and Defendants follow those directions completely.

14. Defendants' operation of Defendants' technologies that have been licensed to governments and their authorized 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 the systems by company employees (or their subcontractors) is prohibited and NSO makes sure to comply with its licenses' restrictions. Each export control license NSO has been granted further requires that NSO's remote access to systems licensed to a customer is permitted solely for purposes of maintenance (which is not related to their operation) and subject to customer's approval.

15. If an NSO customer installs NSO's technology on a particular device, it does so acting on its own behalf to advance its own interests, and it does so without Defendants' involvement.

16. Defendants do not use their technology to monitor anyone, and Defendants prohibit 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 foreign government ever misused NSO's technology to monitor any users' devices for purposes other than fighting terrorism and serious crime, that would be a violation of that government's contract with NSO. If Defendants suspected any improper use of

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

Defendants' technology outside these parameters, service to that customer would be suspended pending investigation. If investigation revealed such ongoing misuse, that customer would be terminated. Defendants have, in fact, terminated customers for misuse of Defendants' technology.

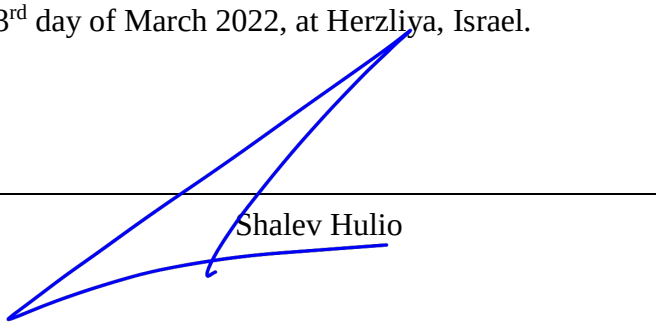
17. Defendants have no knowledge of or control over the information, if any, a customer may have collected from any Apple user's device. It is thus impossible for Defendants to "identify the location of any and all information obtained . . . and to delete all such information," as the injunction Plaintiff requests would require. (Compl. Prayer for Relief ¶¶ A–B.) In order to receive that relief, Plaintiff would have to receive an injunction against Defendants' customers.

18. Defendants have no control over or knowledge of where Plaintiff's servers are located or of which server(s) would be used to send or receive any information involved in the design, testing, and use of Defendants' technology.

19. Since Defendants' government customers use Defendants' technology to investigate and prevent terrorism and serious crime, discovery into Defendants' customers' use of the technology would require foreign governments to reveal sensitive information about their national security, intelligence, and law enforcement operations.

20. If any of Defendants' government customers have witnesses or evidence relevant to this lawsuit, those witnesses and that evidence would be located outside of the United States.

I declare under the penalty of perjury and the laws of the United States that the foregoing is true and correct this 3rd day of March 2022, at Herzliya, Israel.



Shalev Hulio