

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

5 DANIEL J. GROOMS (D.C. Bar No. 219124) (*pro hac vice* forthcoming)
(dgrooms@cooley.com)
6 1299 Pennsylvania Avenue, NW, Suite 700
Washington, DC 20004-2400
7 Telephone: (202) 842-7800
Facsimile: (202) 842-7899

8 Attorneys for Plaintiffs
9 WHATSAPP INC. and FACEBOOK, INC.

10 UNITED STATES DISTRICT COURT
11 NORTHERN DISTRICT OF CALIFORNIA
12

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

15
16 Plaintiffs,

17 v.

18 NSO GROUP TECHNOLOGIES LIMITED
19 and Q CYBER TECHNOLOGIES LIMITED,

20 Defendants.

Case No.

COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiffs WhatsApp Inc. and Facebook, Inc. (collectively, “Plaintiffs”) allege the following
2 against Defendants NSO Group Technologies Ltd. (“NSO Group”) and Q Cyber Technologies Ltd.
3 (“Q Cyber”) (collectively, “Defendants”):

4 **INTRODUCTION**

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

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

17 **PARTIES**

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

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

23 5. Defendant NSO Group was incorporated in Israel on January 25, 2010, as a limited
24 liability company. Ex. 1. NSO Group had a marketing and sales arm in the United States called
25 WestBridge Technologies, Inc. Ex. 2 and 3. Between 2014 and February 2019, NSO Group obtained
26 financing from a San Francisco–based private equity firm, which ultimately purchased a controlling
27 stake in NSO Group. Ex. 4. In and around February 2019, NSO Group was reacquired by its founders
28

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

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

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

13 JURISDICTION AND VENUE

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

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

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

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

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

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

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

5 **FACTUAL ALLEGATIONS**

6 **A. Background on Facebook**

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

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

14 **B. Background on WhatsApp**

15 **1. The WhatsApp Service**

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

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

23 **2. WhatsApp’s Terms of Service**

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

26 20. The WhatsApp Terms stated that “You must use our Services according to our Terms
27 and policies” and that users agreed to “access and use [WhatsApp’s] Services only for legal,
28 authorized, and acceptable purposes.”

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

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

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

15 **C. Background on NSO Group and Pegasus**

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

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

26 26. According to media reports and NSO documents, Defendants claimed that Pegasus
27 could be surreptitiously installed on a victim’s phone without the victim taking any action, such as
28

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

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

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

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

22
23
24
25
26
27 ¹ See Financial Times, “Israel’s NSO: the business of spying on your iPhone” (May 14, 2019),
28 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/qvakh3/inside-nso-group-spyware-demo.

1 **D. Defendants Agreed to the WhatsApp Terms**

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

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

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

9 **1. Overview**

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

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

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

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

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

6 **3. Defendants’ Unauthorized Access of Plaintiff’s Servers**

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

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

20 37. Between approximately April and May 2019, Defendants used and caused to be used,
21 without authorization, WhatsApp Signaling Servers, in an effort to compromise Target Devices. To
22 avoid the technical restrictions built into WhatsApp Signaling Servers, Defendants formatted call
23 initiation messages containing malicious code to appear like a legitimate call and concealed the code
24 within call settings. Disguising the malicious code as call settings enabled Defendants to deliver it to
25 the Target Device and made the malicious code appear as if it originated from WhatsApp Signaling
26 Servers. Once Defendants’ calls were delivered to the Target Device, they injected the malicious code
27 into the memory of the Target Device—even when the Target User did not answer the call.
28

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

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

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

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

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

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

23
24 ² See Fast Company, "Israeli cyberweapon targeted the widow of a slain Mexican journalist" (March
25 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
26 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>;
27 The Guardian, "Israeli firm linked to WhatsApp spyware attack faces lawsuit" (May 18,
28 2019), available at <https://www.theguardian.com/world/2019/may/18/israeli-firm-nso-group-linked-to-whatsapp-spyware-attack-faces-lawsuit>.

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.

1 **PLAINTIFFS RESPECTFULLY DEMAND A JURY TRIAL.**

2
3 Dated: October 29, 2019

Respectively submitted,

4 COOLEY LLP

5
6 /s/ Travis LeBlanc

Travis LeBlanc

7 Daniel J. Grooms

8 Joseph D. Mornin

9 Attorneys for Plaintiffs

WHATSOEVER INC. and FACEBOOK, INC.

10 Platform Enforcement and Litigation

Facebook, Inc.

11 Jessica Romero

Tyler Smith

12 Michael Chmelar

13 Bridget Freeman

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28