

DISSEMINATED BY MERCURY PUBLIC AFFAIRS, LLC, A REGISTERED FOREIGN AGENT, ON BEHALF OF Q CYBER TECHNOLOGIES LTD. MORE INFORMATION IS ON FILE WITH THE DEPT. OF JUSTICE, WASHINGTON, DC.

Good Morning:

Please find attached to this email four (4) new legal documents just filed by US counsel for NSO Group to the United States District Court for the Northern District of California, in the case WhatsApp Inc. v. NSO Group Technologies Limited (4:19-cv-07123).

These new filings include a Motion to Dismiss the Complaint of WhatsApp and Facebook Inc., which outlines NSO's various positions on the merits of the lawsuit brought against it by WhatsApp/Facebook, and a support declaration made by NSO Group's CEO Shalev Hulio.

A third provided document is an extensive declaration made by lead Attorney Joseph Akrotirianakis. Mr. Akrotirianakis' describes, with supporting documentation, Terms of Service "Forum and Venue" language revisions advanced by WhatsApp approximately three months after it filed its suit against NSO Group. This material applies to the "personal jurisdiction" arguments presented by NSO in its Motion to Dismiss.

The fourth document is a proposed order for consideration by the court.

For ease of document navigation, and for your guidance only, please take particular note of the following key arguments set out in the Motion to Dismiss (MTD), and their corresponding sections.

These four filed documents speak for themselves, in great detail. We will not be offering further comment at this time.

NSO's KEY POSITION

(Excerpted directly from the MTD, Page 1)

Plaintiffs = WhatsApp/Facebook

Defendants = NSO Group

"...Plaintiffs bring this action to prevent Defendants from licensing NSO's Pegasus technology that enables sovereign governments to investigate and combat terrorism, child exploitation, and other heinous crimes.

Encrypting communications, like locking doors, serves important goals. As a collateral consequence, however, terrorists and criminals take advantage of Plaintiffs' services to plan and execute illegal schemes, while Plaintiffs disclaim all responsibility for the consequences. NSO supplies governments with a technology they can use to enforce their laws and protect their citizens, much as a manufacturer of a Slim Jim tool outfits police to unlock doors. In this case, however, NSO takes precautions so that only government agencies, not criminals, can use NSO Pegasus technology."

CORE ARGUMENTS IN RESPONSE TO THE WHATSAPP SUIT:

- The conduct alleged by WhatsApp was not and could not have been conducted by NSO

Group, as NSO Group simply licenses its Pegasus software to sovereign governments and their agencies for the purpose of preventing terrorism and other crimes. (MTD, Page 6)

- NSO does not operate its Pegasus system on behalf of its government clients. (MTD Pages 6-7)

- NSO does not sell Pegasus software licenses to private entities, and any such allegations presented by the plaintiffs, WhatsApp, are false. When approached in the past by private parties interested in obtaining access to the capabilities of the Pegasus tool, NSO Group has refused to sell to them. (MTD Page 2, Shalev Hulio declaration, Page 2)

- For this reason, Facebook, the owners of WhatsApp, were turned away by NSO in October of 2017, when they inquired directly to NSO Group about purchasing Pegasus capabilities. (MTD, Page 2, Shalev Hulio declaration, Page 2)

- The above-referenced section from the Hulio declaration (Page 2) is excerpted in full here:

“In October 2017, NSO was approached by two Facebook representatives who asked to purchase the right to use certain capabilities of Pegasus, the same NSO software discussed in Plaintiffs’ Complaint. From Facebook’s communications with NSO at that time, I understand that Facebook had purchased a web analytics company called Onavo in October 2013. Onavo had created a virtual private network (“VPN”) application called Onavo Protect, which analyzed web traffic sent through the VPN to provide statistics on the usage of other applications. Onavo Protect, which has frequently been categorized as “spyware,” allowed Facebook to gather information about Onavo Protect users, including the applications installed on those users’ mobile devices and the amount of time the users spent on each application. The Facebook representatives stated that Facebook was concerned that its method for gathering user data through Onavo Protect was less effective on Apple devices than on Android devices. The Facebook representatives also stated that Facebook wanted to use purported capabilities of Pegasus to monitor users on Apple devices and were willing to pay for the ability to monitor Onavo Protect users. Facebook proposed to pay NSO a monthly fee for each Onavo Protect user. Facebook is a private entity and not a sovereign government or government agency for national security and law enforcement purposes and therefore does not meet NSO’s customer criteria.”

- NSO licenses to government clients are heavily regulated by the Israeli Ministry of Defense (MoD), and are subject to Israeli export control restrictions. NSO conducts thorough due diligence of all potential new clients. (MTD, Pages 3-4)

- If anyone installed Pegasus on any alleged “Target Devices” it was not NSO Group. It would have been an agency of a sovereign government. (MTD, Page 6)

- Under US law, NSO’s government clients are shielded from US federal court actions by the Foreign Sovereign Immunity Act (FSIA) Exceptions to the FSIA would not apply to this case (MTD, Pages 8-10).

- WhatsApp has misapplied the Computer Fraud and Abuse Act (CFAA) in bringing this case. In fact, WhatsApp has failed to state a proper claim under the CFAA because WhatsApp’s

user agreement could not have been violated by the actions it has alleged. (MTD Pages 20 - 25).