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

clicking a link or opening a message (known as remote installation).[1] *Id.* Defendants promoted that Pegasus's remote installation feature facilitated infecting victims' phones without using spearphishing messages that could be detected and reported by the victims.

27. According to NSO Group, Pegasus could "remotely and covertly extract valuable intelligence from virtually any mobile device." *Id.* Pegasus was designed, in part, to intercept communications sent to and from a device, including communications over iMessage, Skype, Telegram, WeChat, Facebook Messenger, WhatsApp, and others. *Id.* On information and belief, Pegasus was modular malware, which meant that it could be customized for different purposes, including to intercept communications, capture screenshots, and exfiltrate browser history and contacts from the device. *Id.*

28. Defendants used a network of computers to monitor and update the version of Pegasus implanted on the victims' phones. *Id.* These Defendant-controlled computers relayed malware, commands, and data between a compromised phone, Defendants, and Defendants' customers. This network served as the nerve center through which Defendants supported and controlled their customers' operation and use of Pegasus. In some instances, Defendants limited the number of concurrent devices that their customers could compromise with Pegasus to 25. Ex. 11.

29. Defendants profited by licensing Pegasus and selling support services to their customers, which included Pegasus installation, monitoring, and training. Ex. 10 and 11. Defendants also offered technical support to customers using Pegasus to infect victims' phones, including: (a) technical support by email and phone; and (b) remote troubleshooting by Defendants' engineers through remote desktop software and a virtual private network. *Id.*

[1] *See* Financial Times, "Israel's NSO: the business of spying on your iPhone" (May 14, 2019), *available at* https://www.ft.com/content/7f2f39b2-733e-11e9-bf5c-6eeb837566c5; Vice, "They Got Everything" (September 20, 2018), *available at* https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo.

D. Defendants Agreed to the WhatsApp Terms

30. Between January 2018 and May 2019, Defendants created and caused to be created various WhatsApp accounts and agreed to the WhatsApp Terms. Defendants' employees and agents accepted and agreed to be bound by the Terms on behalf of Defendants.

31. At all times relevant to this Complaint, Defendants were bound by the WhatsApp Terms.

E. Defendants Accessed and Used Plaintiffs' Servers Without Authorization and Infected Target Users' Devices With Malware

1. Overview

32. Defendants took a number of steps, using WhatsApp servers and the WhatsApp Service without authorization, to send discrete malware components ("malicious code") to Target Devices. *First*, Defendants set up various computer infrastructure, including WhatsApp accounts and remote servers, used to infect the Target Devices and conceal Defendants' identity and involvement. *Second*, Defendants used and caused to be used WhatsApp accounts to initiate calls through Plaintiffs' servers that were designed to secretly inject malicious code onto Target Devices. *Third*, Defendants caused the malicious code to execute on some of the Target Devices, creating a connection between those Target Devices and computers controlled by Defendants (the "remote servers"). *Fourth*, on information and belief, Defendants caused Target Devices to download and install additional malware—believed to be Pegasus or another remote access trojan developed by Defendants—from the remote servers for the purpose of accessing data and communications on Target Devices.

2. Defendants Set Up Computer Infrastructure Used to Infect the Target Devices

33. Between approximately January 2018 and May 2019, Defendants created WhatsApp accounts that they used and caused to be used to send malicious code to Target Devices in April and May 2019. The accounts were created using telephone numbers registered in different counties, including Cyprus, Israel, Brazil, Indonesia, Sweden, and the Netherlands.

34. Beginning no later than 2019, Defendants leased and caused to be leased servers and internet hosting services in different countries, including the United States, in order to connect the

Target Devices to a network of remote servers intended to distribute malware and relay commands to the Target Devices. This network included proxy servers and relay servers (collectively, "malicious servers"). The malicious servers were owned by Choopa, Quadranet, and Amazon Web Services ("AWS"), among others. The IP address of one of the malicious servers was previously associated with subdomains used by Defendants.

3. Defendants' Unauthorized Access of Plaintiff's Servers

35. On information and belief, Defendants reverse-engineered the WhatsApp app and developed a program to enable them to emulate legitimate WhatsApp network traffic in order to transmit malicious code—undetected—to Target Devices over WhatsApp servers. Defendants' program was sophisticated, and built to exploit specific components of WhatsApp network protocols and code. Network protocols generally define rules that control communications between network computers, including protocols for computers to identify and connect with other computers, as well as formatting rules that specify how data is packaged and transmitted.

36. In order to compromise the Target Devices, Defendants routed and caused to be routed malicious code through Plaintiffs' servers—including Signaling Servers and Relay Servers—concealed within part of the normal network protocol. WhatsApp's Signaling Servers facilitated the initiation of calls between different devices using the WhatsApp Service. WhatsApp's Relay Servers facilitated certain data transmissions over the WhatsApp Service. Defendants were not authorized to use Plaintiffs' servers in this manner.

37. Between approximately April and May 2019, Defendants used and caused to be used, without authorization, WhatsApp Signaling Servers, in an effort to compromise Target Devices. To avoid the technical restrictions built into WhatsApp Signaling Servers, Defendants formatted call initiation messages containing malicious code to appear like a legitimate call and concealed the code within call settings. Disguising the malicious code as call settings enabled Defendants to deliver it to the Target Device and made the malicious code appear as if it originated from WhatsApp Signaling Servers. Once Defendants' calls were delivered to the Target Device, they injected the malicious code into the memory of the Target Device—even when the Target User did not answer the call.

38. For example, on May 9, 2019, Defendants used WhatsApp servers to route malicious code, which masqueraded as a series of legitimate calls and call settings, to a Target Device using telephone number (202) XXX-XXXX. On information and belief, the malicious code concealed within the calls was then installed in the memory of the Target Device.

39. Between April and May 2019, Defendants also used and caused to be used WhatsApp's Relay Servers without authorization to send encrypted data packets designed to activate the malicious code injected into the memory of the Target Devices. When successfully executed, the malicious code caused the Target Device to send a request to one of the malicious servers controlled by Defendants.

40. On information and belief, the malicious servers connected the Target Devices to remote servers hosting Defendants' malware. The malicious code on the Target Devices then downloaded and installed Defendants' malware from those servers.

41. On information and belief, after it was installed, Defendants' malware was designed to give Defendants and their customers access to information and data stored on the Target Devices, including their communications.

42. Between approximately April 29, 2019, and May 10, 2019, Defendants caused their malicious code to be transmitted over WhatsApp servers in an effort to infect approximately 1,400 Target Devices. The Target Users included attorneys, journalists, human rights activists, political dissidents, diplomats, and other senior foreign government officials.

43. The Target Users had WhatsApp numbers with country codes from several countries, including the Kingdom of Bahrain, the United Arab Emirates, and Mexico. According to public reporting, Defendants' clients include, but are not limited to, government agencies in the Kingdom of Bahrain, the United Arab Emirates, and Mexico as well as private entities.[2]

[2] *See* Fast Company, "Israeli cyberweapon targeted the widow of a slain Mexican journalist" (March 20, 2019), *available at* https://www.fastcompany.com/90322618/nso-group-pegasus-cyberweapon-targeted-the-widow-of-a-slain-mexican-journalist; New York Times, "Hacking a Prince, and Emir and a Journalist to Impress a Client" (August 31, 2018), *available at* https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html; The Guardian, "Israeli firm linked to WhatsApp spyware attack faces lawsuit" (May 18, 2019), *available at* https://www.theguardian.com/world/2019/may/18/israeli-firm-nso-group-linked-to-whatsapp-spyware-attack-faces-lawsuit.

44. On or about May 13, 2019, Facebook publicly announced that it had investigated and identified a vulnerability involving the WhatsApp Service (CVE-2019-3568). WhatsApp and Facebook closed the vulnerability, contacted law enforcement, and advised users to update the WhatsApp app.

45. Defendants subsequently complained that WhatsApp had closed the vulnerability. Specifically, NSO Employee 1 stated, "You just closed our biggest remote for cellular . . . It's on the news all over the world."

F. Defendants' Unlawful Acts Have Caused Damage and Loss to WhatsApp and Facebook

46. Defendants' actions and omissions interfered with the WhatsApp Service and burdened Plaintiffs' computer network.

47. Defendants' actions injured Plaintiffs' reputation, public trust, and goodwill.

48. Defendants have caused Plaintiffs damages in excess of $75,000 and in an amount to be proven at trial.

FIRST CAUSE OF ACTION

(Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

49. Plaintiffs reallege and incorporate by reference all preceding paragraphs.

50. At various times between April 29, 2019, and May 10, 2019, Defendants accessed, used, or caused to be accessed or used Plaintiffs' Signaling Servers and Relay Servers without authorization in an effort to compromise approximately 1,400 Target Devices.

51. Plaintiffs' Signaling Servers and Relay Servers and the Target Devices were "computers" as defined by 18 U.S.C. § 1030(e)(1).

52. Plaintiffs' Signaling Servers and Relay Servers and the Target Devices were "protected computers" as defined by 18 U.S.C. § 1030(e)(2)(B) because they are "used in or affecting interstate or foreign commerce or communication."

53. Defendants violated 18 U.S.C. § 1030(a)(2) because they intentionally accessed and caused to be accessed (a) Plaintiffs' computers, and (b) Target Devices, without authorization and, on information and belief, obtained data from the Target Devices.

54. Defendants violated 18 U.S.C. § 1030(a)(4) because they knowingly and with intent to defraud accessed and caused to be accessed (a) Plaintiffs' protected computers and (b) Target Devices without authorization, and by means of such conduct furthered the intended fraud and obtained something of value. Defendants' fraud included falsely agreeing to the WhatsApp Terms, sending unauthorized commands to Plaintiffs' computers and concealing the commands as legitimate network traffic, in order to gain access of the Target Devices without the Target Users' knowledge or consent. As a result of the fraud, Defendants obtained money, customers, remote access and control of the Target Devices, data from the Target Devices, and unauthorized use of the WhatsApp service, the value of which exceeds $5,000.

55. Defendants violated 18 U.S.C. § 1030(b) by conspiring and attempting to commit the violations alleged in the preceding paragraphs.

56. Defendants' conduct caused a loss to Plaintiffs and the Target Users in excess of $5,000 during a one-year period.

57. Defendants' actions caused Plaintiffs to incur a loss as defined in 18 U.S.C. § 1030(e)(11), including the expenditure of resources to investigate and remediate Defendants' fraud and unauthorized access. Plaintiffs are entitled to be compensated for losses and damages, and any other amount to be proven at trial.

SECOND CAUSE OF ACTION

(California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502)

58. Plaintiffs reallege and incorporate by reference all of the preceding paragraphs.

59. Defendants knowingly accessed and without permission altered and used Plaintiffs' data, computer, computer system, and computer network in order to (a) devise and execute a scheme and artifice to defraud and deceive, and (b) wrongfully control and obtain money, property, and data in violation of California Penal Code § 502(c)(1).

60. Defendants knowingly and without permission used and caused to be used WhatsApp Signaling Servers and Relay Servers, including servers located in California, in violation of California Penal Code § 502(c)(3).

61. Defendants knowingly and without permission provided and assisted in providing a means of accessing Plaintiffs' computers, computer systems, and computer networks, including those located in California, in violation of California Penal Code § 502(c)(6).

62. Defendants knowingly and without permission accessed and caused to be accessed Plaintiffs' computers, computer systems, and computer networks, including those located in California, in violation of California Penal Code § 502(c)(7).

63. Defendants knowingly introduced a computer contaminant into Plaintiffs' computers, computer systems, and computer networks in violation of California Penal Code § 502(c)(8).

64. Defendants' actions caused Plaintiffs to incur losses and damages, including, among other things, the expenditure of resources to investigate and remediate Defendants' conduct, damage to Plaintiffs' reputation, and damage to the relationships and goodwill between Plaintiffs and their users and potential users. Plaintiffs have been damaged in an amount to be proven at trial.

65. Because Plaintiffs suffered damages and a loss as a result of Defendants' actions and continue to suffer damages as result of Defendants' actions, Plaintiffs are entitled to compensatory damages, attorneys' fees, and any other amount of damages to be proven at trial, as well as injunctive relief under California Penal Code §§ 502(e)(1) and (2).

66. Because Defendants willfully violated California Penal Code § 502, and there is clear and convincing evidence that Defendants acted with malice and oppression and committed "fraud" as defined by section 3294 of the Civil Code, Plaintiffs are entitled to punitive and exemplary damages under California Penal Code § 502(e)(4).

THIRD CAUSE OF ACTION

(Breach of Contract)

67. Plaintiffs reallege and incorporate by reference all preceding paragraphs.

68. Access to and use of WhatsApp is governed by the WhatsApp's Terms and related WhatsApp policies.

69. Defendants agreed to and became bound by the WhatsApp's Terms when they used WhatsApp and the WhatsApp Service.

70. WhatsApp and Facebook have performed all conditions, covenants, and promises required of it in accordance with the WhatsApp's Terms.

71. Defendants' violations of the WhatsApp's Terms have directly and proximately caused and continue to cause harm and injury to WhatsApp.

72. When Defendants agreed to and became bound by the WhatsApp Terms, both Plaintiffs and Defendants knew or could have reasonably foreseen that the harm and injury to Plaintiffs was likely to occur in the ordinary course of events as a result of Defendants' breach.

73. Defendants' actions caused Plaintiffs to incur losses and other economic damages, including, among other things, the expenditure of resources to investigate and remediate Defendants' conduct, damage to Plaintiffs' reputation, and damage to the relationships and goodwill between Plaintiffs and their users and potential users. Plaintiffs have been damaged in an amount to be proven at trial, and in excess of $75,000.

FOURTH CAUSE OF ACTION

(Trespass to Chattels)

74. Plaintiffs reallege and incorporate by reference all of the preceding paragraphs.

75. At all times mentioned in this Complaint, Plaintiffs had legal title to and actual possession of their computer systems.

76. Defendants intentionally and without authorization interfered with Plaintiffs' possessory interest in their computer systems, including by accessing and using Plaintiffs' servers to transmit malicious code for the purpose of unlawfully compromising Target Users' devices, all without authorization from Plaintiffs and Target Users.

77. Defendants' access to Plaintiffs' computer systems exceeded the scope of the conditional access that Plaintiffs grant to legitimate users of the WhatsApp Service.

78. Defendants' actions caused Plaintiffs to incur losses and other economic damages, including, among other things, the expenditure of resources to investigate and remediate Defendants' conduct, damage to Plaintiffs' reputation, and damage to the relationships and goodwill between Plaintiffs and their users and potential users. Plaintiffs have been damaged in an amount to be proven at trial, and in excess of $75,000.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs request judgment against Defendants as follows:

1. That the Court enter judgment against Defendants that Defendants have:

   a. Violated the Computer Fraud and Abuse Act, in violation of 18 U.S.C. § 1030;

   b. Violated the California Comprehensive Computer Data Access and Fraud Act, in violation California Penal Code § 502;

   c. Breached their contracts with WhatsApp in violation of California law;

   d. Wrongfully trespassed on Plaintiffs' property in violation of California law.

2. That the Court enter a permanent injunction enjoining and restraining Defendants and their agents, servants, employees, successors, and assigns, and all other persons acting in concert with or conspiracy with any of them or who are affiliated with Defendants from:

   a. Accessing or attempting to access WhatsApp's and Facebook's service, platform, and computer systems;

   b. Creating or maintaining any WhatsApp or Facebook account;

   c. Engaging in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Plaintiffs' service, platform, and computer systems; and

   d. Engaging in any activity, or facilitating others to do the same, that violates WhatsApp's or Facebook's Terms;

3. That WhatsApp and Facebook be awarded damages, including, but not limited to, compensatory, statutory, and punitive damages, as permitted by law and in such amounts to be proven at trial.

4. That WhatsApp and Facebook be awarded their reasonable costs, including reasonable attorneys' fees.

5. That WhatsApp and Facebook be awarded pre- and post-judgment interest as allowed by law.

6. That the Court grant all such other and further relief as the Court may deem just and proper.

PLAINTIFFS RESPECTFULLY DEMAND A JURY TRIAL.

Dated: October 29, 2019

Respectively submitted,

COOLEY LLP

/s/ Travis LeBlanc
Travis LeBlanc
Daniel J. Grooms
Joseph D. Mornin

Attorneys for Plaintiffs
WHATSAPP INC. and FACEBOOK, INC.

Platform Enforcement and Litigation
Facebook, Inc.
Jessica Romero
Tyler Smith
Michael Chmelar
Bridget Freeman

COOLEY LLP
TRAVIS LEBLANC (251097) (tleblanc@cooley.com)
KYLE C. WONG (224021) (kwong@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) (admitted *pro hac vice*)
(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. 3:19-cv-07123-JSC

PLAINTIFFS' SEPARATE CASE MANAGEMENT STATEMENT AND [PROPOSED] ORDER

Date: February 13, 2020
Time: 1:30 p.m.
Courtroom: E, 15th Floor
Judge: Hon. Jacqueline S. Corley

Plaintiffs WhatsApp Inc. and Facebook, Inc. submit this Separate Case Management Statement and Proposed Order under the Standing Order for All Judges of the Northern District of California and Civil Local Rule 16-9.

I. JURISDICTION AND SERVICE

The basis for the court's subject matter jurisdiction over plaintiff's claims and defendant's counterclaims, whether any issues exist regarding personal jurisdiction or venue, whether any parties remain to be served, and, if any parties remain to be served, a proposed deadline for service.

A. Subject-Matter Jurisdiction

The Court has federal question jurisdiction under 28 U.S.C. § 1331 because this action alleges violations of federal law, namely, the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq*. The Court has supplemental jurisdiction over Plaintiffs' state-law causes of action under 28 U.S.C. § 1367 because they arise from the same nucleus of operative fact as Plaintiffs' CFAA claim.

In addition, the Court has diversity jurisdiction under 28 U.S.C. § 1332 because complete diversity exists between the Plaintiffs and each of the named Defendants and because the amount in controversy exceeds $75,000.

B. Personal Jurisdiction and Venue

The Court has personal jurisdiction over Defendants because they obtained financing from a California-based entity; they directed their actions at California and Plaintiffs, who are headquartered in California; they unlawfully accessed and used WhatsApp's computers, several of which are located in California; and they agreed to WhatsApp's Terms of Service, which required Defendants to submit to the personal jurisdiction of this Court.

Venue is proper in this Judicial District under 28 U.S.C. § 1391(b) because the harm to Plaintiffs occurred in this District.

As explained below, Defendants have not appeared in this litigation, they have not responded to the Complaint, and they have not responded to Plaintiffs' communications concerning this matter. Declaration of Joseph D. Mornin ("Mornin Decl.") ¶ 14. As such, there are currently no issues related to personal jurisdiction or venue.

C. Service

Defendant Q Cyber is the parent company of Defendant NSO Group. Compl. ¶¶ 5–6. Both Defendants' offices are located at 22 Galgalei Haplada, Hertsliya, Israel 4672222. *Id.* Ex. 5. As described below, Plaintiffs have made substantial efforts to notify and serve Defendants by email, physical mail, personal service, and service via the Hague Convention.

1. Defendants were notified via email, physical mail, and personal service.

After filing the Complaint on October 29, 2019, Plaintiffs notified NSO Group and Q Cyber

of this litigation and requested waiver of service by delivering the following materials (the "Service Materials") to each Defendant and their board members:

- A cover letter that requested contact information for Defendants' counsel; requested waiver of service of the summons within 60 days; and informed Defendants of their duty to preserve all documents that may be relevant to this litigation. Mornin Decl. ¶ 2 & Ex. 1.
- The Complaint, Complaint exhibits, and civil cover sheet filed in this case (ECF Nos. 1, 1-1, & 1-2). *Id.* ¶ 2.
- U.S. District Court Forms AO 398 ("Notice of a Lawsuit and Request to Waive Service of a Summons") and AO 399 ("Waiver of the Service of Summons"). *Id.* ¶ 2 & Ex. 2.
- The standing order for all judges of the Northern District of California; the civil standing order for Magistrate Judge Jacqueline Scott Corley; the Northern District of California's general standing order for civil cases entitled "Contents of Joint Case Management Statement"; and the Court's order setting ADR deadlines and the initial case management conference (ECF No. 9). *Id.* ¶ 2.

Plaintiffs delivered the Service Materials to Defendants by the following methods:

- By email:
  - On November 4, 2019, Plaintiffs delivered the Service Materials to Shalev Hulio, NSO Group's CEO and board member, by email. *Id.* ¶ 4 & Ex. 3.[1]
  - On November 4, 2019, Plaintiffs delivered the Service Materials to Eran Gorev, who is identified as Q Cyber's CEO in the company's Israeli corporate filings, by email. On November 12, Plaintiffs received an email response from Gorev, in which Gorev stated that he no longer serves in that role. *Id.* ¶ 5 & Ex. 4.
  - On November 8, 2019, Plaintiffs delivered the Service Materials to each NSO Group board member, as identified on NSO Group's website, by email. *Id.* ¶ 7 & Ex. 6.

[1] All email addresses and physical addresses Plaintiffs contacted are identified in the attached Mornin Declaration and exhibits.

- On November 22, 2019, Plaintiffs attempted to deliver the Service Materials to Nachum Falek, CFO of both Q Cyber and NSO Group, by email. *Id.* ¶ 12 & Ex. 11.

- By physical mail:
  - On November 4, 2019, Plaintiffs sent the Service Materials by DHL Express to Defendants' shared office in Israel. The Service Materials were delivered to the shared office and signed for at reception on November 10. *Id.* ¶ 6 & Ex. 5.
  - On November 9, 2019, Plaintiffs sent the Service Materials by FedEx to the office of each NSO Group board member. The Service Materials were delivered and signed for between November 11 and 13. *Id.* ¶ 8 & Ex. 7.
  - On November 21, 2019, Plaintiffs sent the Service Materials addressed to Nachum Falek, Q Cyber's and NSO Group's CFO, by DHL Express to Defendants' shared office in Israel. The Service Materials were delivered to the shared office and signed for at reception on November 24. *Id.* ¶ 11 & Ex. 10.
- In person:
  - On November 13, 2019, Plaintiffs hand-delivered the Service Materials to both Defendants at their shared office in Israel. Shir Kovner, who serves as the "legal advisor" for both Defendants, personally signed the receipt for the hand-delivered Service Materials. *Id.* ¶ 9 & Ex. 8.
  - On November 15, 2019, Plaintiffs hand-delivered the Service Materials to Omri Lavie, NSO Group's co-founder and a current board member, by delivering the Service Materials to his wife at their residence in New Jersey. *Id.* ¶ 10 & Ex. 9.
  - On November 24, 25, and 27, 2019, Plaintiffs attempted to hand-deliver the Service Materials to Nachum Falek, Q Cyber and NSO Group's CFO, at Defendants' shared office and Falek's home in Israel. When those attempts did not succeed, Plaintiffs sent materials by registered mail in Israel to Defendants' office and left an envelope containing the Service Materials in Falek's mailbox at his residence. *Id.* ¶ 13 & Ex. 12.

The deadline for Defendants to respond to Plaintiffs' requests for waiver of service was January 3, 2020.[2] Defendants have not provided a response as of this filing.

2. Defendants were properly served via the Hague Convention.

In addition to these efforts, Plaintiffs have also successfully served Defendants via the Hague Service Convention. Plaintiffs engaged a vendor to accomplish international process service on November 8, 2019. *Id.* ¶ 16. On December 31, 2019, the vendor reported that Defendants had been served by hand-delivery at their shared office on December 17, 2019. *Id.* ¶ 17 & Exs. 13, 14. Plaintiffs are currently awaiting the issuance of the formal certificate of Hague service by the Central Authority in Israel. *Id.* ¶ 18.

3. Defendants have publicly acknowledged this litigation.

It is undeniable that Defendants have actual notice of this litigation. On October 29, 2019—the same day Plaintiffs filed the Complaint in this case—NSO Group issued a press release discussing the litigation, in which it stated: "In the strongest possible terms, we dispute today's allegations and will vigorously fight them." *Id.* ¶ 19 & Ex. 15. Plaintiffs have also successfully contacted both NSO Group and Q Cyber through multiple channels, as described above. *See, e.g.*, *id.* ¶ 9 & Ex. 8 (showing that the legal advisor for NSO Group—who also serves as the legal advisor for Q Cyber—personally signed for a delivery of the Service Materials listed above), ¶ 8 & Ex. 7 (showing that the Service Materials were delivered and signed for at NSO Group's and Q Cyber's offices).

Moreover, recent public filings under the Foreign Agents Registration Act indicate that Q Cyber executed an agreement with a U.S. public strategy firm, Mercury Public Affairs, on December 19, 2019 (approximately seven weeks after Plaintiffs filed this lawsuit and exactly two days after Hague service was effected), for consulting services related to this litigation:

[2] Rule 4(d)(1)(F) provides that a request for waiver of service must "give the defendant a reasonable time of at least 30 days after the request was sent—or at least 60 days if sent to the defendant outside any judicial district of the United States—to return the waiver." Here, Plaintiffs sent their initial request for waiver of service to both Defendants by physical mail on November 4, 2019, with instructions to return the waiver within 60 days. Mornin Decl. ¶ 2 & Exs. 1, 2. Plaintiffs delivered the same materials by email to both Defendants on the same day. *Id.* ¶ 4. 60 days after November 4, 2019, is January 3, 2020.

> Consultant [Mercury Public Affairs] will provide strategic consulting and management services ("Services") specific to government relations and crisis management issues that the Client [Q Cyber] faces in connection with, and which may impact, ***pending litigation filed against the Client in the U.S. District Court for the Northern District of California*** and/or other US and non-US courts, and in connection with potential future litigation or regulatory actions involving similar issues.

Id. ¶ 20 & Ex. 16 at 10 (emphasis added).[3] The agreement was signed by Q Cyber's General Legal Counsel, Shmuel Sunray, and envisions payments of $120,000 per month until November 30, 2020. *Id.* Ex. 16 at 4, 11.

4. Defendants have not timely responded to the Complaint.

The deadline for Defendants to respond to the complaint was January 7, 2020. *See* Fed. R. Civ. P. 12(a)(1)(A)(i) ("Unless another time is specified by this rule or a federal statute, the time for serving a responsive pleading is as follows: . . . A defendant must serve an answer . . . within 21 days after being served with the summons and complaint."). Despite Plaintiffs' multiple communications to Defendants' corporate headquarters and to their directors, officers, and board members, Defendants have not responded to the Complaint as of this filing and have refused to appear in this litigation.

On February 3, 2020, Plaintiffs' counsel was contacted for the first time by Joseph Akrotirianakis, an attorney at King & Spalding LLP, who stated that he represents NSO Group and Q Cyber. Mornin Decl. ¶ 15. Counsel for all parties spoke by phone on February 4. *Id.* During that phone conversation, Mr. Akrotirianakis stated that he was not currently willing to enter an appearance as an attorney of record in this case. *Id.* Plaintiffs' counsel stated that Plaintiffs were concerned about discussing the litigation with counsel who are not attorneys of record. *Id.* Plaintiffs later confirmed by email that they would only discuss the litigation with an attorney of record. *Id.* As of this filing, Plaintiffs have not received a reply. *Id.*

II. FACTS

A brief chronology of the facts and a statement of the principal factual issues in dispute.

[3] No other litigation has been filed in the Northern District against Q Cyber or NSO Group. Thus, it is indisputable that this agreement contemplates consulting services related to this case.

Defendants manufactured, distributed, and operated surveillance technology, also known as "spyware," designed to intercept and extract information and communications from mobile phones and devices. Defendants' products included "Pegasus," a type of spyware that could be surreptitiously installed on a victim's phone without the victim taking any action, such as clicking a link or opening a message. Once installed, Pegasus could access a broad array of private information, including the phone's location, camera, microphone, memory, and hard drive, as well as private emails, calls, texts, and messages sent via iMessage, Skype, Telegram, WeChat, Facebook Messenger, WhatsApp, and other platforms. Defendants' clients included government agencies in the Kingdom of Bahrain, the United Arab Emirates, and Mexico, as well as private entities.

Between in and around April 2019 and May 2019, Defendants used WhatsApp servers, located in the United States and elsewhere, to send their spyware to approximately 1,400 mobile phones and devices belonging to attorneys, journalists, human rights activists, government officials, and others. Unable to break WhatsApp's end-to-end encryption, Defendants developed their malware to access messages and other communications after they were decrypted on a device. Defendants' actions were not authorized by Plaintiffs. In May 2019, Plaintiffs detected and stopped Defendants' unauthorized access and abuse of the WhatsApp service and computers. On October 29, 2019, Plaintiffs filed this lawsuit seeking injunctive relief and damages based on federal and state claims.

Since the filing of the Complaint, there have been several reports of NSO Group's continued manufacturing, distribution, and operation of surveillance technology. The *New York Times* reported that Saudi Arabia attempted to install NSO Group's malware on a *Times* reporter's phone, and Reuters reported that the FBI is investigating NSO Group's role in possible hacks of American residents and companies. *Id.* ¶¶ 21–22 & Exs. 17, 18.

III. LEGAL ISSUES

A brief statement, without extended legal argument, of the disputed points of law, including reference to specific statutes and decisions.

Given Defendants' failure to timely respond to the Complaint, there are no disputed legal issues at this time.

IV. MOTIONS

All prior and pending motions, their current status, and any anticipated motions.

Plaintiffs previously filed an administrative motion to reschedule the case management conference, which the Court granted. ECF Nos. 16 (motion), 17 (order). There are no pending motions. Plaintiffs anticipate filing motions necessary to obtain a default judgment.

V. AMENDMENT OF PLEADINGS

The extent to which parties, claims, or defenses are expected to be added or dismissed and a proposed deadline for amending the pleadings.

At this time, Plaintiffs do not expect to add any parties, claims, or defenses. In accordance with Fed. R. Civ. P. 15(a), and given that Defendants have not served a responsive pleading, Plaintiffs propose that no deadline for amending the pleadings be set at this time.

VI. EVIDENCE PRESERVATION

A brief report certifying that the parties have reviewed the Guidelines Relating to the Discovery of Electronically Stored Information ("ESI Guidelines"), and confirming that the parties have met and conferred pursuant to Fed. R. Civ. P. 26(f) regarding reasonable and proportionate steps taken to preserve evidence relevant to the issues reasonably evident in this action.

Plaintiffs have reviewed the ESI Guidelines and are taking reasonable and proportionate steps to preserve evidence relevant to the issues reasonably evident in this action.

Plaintiffs have been unable to meet and confer with Defendants regarding evidence preservation because Defendants have refused to appear and Defendants have not replied to any of Plaintiffs' communications. Mornin Decl. ¶ 14.

VII. DISCLOSURES

Whether there has been full and timely compliance with the initial disclosure requirements of Fed. R. Civ. P. 26, and a description of the disclosures made.

Because Defendants have not responded to the Complaint, Plaintiffs believe initial disclosures under Fed. R. Civ. P. 26 are premature but are ready to make such disclosures when Defendants appear in this litigation.

VIII. DISCOVERY

Discovery taken to date, if any, the scope of anticipated discovery, any proposed limitations or modifications of the discovery rules, a brief report on whether the parties have considered entering into a stipulated e-discovery order, a proposed discovery plan pursuant to Fed. R. Civ. P. 26(f), and any identified discovery disputes.

No discovery has been taken to date. In view of Defendants' failure to appear in this litigation or respond to the Complaint, Plaintiffs believe a proposed discovery plan is premature.

IX. CLASS ACTIONS

If a class action, a proposal for how and when the class will be certified, and whether all attorneys of record for the parties have reviewed the Procedural Guidance for Class Action Settlements.

Not applicable.

X. RELATED CASES

Any related cases or proceedings pending before another judge of this court, or before another court or administrative body.

On November 26, 2019 (approximately one month after Plaintiffs filed their Complaint in this case), eight current and former employees of NSO Group filed a lawsuit against Facebook in Israel. *Azarzar v. Facebook, Inc.*, Civil File 62584-11-19 (Tel Aviv—Jaffa District Court). The plaintiffs in that case allege that Facebook unlawfully terminated their Facebook and Instagram accounts.

XI. RELIEF

All relief sought through complaint or counterclaim, including the amount of any damages sought and a description of the bases on which damages are calculated. In addition, any party from whom damages are sought must describe the bases on which it contends damages should be calculated if liability is established.

Plaintiffs seek the following relief:

- Judgment against Defendants that Defendants have:
    - Violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

- Violated the California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502;
- Breached their contracts with WhatsApp in violation of California law; and
- Wrongfully trespassed on Plaintiffs' property in violation of California law.

- A permanent injunction enjoining and restraining Defendants and their agents, servants, employees, successors, and assigns, and all other persons acting in concert with or conspiracy with any of them or who are affiliated with Defendants from:
  - Developing or selling malware or computer code that targets Facebook, Facebook Products, or Facebook Company Products;
  - Accessing or attempting to access WhatsApp's and Facebook's service, platform, and computer systems;
  - Creating or maintaining any WhatsApp or Facebook account;
  - Engaging in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Plaintiffs' service, platform, and computer systems; and
  - Engaging in any activity, or facilitating others to do the same, that violates WhatsApp's or Facebook's Terms.
- That WhatsApp and Facebook be awarded damages, including, but not limited to, compensatory, statutory, and punitive damages, as permitted by law and in such amounts to be proven at trial.
- That WhatsApp and Facebook be awarded their reasonable costs, including reasonable attorneys' fees.
- That WhatsApp and Facebook be awarded pre- and post-judgment interest as allowed by law.
- That the Court grant all such other and further relief as the Court may deem just and proper.

XII. SETTLEMENT AND ADR

Prospects for settlement, ADR efforts to date, and a specific ADR plan for the case, including

compliance with ADR L.R. 3-5 and a description of key discovery or motions necessary to position the parties to negotiate a resolution.

In view of Defendants' failure to appear in this litigation or respond to the Complaint, Plaintiffs do not believe that the prospects for settlement are favorable, and the parties have not conferred in an attempt to agree on an ADR process in accordance with ADR L.R. 3-5.

XIII. CONSENT TO MAGISTRATE JUDGE FOR ALL PURPOSES

*Whether **all** parties will consent to have a magistrate judge conduct all further proceedings including trial and entry of judgment. ___ Yes ___ No*

Plaintiffs consent to a magistrate judge for all purposes. *See* ECF No. 14 (Plaintiffs' consent to magistrate judge jurisdiction). Because Defendants have not appeared, Plaintiffs are unaware of whether Defendants consent to a magistrate judge for all purposes.

XIV. OTHER REFERENCES

Whether the case is suitable for reference to binding arbitration, a special master, or the Judicial Panel on Multidistrict Litigation.

This case is not suitable for reference.

XV. NARROWING OF ISSUES

Issues that can be narrowed by agreement or by motion, suggestions to expedite the presentation of evidence at trial (e.g., through summaries or stipulated facts), and any request to bifurcate issues, claims, or defenses.

In view of Defendants' failure to appear in this litigation or respond to the Complaint, Plaintiffs do not believe the issues can be narrowed by agreement at this time.

XVI. EXPEDITED TRIAL PROCEDURE

Whether this is the type of case that can be handled under the Expedited Trial Procedure of General Order No. 64 Attachment A. If all parties agree, they shall instead of this Statement, file an executed Agreement for Expedited Trial and a Joint Expedited Case Management Statement, in accordance with General Order No. 64 Attachments B and D.

Plaintiffs do not believe this is the type of case that should be handled under the Expedited Trial Procedure of General Order No. 64.

XVII. SCHEDULING

Proposed dates for designation of experts, discovery cutoff, hearing of dispositive motions, pretrial conference and trial.

In view of Defendants' failure to appear in this litigation or respond to the Complaint, Plaintiffs believe that a case schedule is not necessary at this time.

XVIII. TRIAL

Whether the case will be tried to a jury or to the court and the expected length of the trial.

In view of Defendants' failure to appear in this litigation or respond to the Complaint, Plaintiffs believe that a trial plan is not necessary at this time. Nonetheless, Plaintiffs request a jury trial and expect the length of the trial to be ten court days.

XIX. DISCLOSURE OF NON-PARTY INTERESTED ENTITIES OR PERSONS

Whether each party has filed the "Certification of Interested Entities or Persons" required by Civil Local Rule 3-15. In addition, each party must restate in the case management statement the contents of its certification by identifying any persons, firms, partnerships, corporations (including parent corporations) or other entities known by the party to have either: (i) a financial interest in the subject matter in controversy or in a party to the proceeding; or (ii) any other kind of interest that could be substantially affected by the outcome of the proceeding. In any proposed class, collective, or representative action, the required disclosure includes any person or entity that is funding the prosecution of any claim or counterclaim.

Plaintiffs filed their Certificate of Interested Entities on October 29, 2019. ECF No. 6. Plaintiffs hereby restate the contents of that Certificate: there is no such interest to report.

XX. PROFESSIONAL CONDUCT

Whether all attorneys of record for the parties have reviewed the Guidelines for Professional Conduct for the Northern District of California.

All attorneys of record for Plaintiffs have reviewed the Guidelines for Professional Conduct for the Northern District of California.

XXI. OTHER

Such other matters as may facilitate the just, speedy and inexpensive disposition of this

matter.

Plaintiffs intend to secure the just, speedy, and inexpensive disposition of this matter with a motion for default judgment.

Dated: February 6, 2020

Respectfully submitted,

COOLEY LLP

/s/ Travis LeBlanc
Travis LeBlanc
Daniel J. Grooms
Kyle C. Wong
Joseph D. Mornin

Attorneys for Plaintiffs
WHATSAPP INC. and FACEBOOK, INC.

CASE MANAGEMENT ORDER

The above SEPARATE CASE MANAGEMENT STATEMENT AND [PROPOSED] ORDER is approved as the Case Management Order for this case and all parties shall comply with its provisions. [In addition, the Court makes the further orders stated below:]

IT IS SO ORDERED.

Dated:

U.S. Magistrate Judge Jacqueline S. Corley