Greg D. Andres
Antonio J. Perez-Marques
Craig T. Cagney
Gina Cora
Luca Marzorati
(admitted *pro hac vice*)
DAVIS POLK & WARDWELL LLP
450 Lexington Avenue
New York, New York 10017
Telephone: (212) 450-4000
Facsimile: (212) 701-5800
Email: greg.andres@davispolk.com
antonio.perez@davispolk.com
craig.cagney@davispolk.com
gina.cora@davispolk.com
luca.marzorati@davispolk.com

Micah G. Block (SBN 270712)
DAVIS POLK & WARDWELL LLP
1600 El Camino Real
Menlo Park, California 94025
Telephone: (650) 752-2000
Facsimile: (650) 752-2111
Email: micah.block@davispolk.com

Attorneys for Plaintiffs
WhatsApp LLC and Meta Platforms, Inc.

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

WHATSAPP LLC and META PLATFORMS, INC., a Delaware corporation, Plaintiffs, v. NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED, Defendants.	Case No. 4:19-cv-07123-PJH **REPLY DECLARATION OF DAVID J. YOUSSEF IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT** Action Filed: October 29, 2019

I, David J. Youssef, declare as follows:

1. I submit this reply declaration in support of Meta Platforms, Inc. and WhatsApp LLC's (collectively, "Plaintiffs") Motion for Partial Summary Judgment ("Plaintiffs' Motion") in the above-captioned action (the "Action").

2. I am employed as a Managing Director at FTI Consulting, Inc. in its Cybersecurity practice. I have been engaged by Plaintiffs' counsel to serve as a technical expert in this Action.

3. Attached as **Exhibit A** is a true and correct excerpt of the expert report I submitted on August 30, 2024 (the "Opening Report).

4. Attached as **Exhibit B** is a true and correct excerpt of the rebuttal expert report I submitted on September 21, 2024 (the "Rebuttal Report") in response to the report of Terrence McGraw, dated August 30, 2024.

5. I have personal knowledge of the facts set forth in this declaration, and of the opinions and bases for the opinions set forth in my Opening and Rebuttal Reports, including the excerpts in Exhibits A and B, and if called upon as a witness, I could and would testify truthfully to them.

6. I have reviewed the Declaration of Tamir Gazneli in Support of Defendants NSO Group Technologies Limited and Q Cyber Technologies Limited's (collectively, "NSO") Opposition to Plaintiff's Motion. (Dkt. No. 421-2 (Gazneli Decl.)). I have also reviewed code and configuration files, and software logs, all of which I understand were from an Amazon Web Services server (the "AWS Server") obtained from the U.S. Department of Justice. I also understand that NSO admitted it controlled the AWS Server and it housed certain "Pegasus code, Python scripts, [and] configuration files" during "periods prior to January 2021." Dkt. No. 339-1 (Gelfand Decl.) ¶¶ 6-8. The files from the AWS Server that I received are incomplete, and do not contain all of the code necessary to run all of NSO's installation vectors.

7. In my Opening Report, based on my review of the files from the AWS Server, Plaintiffs' documents, and the few documents produced by NSO, I opined that "Defendants were not using the official WhatsApp Client Application to carry out the exploit," but "[i]n place of a genuine WhatsApp Client Application, Defendants designed and used their own system, a

component of 'heaven' referred to internally by Defendants as the 'WhatsApp Installation Service' or 'WIS,' to emulate the official WhatsApp Client and send messages to the Target Device via the WhatsApp Signaling and Relay Servers, using authentication credentials taken from a registered WhatsApp Client to gain access to the servers." Ex. A at 27-28. In my Rebuttal Report, I noted that Mr. Gazneli's deposition testimony confirmed my opinion, because he admitted the WIS "was 'not an actual WhatsApp client' and only 'uses part of the protocol capabilities to be sent from one source to the target.'" Ex. B at 15-16 (quoting Gazneli Dep. at 161-162). In addressing Mr. Gazneli's claim later in his deposition that "the message is created by the WIS but transmitted through that WhatsApp client," I opined that "this testimony is misleading" because "I have seen no evidence that the WIS utilizes the legitimate WhatsApp Client Application, and the messages sent by Defendants' malware could not be sent by the legitimate WhatsApp Client Application without modifying it and bypassing its technological limitations." Ex. B at 16 (quoting Gazneli Dep. Tr. at 187-188). Based on Mr. Gazneli's description earlier in the deposition that the WIS "uses ***part*** of the protocol capabilities [of a legitimate WhatsApp Client Application] to be sent from one source to the target," in my opinion, the WIS appears to incorporate parts of the legitimate WhatsApp Client Application's code to send messages, and "Mr. Gazneli appears to be using 'WhatsApp client' to refer not to the legitimate WhatsApp Client Application, but to the messages sent 'through an active WhatsApp account,' using actual but misappropriated WhatsApp authentication credentials as explained in the [Opening] Report." Ex. B. at 16.

8. Mr. Gazneli repeats his claim in his Declaration that NSO used the WhatsApp Installation Server (the "WIS") to "create[] the WhatsApp messages" but "those messages were sent to the target device (via WhatsApp servers) using a genuine WhatsApp client." Gazneli Decl. ¶¶ 4-5. I am not aware of any documentary evidence supporting Mr. Gazneli's contention, and note that, once again, Mr. Gazneli does not specifically say the WIS's messages were sent using WhatsApp's genuine and unmodified WhatsApp client *application* (the "Official Client"), but only by what he refers to as "a genuine WhatsApp client," which as explained in my Rebuttal Report, appears to refer to a registered WhatsApp account, and not the Official Client. NSO has not produced any computer code for Pegasus that is available for my review, and Mr. Gazneli has not

provided any detail on how messages created by the WIS could be sent using an unmodified Official Client, which as explained in my Rebuttal Report, they could not. Ex. B at 16.

9. In fact, Mr. Gazneli's suggestion that WIS-created messages were sent using the Official Client is inconsistent with the computer code from the AWS Server used by the WIS for NSO's Heaven and Eden exploits. The code on the AWS Server does not include any mechanism by which the WIS could have interfaced with an unmodified Official Client for the purpose of sending the WIS-created messages to WhatsApp's servers. Instead, that code contains multiple technical indicators that the WIS was designed to interact directly with WhatsApp's servers, including domain names and ports associated with WhatsApp's Signaling servers, and functions for interacting with WhatsApp Signaling and Relay Servers.

10. For example, the AWS Server contained the following files used by the WIS, which contain the following indicators that they interacted directly with WhatsApp's servers:

Bates Number	File Name	Description
WA-NSO-00195098	[redacted]	Contains a list of domain names and ports associated with WhatsApp Signaling Servers, and functions for interacting with them.
WA-NSO-00195085	[redacted]	For communication using FunXMPP, WhatsApp's proprietary version of the XMPP instant messaging protocol, used for Chat and Signaling.
WA-NSO-00195088 / WA-NSO-00195137	[redacted]	For using Noise, a cryptography protocol used by WhatsApp for various functions.
WA-NSO-00195140	[redacted]	For interacting with Session Traversal Utilities for NAT, a networking protocol used by the WhatsApp Relay Servers.

11. [redacted] SSL pinning

is a security mechanism employed by the Official Client in 2019 by which the Official Clientwould associate certain devices, e.g. WhatsApp servers, with specific cryptographic certificates, in order to prevent the interception, modification, or redirection of traffic intended for those devices.

13. In my expert opinion, it would not have been possible for the Official Client to send messages created by the WIS to WhatsApp's servers, as described by Mr. Gazneli, unless the Official Client had been modified, or the traffic generated by the Official Client was intercepted and manipulated by the WIS and then sent by the WIS to WhatsApp's servers. NSO has not produced any technical documentation that shows, or even indicates, that this would have been possible using an unmodified Official Client.

14. In my Opening Report, based on my personal experience and research, I state that "the user's acceptance of WhatsApp's Terms of Service . . . must be done before completing the WhatsApp registration process," and "[o]nly once the sign-up process has been completed can the user access the WhatsApp services and the full functionality of the WhatsApp Client Application." Ex. A at 26-27.

15. Counsel for Plaintiffs has asked me to determine, to the extent possible, from publicly available materials how WhatsApp's registration process would have appeared to NSO in 2018 and 2019.

16. Based on the logs from the AWS Server, I identified two versions of WhatsApp targeted by NSO's exploit in 2018 and 2019 ("2.18.380-45261" and "2.19.98-452742"). I was then able to locate copies of the Android Package Kit ("APK") files for those versions of WhatsApp on APK Mirror,[1] an online repository that archives APK files for older versions of mobile Android applications. Version 2.18.380-45261 was uploaded to APK Mirror on December 13, 2018, and version 2.19.98-452742 was uploaded on April 10, 2019. In my expert opinion, APK Mirror is a reliable source for such archived APK files that I use in the regular course of my work.

17. After installing the APK files on a test Android device, I was able to run the applications and determined that the first screen shown to a user in both versions is the same, and

[1] https://www.apkmirror.com

requires the user to consent to WhatsApp's Terms of Service before the user can progress further in the application. Figures 1 and 2 below are screenshots of the initial screen on version 2.18.380-45261 and version 2.19.98-452742, respectively. The screen contains the language "Read our Privacy Policy. Tap 'Agree and Continue' to accept the Terms of Service," immediately above a large green button that reads "Agree and Continue." The terms "Privacy Policy" and "Terms of Service" are blue hyperlinks, and the hyperlink for "Terms of Service" directs users to https://www.whatsapp.com/legal/#terms-of-service. That URL directs to a webpage currently containing WhatsApp's Terms of Service. Archived versions of that webpage from the dates that the APK files were uploaded to APK Mirror also contain the Terms of Service, with a notation that they were last modified on August 25, 2016.[2] The user must click on the "Agree & Continue" button in order to progress further in the application, including to create an account and send messages.

[2] https://web.archive.org/web/20181213053133/https://www.whatsapp.com/legal/#terms-of-service (archive on Dec. 13, 2018); https://web.archive.org/web/20190410071846/https://www.whatsapp.com/legal/#terms-of-service (archived on Apr. 10, 2019).

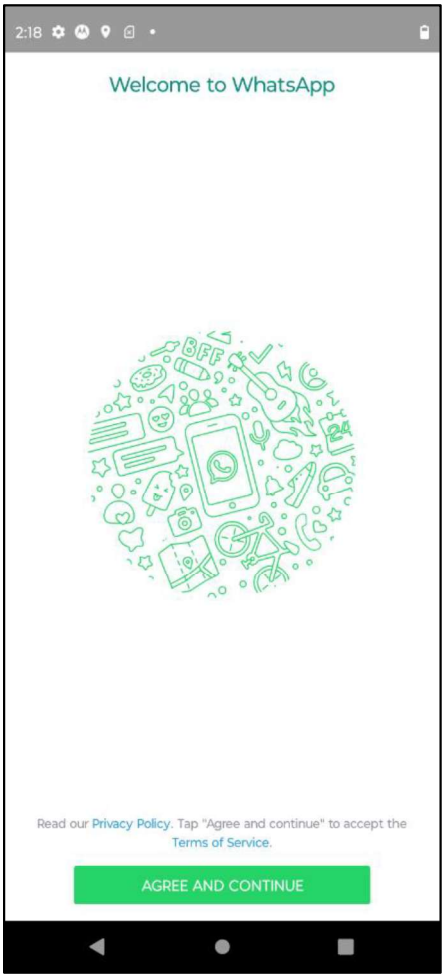

Figure 1: Initial Screen on WhatsApp version "2.18.380--45261"

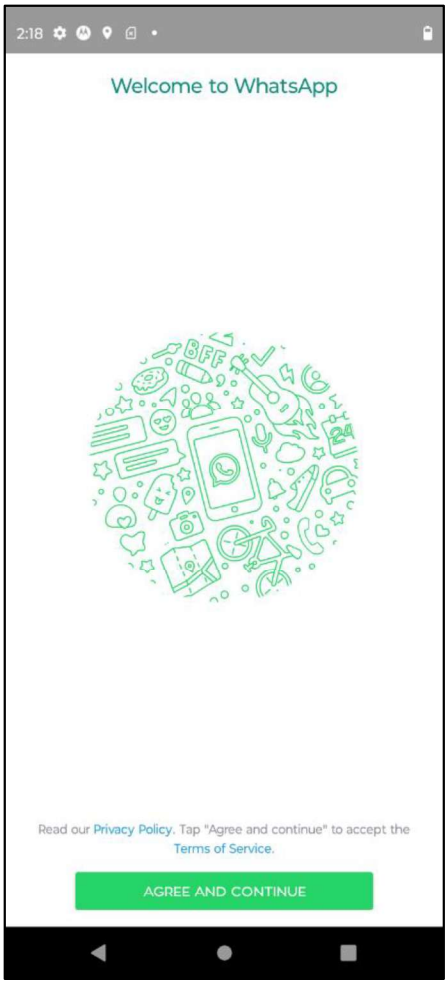

Figure 2: Initial Screen on WhatsApp version "2.19.98-45274".

I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 18, 2024 in New York, NY.

/s/ DocuSigned by: David Youssef 75FB98DF156B485...

David J. Youssef