COOLEY LLP
TRAVIS LEBLANC (251097) (tleblanc@cooley.com)
JOSEPH D. MORNIN (307766) (jmornin@cooley.com)
101 California Street, 5th floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

DANIEL J. GROOMS (D.C. Bar No. 219124) (*pro hac vice* forthcoming)
(dgrooms@cooley.com)
1299 Pennsylvania Avenue, NW, Suite 700
Washington, DC 20004-2400
Telephone: (202) 842-7800
Facsimile: (202) 842-7899

Attorneys for Plaintiffs
WHATSAPP INC. and FACEBOOK, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC., a Delaware corporation, and FACEBOOK, INC., a Delaware corporation,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No.

COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs WhatsApp Inc. and Facebook, Inc. (collectively, "Plaintiffs") allege the following against Defendants NSO Group Technologies Ltd. ("NSO Group") and Q Cyber Technologies Ltd. ("Q Cyber") (collectively, "Defendants"):

INTRODUCTION

1. Between in and around April 2019 and May 2019, Defendants used WhatsApp servers, located in the United States and elsewhere, to send malware to approximately 1,400 mobile phones and devices ("Target Devices"). Defendants' malware was designed to infect the Target Devices for the purpose of conducting surveillance of specific WhatsApp users ("Target Users"). Unable to break WhatsApp's end-to-end encryption, Defendants developed their malware in order to access messages and other communications after they were decrypted on Target Devices. Defendants' actions were not authorized by Plaintiffs and were in violation of WhatsApp's Terms of Service. In May 2019, Plaintiffs detected and stopped Defendants' unauthorized access and abuse of the WhatsApp Service and computers.

2. Plaintiffs bring this action for injunctive relief and damages pursuant to the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502, and for breach of contract and trespass to chattels.

PARTIES

3. Plaintiff WhatsApp Inc. ("WhatsApp") is a Delaware corporation with its principal place of business in Menlo Park, California.

4. Plaintiff Facebook, Inc. ("Facebook") is a Delaware corporation with its principal place of business in Menlo Park, California. Facebook acts as WhatsApp's service provider for security-related issues.

5. Defendant NSO Group was incorporated in Israel on January 25, 2010, as a limited liability company. Ex. 1. NSO Group had a marketing and sales arm in the United States called WestBridge Technologies, Inc. Ex. 2 and 3. Between 2014 and February 2019, NSO Group obtained financing from a San Francisco–based private equity firm, which ultimately purchased a controlling stake in NSO Group. Ex. 4. In and around February 2019, NSO Group was reacquired by its founders

and management. *Id.* NSO Group's annual report filed on February 28, 2019, listed Defendant Q Cyber as the only active director of NSO Group and its majority shareholder. Ex. 5.

6. Defendant Q Cyber was incorporated in Israel on December 2, 2013, under the name L.E.G.D. Company Ltd. Ex. 6 and 7. On May 29, 2016, L.E.G.D. Company Ltd. changed its name to Q Cyber. Ex. 7. Until at least June 2019, NSO Group's website stated that NSO Group was "a Q Cyber Technologies company." Ex. 8. Q Cyber's annual report filed on June 17, 2019, listed OSY Technologies S.A.R.L. as the only Q Cyber shareholder and active Director. Ex. 9

7. At all times material to this action, each Defendant was the agent, partner, alter ego, subsidiary, and/or coconspirator of and with the other Defendant, and the acts of each Defendant were in the scope of that relationship. In doing the acts and failing to act as alleged in this Complaint, each Defendant acted with the knowledge, permission, and consent of each other; and, each Defendant aided and abetted each other.

JURISDICTION AND VENUE

8. The Court has federal question jurisdiction over the federal causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1331.

9. The Court has supplemental jurisdiction over the state law causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1367 because these claims arise out of the same nucleus of operative fact as Plaintiffs' federal claims.

10. In addition, the Court has jurisdiction over all the causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1332 because complete diversity between the Plaintiffs and each of the named Defendants exists, and because the amount in controversy exceeds $75,000.

11. The Court has personal jurisdiction over Defendants because they obtained financing from California and directed and targeted their actions at California and its residents, WhatsApp and Facebook. The claims in this Complaint arise from Defendants' actions, including their unlawful access and use of WhatsApp computers, several of which are located in California.

12. The Court also has personal jurisdiction over Defendants because Defendants agreed to WhatsApp's Terms of Service ("WhatsApp Terms") by accessing and using WhatsApp. In relevant part, the WhatsApp Terms required Defendants to submit to the personal jurisdiction of this Court.

13. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b), as the threatened and actual harm to WhatsApp and Facebook occurred in this District.

14. Pursuant to Civil L.R. 3-2(d), this case may be assigned to either the San Francisco or Oakland division because WhatsApp and Facebook are located in San Mateo County.

FACTUAL ALLEGATIONS

A. Background on Facebook

15. Facebook is a social networking website and mobile application that enables its users to create their own personal profiles and connect with each other on their personal computers and mobile devices. As of June 2019, Facebook daily active users averaged 1.59 billion and monthly active users averaged 2.41 billion.

16. In October 2014, Facebook acquired WhatsApp. At all times relevant to this action, Facebook has served as WhatsApp's service provider, which entails providing both infrastructure and security for WhatsApp.

B. Background on WhatsApp

1. The WhatsApp Service

17. WhatsApp provides an encrypted communication service available on mobile devices and desktop computers (the "WhatsApp Service"). Approximately 1.5 billion people in 180 countries use the WhatsApp Service. Users must install the WhatsApp app to use the WhatsApp Service.

18. Every type of communication (calls, video calls, chats, group chats, images, videos, voice messages, and file transfers) on the WhatsApp Service is encrypted during its transmission between users. This encryption protocol was designed to ensure that no one other than the intended recipient could read any communication sent using the WhatsApp Service.

2. WhatsApp's Terms of Service

19. Every WhatsApp user must create an account and agree and consent to WhatsApp's Terms (available at https://www.whatsapp.com/legal?eea=0#terms-of-service).

20. The WhatsApp Terms stated that "You must use our Services according to our Terms and policies" and that users agreed to "access and use [WhatsApp's] Services only for legal, authorized, and acceptable purposes."

21. The WhatsApp Terms prohibited using the WhatsApp services in ways that (a) "violate, misappropriate, or infringe the rights of WhatsApp, our users, or others, including privacy;" (b) "are illegal, intimidating, harassing, . . . or instigate or encourage conduct that would be illegal, or otherwise inappropriate;" [or] . . . (e) "involve sending illegal or impermissible communications."

22. The WhatsApp Terms prohibited users from "exploiting [WhatsApp's] Services in impermissible or unauthorized manners, or in ways that burden, impair, or harm us, our Services, systems, our users, or others." The Terms also required users to agree not to: "(a) reverse engineer, alter, modify, create derivative works from, decompile, or extract code from our Services; (b) send, store, or transmit viruses or other harmful computer code through or onto our Services; (c) gain or attempt to gain unauthorized access to our Services or systems; (d) interfere with or disrupt the safety, security, or performance of our Services; [or] . . . (f) collect the information of or about our users in any impermissible or unauthorized manner."

23. The WhatsApp Terms prohibited users not just from personally engaging in the conduct listed above, but also from assisting others in doing so.

C. Background on NSO Group and Pegasus

24. Defendants manufactured, distributed, and operated surveillance technology or "spyware" designed to intercept and extract information and communications from mobile phones and devices. Defendants' products included "Pegasus," a type of spyware known as a remote access trojan. Ex. 10 and 11. According to Defendants, Pegasus and its variants (collectively, "Pegasus") were designed to be remotely installed and enable the remote access and control of information—including calls, messages, and location—on mobile devices using the Android, iOS, and BlackBerry operating systems. *Id.*

25. On information and belief, in order to enable Pegasus' remote installation, Defendants exploited vulnerabilities in operating systems and applications (e.g., CVE-2016-4657) and used other malware delivery methods, like spearphishing messages containing links to malicious code. *Id.*

26. According to media reports and NSO documents, Defendants claimed that Pegasus could be surreptitiously installed on a victim's phone without the victim taking any action, such as

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.