COOLEY LLP
MICHAEL G. RHODES (116127) (rhodesmg@cooley.com)
TRAVIS LEBLANC (251097) (tleblanc@cooley.com)
BETHANY C. LOBO (248109) (blobo@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)
ELIZABETH B. PRELOGAR (262026) (admission pending)
(eprelogar@cooley.com)
1299 Pennsylvania Avenue, NW, Suite 700
Washington, DC 20004-2400
Telephone: (202) 842-7800
Facsimile: (202) 842-7899

O'MELVENY & MYERS LLP
MICHAEL R. DREEBEN (D.C. Bar No. 370586) (*pro hac vice* pending)
(mdreeben@omm.com)
1625 I Street NW
Washington, D.C. 20006
Telephone: (202) 383-5300

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. 4:19-cv-07123-PJH

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Date: May 27, 2020
Time: 9:00 a.m.
Courtroom: 3
Judge: Hon. Phyllis J. Hamilton

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

PAGE

Statutes

Other Authorities

I. INTRODUCTION

A flawed premise runs through the motion to dismiss ("MTD"). Defendants contend that they cannot be held responsible for designing and marketing spyware and then deploying it using WhatsApp's U.S.-based servers, including in California, to hack into WhatsApp users' devices. Instead, Defendants pin blame on unidentified foreign sovereigns. That argument fails at every turn: Defendants cannot cloak themselves in their putative clients' immunity; they are accountable for suit in a California court; and the Complaint states valid claims for relief based on Defendants' unauthorized access to and hijacking of WhatsApp's servers. The motion should be denied.

First, the Foreign Sovereign Immunities Act ("FSIA") affords Defendants no protection. The statute confers immunity only on foreign states—not private companies who develop and operate their own technology and then claim to act on a foreign state's behalf. Defendants seek to expand the *domestic* doctrine of derivative sovereign immunity to cover contractors of *foreign* sovereigns—an unwarranted leap that no court in this circuit has endorsed and that conflicts with the Supreme Court's decision in *Samantar v. Yousuf*, 560 U.S. 305 (2010). Nor can Defendants satisfy the prerequisites for derivative sovereign immunity even assuming it applies, given the discretion, control, and independence they concede they exercised in carrying out the attacks alleged in the Complaint. In any event, this issue cannot be resolved in Defendants' favor at the pleading stage: their showing is conclusory, identifies no specific foreign sovereigns, and would require discovery.

Second, Defendants' putative foreign clients are not "required parties" under Fed. R. Civ. P. 19(a). The Complaint alleges only wrongdoing by Defendants—not any other actor. And Rule 19(b)'s considerations of "equity and good conscience" require the action to proceed.

Third, the Court has personal jurisdiction over Defendants. They agreed to litigate here, under California law; obtained financing from a California firm; accessed and exploited Plaintiffs' California servers—as well as used separate servers in California—to carry out their attacks; intentionally directed their tortious conduct towards California-based corporations; and the effects of their actions were foreseeably felt in California by Plaintiffs and WhatsApp users.

Finally, the Complaint validly alleges violations of the Computer Fraud and Abuse Act ("CFAA") and trespass to chattels. Defendants had no authority to access WhatsApp's servers with

an imposter program, manipulate network settings, and commandeer the servers to attack WhatsApp users. That invasion of WhatsApp's servers and users' devices constitutes unlawful computer hacking at the heart of the CFAA's unauthorized-access offense. And Defendants' interference with the intended functioning of Plaintiffs' servers constitutes trespass to chattels under established law.

II. BACKGROUND

WhatsApp provides an end-to-end encrypted communication service on mobile devices. Compl. ¶ 17. Users must install the WhatsApp app to use the WhatsApp Service. *Id.* WhatsApp routes end-to-end encrypted calls and messages between users using network protocols built into its app. *Id.* ¶¶ 17-18, 35.

According to the allegations in the Complaint, which must be taken as true on a motion to dismiss under Fed. R. Civ. P. 12(b), Defendants NSO Group Technologies Inc. and Q Cyber Technologies Inc. (collectively, "NSO") manufactured, distributed, and operated surveillance technology, also known as "spyware," designed to intercept and extract information and communications from mobile phones and devices of WhatsApp users ("Target Devices"). Compl. ¶¶ 24–29. NSO's spyware includes a product called "Pegasus," which was designed to be surreptitiously installed on a victim's phone without her knowing her phone had been compromised. *Id.* ¶¶ 24-29, Ex. 10.[1] Once installed, Pegasus captured an 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 WhatsApp and other services. *Id.* ¶¶ 24-29. NSO ultimately deployed its spyware to hack into approximately 1,400 phones and devices belonging to WhatsApp users, including attorneys, journalists, human rights activists, government officials, and others. *Id.* ¶ 42.

To carry out the attacks, NSO created WhatsApp accounts, gained unauthorized access to WhatsApp's servers in the United States, including in California, and deployed spyware to connect users' devices to a network of remote servers in California that NSO controlled. *Id.* ¶¶ 32, 35-48, 60-61. First, NSO reverse-engineered the WhatsApp app and wrote a program that emulated legitimate WhatsApp network traffic while hiding malware transmitted to users. *Id.* ¶¶ 35-48. By using its

[1] Defendants' claim (MTD at 2 n.2) that Facebook sought to purchase Pegasus to monitor Onavo app users is inaccurate and an attempt to distract from Defendants' own conduct and the issues in this case.

unauthorized program to access WhatsApp servers, NSO circumvented technical restrictions and security measures that prevent users from altering network call settings. *Id.* NSO then manipulated those settings to covertly transmit malicious code through WhatsApp servers and inject the code into users' devices, even when the victims did not answer the call. *Id.* Once NSO's malicious code was activated, NSO's malicious servers transmitted additional malware that gave NSO and its customers remote access to the devices. *Id.* ¶¶ 39-41. NSO used a network of computers to monitor and update Pegasus after it was implanted on users' devices. *Id.* ¶ 28. These NSO-controlled computers served as the nerve center through which NSO controlled its customers' operation and use of Pegasus. *Id.*

In May 2019, Plaintiffs detected and stopped NSO's unauthorized access and abuse of the WhatsApp service and computers. *Id.* ¶ 44. The attack damaged Plaintiffs' goodwill and forced them to incur costs to investigate and prevent NSO's hacking activities, including updating the WhatsApp app on users' devices. *Id.* ¶¶ 44-45, 57. This suit followed.

III. ARGUMENT

A. NSO Has No Valid Claim to Immunity.

1. The Foreign Sovereign Immunities Act only applies to foreign states.

NSO's claim to FSIA immunity, MTD at 8-9, is precluded by the Supreme Court's decision in *Samantar v. Yousuf*, 560 U.S. 305 (2010). *Samantar* held that the FSIA confers immunity only on a "foreign state" itself, "as the Act defines that term." *Id.* at 325. A "foreign state," as defined in the FSIA, does not "include an official acting on behalf of the foreign state," *id.* at 319, let alone a private contractor claiming to act for a foreign state, *see Broidy Capital Management LLC v. Muzin*, 2020 WL 1536350, at *5 (D.D.C. Mar. 31, 2020) (FSIA inapplicable to consulting firm's claim for immunity as Qatari agent); *Doğan v. Barak*, 932 F.3d 888, 893 & n.4 (9th Cir. 2019) (FSIA immunity "does not extend" to entities other than "foreign states"). Here, NSO is a for-profit commercial company—decidedly *not* a foreign state. *See* Compl. ¶¶ 1, 5-7, 29. The FSIA has no bearing here.

To avoid this straightforward conclusion, NSO asserts that the allegedly unlawful conduct was "carried out by sovereign governments." MTD at 8. But it offers no support for its novel theory that the FSIA confers immunity on private companies, sued in their own name, when those entities attribute

their unlawful activity to a foreign sovereign.[2] The FSIA remains inapplicable because this suit asserts no claims against and seeks no relief from a *foreign state*. Indeed, even where the FSIA protects an "agency or instrumentality of a foreign state," it restricts immunity to entities that are "organ[s]" of the state or are majority-owned by the state. 28 U.S.C. § 1603(b)(1)-(2); *see Dole Food Co. v. Patrickson,* 538 U.S. 468, 474 (2003). NSO qualifies as neither, *see* Compl. ¶¶ 5-6, and its position would render those limitations on foreign state corporate immunity superfluous. *Cf. Dole*, 538 U.S. at 476-77 (relying on superfluity canon in construing the FSIA).

NSO's attempt to shift liability to foreign states is further flawed because NSO does not dispute that it engaged in critical conduct at the heart of the complaint: NSO concedes that it (1) "design[ed]," manufactured, "market[ed]," sold, "configure[d]," and "deploy[ed]" Pegasus; (2) "assist[ed] with the training, setup, and installation of the Pegasus technology" and provided "technical support" post-installation; (3) and, at NSO's discretion, canceled or suspended customers' use of Pegasus. MTD at 2-6.[3] And while NSO provides no explanation of its precise role in routing malicious code through Plaintiffs' servers other than an unadorned denial, MTD at 7, the Complaint specifically and credibly alleges that NSO was deeply involved in carrying out the attack and claimed ownership of the attack after WhatsApp stopped it. Compl. ¶¶ 32, 35-39, 42, 45. NSO's unsupported claim that the FSIA immunizes all of the conduct at issue thus affords no basis for dismissal.

2. No "derivative foreign sovereign immunity" exists.

NSO has no sounder basis for claiming "derivative foreign sovereign immunity" as a private contractor working for foreign governments. MTD at 9-10. Although such immunity protects certain contractors working "*with the United States*," *Campbell-Ewald Co. v. Gomez*, 136 S. Ct. 663, 672 (2016) (emphasis added), no court in this Circuit has extended that doctrine to work performed for *foreign* sovereigns. Nor should this Court create such federal common law; the foreign context implicates international comity concerns for the Executive Branch, not courts, to address.

---

[2] The nature of the victims targeted during the attack, including journalists and attorneys, is not consistent with the type of government operations NSO claims to support in its motion.

[3] NSO offers no evidence that the development, testing, or upgrading of Pegasus was commissioned by a foreign state, nor does it dispute that its own use of its product for development purposes is primarily for commercial advantage over other companies that provide similar services.

The leap from the domestic to the foreign context is not "small." MTD at 10. Domestic "derivative sovereign immunity" reflects that the United States and its agents have "the same interest in getting the Government's work done." *Boyle v. United Techs. Corp.*, 487 U.S. 500, 505 (1988). In that context, federal courts have created a federal common law rule to protect unique federal interests. *Id.* at 504-05. This is one of the rare instances where fashioning federal common law is appropriate. But foreign sovereign immunity is instead based on international comity, *Broidy*, 2020 WL 1536350, at *7, and federal courts have no freewheeling license to fashion common law rules to protect international relations. Because "the Executive is the sole organ of the federal government in the field of international relations," and has the responsibility to account for comity considerations, *Pasquantino v. United States*, 544 U.S. 349, 369 (2005) (citation omitted), separation-of-powers concerns preclude judicial creation of a new derivative sovereign immunity doctrine for contractors working for foreign sovereigns. *See Hernandez v. Mesa*, 140 S. Ct. 735, 747 (2020) (cautioning against "unwarranted judicial interference in the conduct of foreign policy") (citation omitted).

In determining whether a *foreign* entity is entitled to immunity, courts therefore confine themselves to established sources of law. *See Doğan*, 932 F.3d at 891-93; *Broidy*, 2020 WL 1536350, at *6-7. Here, no established law recognizes the novel immunity NSO seeks.[4] Indeed, even common-law *foreign-official* immunity requires either a Suggestion of Immunity from the U.S. State Department, or a judicial determination that the official (by virtue of his position or conduct) possesses the established prerequisites for immunity. *See Doğan*, 932 F.3d at 891-93. Here, the State Department has not filed a Suggestion of Immunity. And as a private non-governmental entity, NSO has no claim by virtue of its position. *See Broidy*, 2020 WL 1536350, at *5 ("Status-based immunity" "is unavailable here because the defendants are neither Qatari diplomats nor Qatari heads of state.").

That leaves only conduct-based foreign-official immunity, which sets a standard NSO cannot meet. As articulated by the Restatement (Second), a foreign official may have common law immunity "with respect to acts performed in his official capacity if the effect of exercising jurisdiction would be

[4] Courts sometimes also consider whether the State Department has an "established policy" recognizing the asserted immunity. *See Broidy*, 2020 WL 1536350, at *5-6 (citation omitted). NSO identifies no State Department guidance recognizing immunity for foreign government contractors.

to enforce a rule of law against the [foreign] state." RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW § 66(f) (1965); *Doğan*, 932 F.3d at 893-95. Here, Plaintiffs seek to halt wrongdoing by *NSO*, not a foreign state; NSO's liability rests on its own conduct. And the effect of a judgment in Plaintiffs' favor would not be to enforce a rule of law against the unidentified foreign states that transacted with NSO. Specifically, a judgment enjoining *NSO* from creating accounts with Plaintiffs, accessing their services, or violating or facilitating violations of their terms of service, *see* Compl. at 14, would bind only NSO. And any damages judgment would not be paid from a foreign state's coffers. Accordingly, NSO cannot prevail even under the common-law foreign-*official* immunity framework.

It is thus unsurprising that hardly any authorities (even outside this Circuit) recognize "foreign derivative sovereign immunity" for private contractors. NSO relies on *Butters v. Vance International, Inc.*, 225 F.3d 462 (4th Cir. 2000), and its progeny. MTD at 10. But *Butters* is no longer good law. *Butters* is a pre-*Samantar* decision interpreting the FSIA—not common-law immunity—to confer immunity on private agents of foreign governments. *See* 225 F.3d at 464, 466-67; *see also Ruddell v. Triple Canopy, Inc.*, 2016 WL 4529951, at *7 (E.D. Va. Aug. 29, 2016) ("*Butters* . . . confronted a contractor's immunity claim derived from the [FSIA], not immunity derived from the United States' common law sovereign immunity"). *Samantar* has since made clear that the FSIA confers immunity only on foreign states, *see* III.A.1, *supra*, effectively abrogating *Butters*' holding.

3. NSO cannot satisfy the requirements for the "derivative sovereign immunity" applicable to certain U.S.-government contractors.

Even if *foreign*-government contractors could invoke the "derivative sovereign immunity" available to *U.S.-government* contractors, NSO cannot satisfy that doctrine's requirements.

Immunity for U.S.-government contractors, "unlike the sovereign's, is not absolute." *Campbell-Ewald*, 136 S. Ct. at 672. Derivative sovereign immunity "is limited to cases in which a contractor had no discretion in the design process and completely followed government specifications." *Cabalce v. Thomas E. Blanchard & Assocs., Inc.*, 797 F.3d 720, 732 (9th Cir. 2015) (internal quotations and citation omitted). Where a contractor "had a significant role in the design of the Program" and was not "acting merely and solely as directed by the Government," *Salim v. Mitchell*, 268 F. Supp. 3d 1132, 1150 (E.D. Wash. 2017) (*Salim II*)—or where a contractor had "discretion" in

"administering" the contracted-for program, *Novoa v. GEO Grp., Inc.*, 2018 WL 4057814, at *3 (C.D. Cal. Aug. 22, 2018)—no derivative sovereign immunity exists.

NSO bears no resemblance to the no-discretion contractor archetype protected by U.S.-government derivative sovereign immunity, as its own statements confirm.[5] No foreign government identified a need for NSO's services, hired NSO, and directed NSO to deliver a product according to particular specifications and subject to governmental control. Just the opposite: Pegasus was NSO's brainchild—conceived, executed, and marketed by NSO. NSO designed Pegasus, promoted and licensed Pegasus to multiple parties, and trained those customers to use Pegasus. Compl. ¶¶ 1, 24, 26-27, 29. Even if foreign sovereigns identified which users to target, NSO determined the parameters and operation of the Pegasus technology—including by providing technical support and continuously monitoring customers for compliance with NSO's terms. *Id.* ¶¶ 28-29. Courts in this Circuit routinely reject claims of derivative sovereign immunity on analogous facts. *See, e.g.*, *Cabalce*, 797 F.3d at 732 (denying immunity where contractor "designed the destruction plan" for seized fireworks "without government control or supervision"); *Salim II*, 268 F. Supp. 3d at 1148 (no immunity when contractors did not "act[] specifically at the direction of the Government, but rather . . . designed and implemented" a program as "architects" who then "trained" CIA personnel); *Washington v. GEO Grp., Inc.*, 2019 WL 3565105, at *5 (W.D. Wash. Aug. 6, 2019) (denying immunity because contractor failed to show it had "no discretion in the design process and completely followed government specifications").

4. NSO's "extrinsic evidence" cannot save its immunity defense.

Although NSO's immunity claims have no legal basis and should be dismissed outright, at a minimum, NSO wrongly relies on extrinsic evidence to press those claims. MTD at 8-10 & n.7. Derivative sovereign immunity is not a jurisdictional doctrine. *E.g.*, *Adkisson v. Jacobs Eng'g*

[5] *See* MTD at 2 (NSO "design[ed] and market[ed]" its technology to governments); *id.* at 3-4 ("NSO has voluntarily undertaken additional steps" to monitor the use of Pegasus, and NSO "contractually can suspend—and ha[s] suspended, and would terminate—service to customers engaged in any improper use of NSO's Pegasus technology"); *id.* at 3-4 ("NSO requires its customers" to agree to use NSO technology for specified purposes and to "immediately notify NSO of any potential misuse"); *see also* Compl., Ex. 10 (NSO's Pegasus Manual) at 55 ("NSO is responsible to deploy and configure the Pegasus hardware and software at the customer premises"); *id.* at 58 ("[a]ll the necessary hardware is supplied with the system upon deployment"); *id.* at 61 ("[NSO] [is] responsible for the system setup and training before its hand-over to the customer").

Grp., Inc., 790 F.3d 641, 645 (6th Cir. 2015); *accord Gomez v. Campbell-Ewald Co.*, 768 F.3d 871, 874, 879-82 (9th Cir. 2014), *aff'd*, 136 S. Ct. 663 (2016). And even if it were, "[w]here jurisdiction is intertwined with the merits"—as it is here, where NSO's twin defenses hinge on the identity of its customers and the services it provided—"the truth of the [complaint's] allegations" must be assumed "unless controverted by undisputed facts in the record." *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1139 (9th Cir. 2003) (citation omitted). Accordingly, the allegations in Plaintiffs' Complaint control. *Moore v. McAleenan*, 2019 WL 2870079, at *2 (D. Alaska July 3, 2019).

Beyond that, NSO's factual showing does not come close to supporting an attack on jurisdiction. The Complaint alleges targeting of 1,400 separate devices, Compl. ¶ 42, and NSO does not specify who it was working for in each attack. Instead, NSO relies on a conclusory declaration from its CEO Shalev Hulio stating that "NSO markets and licenses its Pegasus technology exclusively to sovereign governments and authorized agencies," and those sovereigns—not NSO—"operate [the] Pegasus technology." Hulio Decl. ¶¶ 9, 14-15. But Hulio fails to identify *any* specific foreign sovereign for whom NSO worked—let alone cite a single contract or any evidence establishing NSO's purportedly limited operational role. That factual showing is plainly insufficient.

Finally, before any fact-based immunity defense could be entertained, Plaintiffs would be entitled to discovery. *See Laub v. U.S. Dep't of Interior*, 342 F.3d 1080, 1093 (9th Cir. 2003) (discovery appropriate when "jurisdictional facts are contested or more facts are needed" to determine jurisdiction). All information relating to NSO's customers and NSO's services is in NSO's possession. Absent discovery on these subjects, NSO's motion cannot be granted. *See id.* (reversing denial of jurisdictional discovery where plaintiff sought "detailed accounting of all [defendant's] transactions"); *Salim v. Mitchell*, 183 F. Supp. 3d 1121, 1130-31 (E.D. Wash. 2016) ("*Salim I*") (denying motion to dismiss that asserted "derivative sovereign immunity" defense because "no discovery has been conducted"); *Novoa*, 2018 WL 4057814, at *3 (same).[6]

[6] NSO's passing reference to the act of state doctrine also fails. MTD at 10-11 & n.12. NSO concedes that this argument is not ripe for decision, *id.*, and it also lacks merit. *NSO* is alleged to have engaged in unlawful hacking and breach of contract, and proving those violations does not require the Court to rule on the validity of the act of any *foreign sovereign*. *W.S. Kirkpatrick & Co. v. Envtl. Tectonics Corp, Int'l*, 493 U.S. 400, 409-10 (1990). Further, gaining unauthorized access to WhatsApp's servers

B. The Complaint Does Not Fail to Join a Required Party.

NSO is wrong to contend that the Complaint must be dismissed because Plaintiffs did not join NSO's foreign-sovereign customers. MTD at 18-19. NSO's customers are not "required part[ies]" under Rule 19(a), and even if they were, considerations of "equity and good conscience" evaluated under Rule 19(b) require the action to "proceed among the existing parties." Fed. R. Civ. P. 19; *see* Fed. R. Civ. P. 12(b)(7).

NSO argues that under Rule 19(a)(1)(A) "the court cannot accord complete relief among existing parties" without NSO's foreign-sovereign clients. But this suit seeks to enjoin wrongdoing by *NSO*—not any other actor. An order enjoining NSO from, *inter alia*, accessing or attempting to access Plaintiffs' systems, or violating or facilitating violations of Plaintiffs' terms of service, will afford Plaintiffs "complete relief." NSO's allusion (MTD at 19) to hypothetical relief against sovereign clients, not sought by Plaintiffs, is irrelevant—Rule 19(a)(1)(A) "is concerned only with relief as between the persons already parties, not as between a party and the absent person." *Eldredge v. Carpenters 46 N. Cal. Ctys. Joint Apprenticeship & Training Comm.*, 662 F.2d 534, 537 (9th Cir. 1981) (internal quotations and citation omitted). Nor can NSO rely on "possible future conduct" by third-party sovereigns that might "frustrate the remedial purposes of [a] court-order[]" enjoining NSO in order to "avoid [its] own liability for [illegal] practices." *Id.*

NSO incorrectly suggests that an injunction restraining it "and all other persons acting in concert with or conspiracy with" it must include foreign sovereigns. Compl. at 14. Such language is "standard boilerplate drawn from Rule 65 describing the 'persons bound' by 'every injunction.'" *E.E.O.C. v. Peabody W. Coal Co.*, 610 F.3d 1070, 1080 (9th Cir. 2010) (quoting Fed. R. Civ. P. 65). The "better reading" is that the language does not seek "injunctive relief against" an immune sovereign. *Id.*; *see In re Estate of Ferdinand Marcos Human Rights Litig.*, 94 F.3d 539, 545-46 (9th Cir. 1996). But even if NSO's reading were correct, "the proper response . . . would . . . be[] simply

---

located in the United States could never be considered an "act of state." That doctrine bars adjudicating only the sovereign acts of a foreign government done "within its own territory." *Id.* Courts are free to "judge the legality and propriety of an act that occurred within the borders of the United States." *Liu v. Republic of China*, 892 F.2d 1419, 1433 (9th Cir. 1989).

to deny [the] request for injunctive relief" against a sovereign, "shap[e] the relief" sought under Rule 19(b)(2)(B), or permit Plaintiffs leave to amend under Rule 15. *Peabody*, 610 F.3d at 1077, 1080.

Finally, even if NSO's sovereign clients were "required parties" under Rule 19(a), Rule 19(b) dismissal is unwarranted. NSO argues that this action would "prejudice [its] customers" by "ignoring their sovereign status." MTD at 19 (citation omitted). But the rule for foreign sovereigns is not categorical; rather, the inquiry turns on multiple "factors varying with the different cases." *Republic of Phil. v. Pimentel*, 553 U.S. 851, 863 (2008) (citation omitted). An action should continue without a required sovereign where considerations of "equity and good conscience" weigh against the severe remedy of dismissal. *Id.* at 862-63 (quoting Rule 19(b)). That is true here: If NSO is liable for the violations alleged, it cannot remain free to abuse Plaintiffs' systems and victimize Plaintiffs' users by hiding behind the actions of absent sovereign clients that can pursue their own interests.[7]

C. The Court Has Personal Jurisdiction Over NSO.

Personal jurisdiction over NSO exists for two independent reasons: NSO (1) consented to jurisdiction by accepting WhatsApp's Terms; and (2) directed its conduct at California. Plaintiffs need only identify "facts that if true would support jurisdiction" to defeat a Rule 12(b)(2) dismissal. *Mavrix Photo, Inc. v. Brand Techs., Inc.*, 647 F.3d 1218, 1223 (9th Cir. 2011); *Ballard v. Savage*, 65 F.3d 1495, 1498 (9th Cir. 1995).[8] Plaintiffs have made this showing.

1. NSO consented to this Court's jurisdiction.

By agreeing to WhatsApp's Terms, which include a forum selection clause designating this Court, NSO "consented to personal jurisdiction." *Automattic, Inc. v. Steiner*, 82 F. Supp. 3d 1011, 1022 (N.D. Cal. 2015) (Hamilton, J.) (citation omitted); *Craigslist, Inc. v, Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1052 (N.D. Cal. 2010) (Hamilton, J.) (defendants consented to jurisdiction by "agree[ing] to the TOUs as a condition to accessing Plaintiff's website"). Such forum selection clauses are "*prima facie* valid" and are "enforceable absent a strong showing" by the opposing party that the

[7] NSO's suggestion that it will be hampered in obtaining discovery needed for its defense, MTD at 19 n.18, is unfounded. NSO can prove its own conduct without relying on others' evidence.

[8] Under Rule 12(b)(2), the Court takes Plaintiffs' "uncontroverted allegations in the complaint" as true, *Mavrix*, 647 F.3d at 1223, and resolves conflicts "over statements contained in affidavits" in "[P]laintiff[s'] favor," *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004).

clause is invalid or its enforcement would otherwise be "unreasonable or unjust." *Manetti-Farrow, Inc. v. Gucci Am., Inc.*, 858 F.2d 509, 514 (9th Cir. 1988) (citation omitted).

The WhatsApp Terms applicable to NSO contained a "Dispute resolution" section with the following forum selection clause and choice of law provision:

> If you are not subject to the "Special Arbitration Provision for United States or Canada Users" section below, you agree that you will resolve any Claim you have with us relating to, arising out of, or in any way in connection with our Terms, us, or our Services (*each, a "Dispute," and together, "Disputes"*) exclusively in the United States District Court for the Northern District of California or a state court located in San Mateo County in California, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating *all such Disputes*.
>
> Governing Law: The laws of the State of California govern our Terms, as well as any Disputes, whether in court or arbitration, which might arise between WhatsApp and you, without regard to conflict of law provisions.

Duffy Decl. ¶¶ 4, 6, Ex. 1 (emphasis added). The arbitration provision referenced in the forum selection clause states that arbitration applies to "all disputes" that involve U.S. or Canadian users, with the exception of a subset of actions. *Id.*

NSO does not deny that it accepted WhatsApp's Terms or that the forum selection clause is enforceable. *See* MTD at 11-12. Instead, NSO wrongly urges the Court to interpret the term "Dispute" to apply only to users' claims against WhatsApp, and not vice versa. *See* MTD at 11-12. That reading ignores the plain meaning of the forum selection clause, as this suit involves a Dispute that NSO "ha[s] with [WhatsApp]"—*i.e.*, a dispute *between* NSO and WhatsApp.

NSO's one-sided reading of the term "Dispute" in the forum selection clause is likewise inconsistent with the use of the same term in the choice-of-law and arbitration provisions. "[E]ach clause" of the Terms "help[s] to interpret the other." Cal. Civ. Code § 1641; *see Principal Mut. Life Ins. Co. v. Vars, Pave, McCord & Freedman*, 65 Cal. App. 4th 1469, 1478 (1998) ("[W]ords used in a certain sense in one part of a contract are deemed to have been used in the same sense elsewhere.") The choice-of-law provision makes clear that the term "Dispute" applies to all actions *between* users and WhatsApp, providing that California law "govern[s] [WhatsApp's] Terms, as well as any Disputes . . . which might arise between WhatsApp and you." *See* Duffy Decl. ¶¶ 4, 6, Ex. 1. And the arbitration

provision uses "dispute" the same way, applying to "all disputes" whether WhatsApp or the user initiates them. Based on the consistent meaning of "Dispute" as used throughout the Terms, NSO consented to this Court's exercise of personal jurisdiction. *See Craigslist*, 649 F. Supp. 2d at 1052.

2. Alternatively, NSO's contacts with California establish specific jurisdiction.

Specific jurisdiction over a defendant exists when (1) the defendant "purposefully avail[ed]" itself of the forum's benefits regarding a contract claim or "purposefully direct[ed]" its activities at the forum with respect to a tort claim; (2) the plaintiff's claims "arise[] out of or relate[] to" those "forum-related activities"; and (3) the exercise of jurisdiction is consistent with fair play and substantial justice. *See Dole Food Co. v. Watts*, 303 F.3d 1104, 1111 (9th Cir. 2002). Here, specific jurisdiction exists because Plaintiffs have established the first two prongs, and NSO has not "present[ed] a compelling case that the exercise of jurisdiction . . . would be unreasonable." *Id.* at 1117 (citation omitted).

a. NSO purposefully availed itself of California's benefits.

NSO contends that it did not purposefully avail itself of California's benefits because it has not engaged in in-forum conduct. MTD at 16. To the contrary, NSO "deliberately [] engaged in significant activities" and created "continuing obligations" in California, receiving "manifold benefits." *See Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475-76, 480 (1985). NSO: (1) contracted with California-based WhatsApp and agreed that California law governed; (2) committed to perform under WhatsApp's Terms; and (3) benefited from business activities directed at California.

First, NSO concedes that it contracted with WhatsApp and agreed to WhatsApp's Terms with a California choice-of-law clause when creating user accounts; indeed, NSO does not dispute that Plaintiffs have stated a claim for breach of those Terms. *See* Compl. ¶¶ 19, 30-31, 67-73; MTD at 7-8, 11. Contracting under California law shows that a defendant "chose[] to avail itself of the benefits and protections of California's laws." *Google, Inc. v. Eolas Techs. Inc.*, 2014 WL 2916621, at *3 (N.D. Cal. June 24, 2014) (finding personal jurisdiction). This is particularly true where "sophisticated" entities, like NSO, agree to a choice-of-law clause. *Facebook, Inc. v. Rankwave Co.*, No. 19-3738, at *8-9 (N.D. Cal. Nov. 14, 2019) (ECF No. 34); *see Burger King*, 471 U.S. at 481-82.

Second, NSO committed to perform continuously under the Terms, including by complying with WhatsApp's policies for ongoing use of the platform. *See* Compl. ¶¶ 20-22 (Terms require users,

e.g., not to "send . . . harmful computer code through or onto our Services[.]"). The "continuous course of dealing" under a contract governed by California law supports a finding of "purposeful availment." *Facebook*, No. 19-3738, at *8-10 (finding jurisdiction where foreign defendant agreed to plaintiff's Terms, including a California choice-of-law clause, as a condition of accessing plaintiff's data).

Third, NSO engaged in significant activities directed at California. NSO developed Pegasus using financing from a California-based private equity firm.[9] NSO also intentionally exploited WhatsApp's California-based infrastructure to develop its product and deliver malware to Target Devices. *See* Compl. ¶¶ 5, 11, 27-29, 34-40, 60-62; *see also* Exs. 4, 10 (advertising the surveillance capability of NSO's technology); MTD at 5 (admitting use and exploitation of WhatsApp's platform).

Additionally, to execute its scheme and install its spyware on WhatsApp users' devices, NSO separately entered into a contract with a California-based technology company, QuadraNet, that included a California choice-of-law clause. Compl. ¶ 34; Gheorghe Decl. ¶¶ 3-5; LeBlanc Decl. ¶¶ 2-3, Exs. 1, 2; Mornin Decl. ¶¶ 2-4, Exs. 1-5. NSO used QuadraNet's California-based server more than 700 times during the attack to direct NSO's malware to WhatsApp user devices in April and May 2019. Gheorghe Decl. ¶ 4; Mornin Decl. ¶¶ 2-4, Exs. 1-5; Compl. ¶ 34. And NSO knew or should have known the QuadraNet server was in California. *Id.*; *Panavision Intl., L.P. v. Toeppen*, 141 F.3d 1316, 1322 (9th Cir. 1998) (purposeful availment established because defendant was "likely" to know his conduct "had the effect of injuring" plaintiff "in California"). Tellingly, NSO does not deny that it contracted with QuadraNet, or that the QuadraNet server was used in the attack. *See* MTD at 14.

NSO's contacts with California, taken together, show that NSO purposefully availed itself of the forum's benefits. *See CompuServe, Inc. v. Patterson*, 89 F.3d 1257, 1264 (6th Cir. 1996) (specific jurisdiction where defendant contracted with in-forum plaintiff, including a forum state choice-of-law clause, and used plaintiff's server infrastructure); *Panavision*, 141 F.3d at 1321 (discussing

[9] NSO submits no evidence that this financing was not used to build Pegasus, and NSO's conclusory assertion that the financing is irrelevant (MTD at 16) fails on a Rule 12(b)(2) challenge. *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1019 (9th Cir. 2002); *see* Compl. ¶ 33, Ex. 4 (indicating that NSO created Pegasus while funded by a California firm). NSO issued "major upgrades" to Pegasus annually—and no evidence shows that this stopped from 2014 to February 2019, when a California firm owned 70 percent of NSO's business. *See* Compl., Ex. 10 at 64; fastcompany.com/90307864/u-s-fund-sells-israeli-hacking-firm-nso-group-amid-spy-mystery.

CompuServe with approval); *Summit Entm't, LLC v. Santia*, 2014 WL 12577430, at *3 (C.D. Cal. June 24, 2014) (purposeful availment met based on knowing use of California servers to commit breach).[10]

b. NSO purposefully directed its conduct at California.

A defendant purposefully directs its activities at California if it (1) commits an intentional act (2) expressly aimed at California (3) that causes harm it knows will likely be suffered here. *See Axiom Foods, Inc. v. Acerchem Int'l, Inc.*, 874 F.3d 1064, 1069 (9th Cir. 2017). Here, NSO purposefully directed its conduct to California: it marketed its ability to compromise California-based WhatsApp's security and used reverse-engineered WhatsApp technology and QuadraNet's California-based servers to hijack WhatsApp's servers, including in California, to distribute malware. Compl. ¶¶ 34-39, 60-62 & Ex. 10; Gheorghe Decl. ¶¶ 3-4; Mornin Decl. ¶¶ 2-6, Exs. 1-9. That satisfies *Axiom.*

The intentional-act element is beyond dispute. Plaintiffs allege that NSO violated California's Computer Data Access and Fraud Act ("CDAFA") by "knowingly" and "willfully" targeting WhatsApp's systems to disseminate malware. *See* Compl. ¶¶ 60-61, 64, 66; *see also* MTD at 2 & n.1; *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 826 (N.D. Cal. 2014) (exercising jurisdiction over foreign defendant who "had reason to know" that he was accessing plaintiff's "computer systems in California" through his affirmative acts directed towards the forum state). Indeed, NSO's product description of Pegasus specifically mentions WhatsApp and Facebook. Compl. ¶ 24, Ex. 10 at 33. NSO's willful targeting of WhatsApp's infrastructure suffices. *See Panavision*, 141 F.3d at 1321. Likewise, the harm element also exists: NSO's acts caused harm NSO knew would likely be suffered in California, Plaintiffs' principal place of business. *See id.*; *see also Dole*, 303 F.3d at 1113-14.

NSO appears to challenge only the express-aiming element, arguing that it did not target its conduct at California.[11] *See* MTD at 14-15. But NSO's actions aimed at, and caused effects in,

[10] Contrary to NSO's assertion (MTD at 16), *Boschetto v. Hansing*, 539 F.3d 1011 (9th Cir. 2008) and *Picot v. Weston*, 780 F.3d 1206 (9th Cir. 2015), are consistent with finding specific jurisdiction here. *See Boschetto*, 539 F.3d at 1019 (specific jurisdiction appropriate where (as here) a non-forum defendant contracts with forum plaintiff, then uses plaintiff's platform as "vehicle for commercial activity"); *Picot*, 780 F.3d at 1212 (no purposeful availment where, unlike here, parties contracted wholly in non-forum state and only plaintiff took significant in-forum actions under contract).

[11] NSO renews its improper contention that foreign governments (not NSO) committed the attacks. *See* MTD at 14. The Court cannot accept that contention at the pleading stage. *See* Section III.A.1,

California: its attacks targeted a California-based company and used WhatsApp's and QuadraNet's California-based servers. *See* Section II, *supra*. Such allegations satisfy the purposeful direction test. *See, e.g.*, *Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 2017 WL 3485881, at *24-25 (N.D. Cal. Aug. 15, 2017) (test met where defendant contracted with California company to access files via California servers to harm California-based company); *Craigslist*, 694 F. Supp. 2d at 1053 (same, where defendants knowingly used California plaintiff's website to sell services to enable users to bypass plaintiff's website's security measures, in violation of plaintiff's terms of service); *Seattle Sperm Bank, LLC v. Cryobank Am., LLC*, 2018 WL 3769803, at *2 (W.D. Wash. Aug. 9, 2018) (same, where defendant used in-forum server to misappropriate information belonging to in-forum company).

NSO errs in suggesting that it is irrelevant that Plaintiffs' servers are located in California. MTD at 14. NSO's cases hold only that purposeful direction is not shown *solely* by a defendant's *incidental* access to *third-party* servers in the forum state. *Rosen v. Terapeak, Inc.*, 2015 WL 12724071, at *9 (C.D. Cal. Apr. 28, 2015); *Hungerstation LLC v. Fast Choice LLC*, 2020 WL 137160, at *4-5 (N.D. Cal. Jan. 13, 2020). Here, in contrast, NSO intentionally targeted and exploited WhatsApp's California-based infrastructure; heavily marketed its ability to do so through a U.S.-based advertising arm, knowing this would damage WhatsApp; and contracted with California-based QuadraNet to lease and knowingly use its California servers to carry out the attack on WhatsApp and its users. Compl. ¶¶ 11, 60-62; *see* MTD at 2 n.1. Taken together, these actions underscore that California is "the focal point" of both the conduct and the harm suffered. *Axiom Foods, Inc.*, 874 F.3d at 1071; *see DEX Sys., Inc. v. Deutsche Post AG*, 727 F. App'x 276, 278 (9th Cir. 2018) (specific jurisdiction is often proper where defendants improperly exploit a plaintiff's in-forum servers).

Indeed, while NSO relies on *Axiom* and *Walden v. Fiore*, 571 U.S. 277 (2014), MTD at 13-14, those cases demonstrate that a defendant's international targeting of the forum state is relevant and, when *coupled with* injuries that the defendant knows are likely to be felt within the forum, will suffice to establish purposeful direction. *Axiom*, 874 F.3d at 1070-71; *Walden*, 571 U.S. at 287-88. That is

---

supra. That is particularly true where NSO's own description of its Pegasus software shows that it is NSO's software that accomplishes the attack: customers need "only insert the target phone number" and "[t]he rest is done automatically by [NSO's] system." Compl., Ex. 10 at 13. NSO does not dispute that Exhibit 10 is accurate; indeed, NSO invokes that exhibit itself. *See* MTD at 2 n.1.

the situation here. *See, e.g.*, *Panavision*, 141 F.3d at 1322; *Facebook, Inc. v. ConnectU LLC*, 2007 WL 2326090, at *2, *5-6 (N.D. Cal. Aug. 13, 2007) (purposeful direction where defendant's software used falsified login information to access Facebook and improperly export other users' information).

c. This suit arises from NSO's contacts with California.

All of Plaintiffs' claims and related injuries—including their CDAFA and breach of contract claims, which NSO does not move to dismiss—arise from NSO's creation of WhatsApp accounts, related agreement to the WhatsApp Terms, and misuse of WhatsApp's and QuadraNet's California-based infrastructure. *See* Compl. ¶¶ 11, 35-39, 60-62. That is sufficient. *In re W. States Wholesale Nat. Gas Antitrust Litig.*, 715 F.3d 716, 742 (9th Cir. 2013) (direct nexus satisfies test).

d. Exercising jurisdiction here is reasonable.

NSO has not made a "compelling case" that the exercise of jurisdiction would be unreasonable. *CollegeSource v. AcademyOne*, 653 F.3d 1066, 1079 (9th Cir. 2011). The reasonableness factors, far from tipping "sharply" towards NSO, *id.*, weigh strongly in favor of personal jurisdiction.

First, Defendants are wrong that their "purposeful interjection" into California's affairs is "negligible at best." *See* MTD at 17. Instead, this factor favors Plaintiffs based on the purposeful availment showing. *See* Section III.C.2.a, *supra*; *Roth v. Garcia Marquez*, 942 F.2d 617, 623 (9th Cir. 1991) (purposeful interjection redundant of purposeful availment test).

Second, the supposed burden an Israeli company faces litigating in California (MTD at 17-18) is not dispositive. *Dole*, 303 F.3d at 1115. NSO ignores its U.S. ties,[12] and that "the Supreme Court has preferred nonjurisdictional methods of lessening the inconvenience faced by defendants." *Sinatra v. Nat'l Enquirer, Inc.*, 854 F.2d 1191, 1199 (9th Cir. 1988) (citing, *inter alia*, *Burger King*, 471 U.S. at 477-78). Plaintiffs would be burdened if forced to litigate in Israel, when their witnesses and evidence are concentrated in California. And it is most efficient to litigate in California, given that California is both the place where Plaintiffs' injury occurred and the forum whose law will be applied. *Raffaele v. Compagnie Generale Mar.*, 707 F.2d 395, 399 (9th Cir. 1983).

[12] NSO fails to acknowledge that it owns a U.S.-based marketing and sales arm that engaged in lengthy sales discussions with the U.S. Drug Enforcement Administration, Compl. ¶ 5, Exs. 2, 3; that its co-founder, who is a member of its board, lives in the United States, ECF No. 20-3 ¶ 14, Ex. 12; and that it was funded by a San Francisco-based equity firm until February 2019, Comp. ¶ 5 & Ex. 4.

Third, NSO asserts that exercising jurisdiction over it would "conflict[] with Israel's sovereignty" due to NSO's claimed lack of California operations. *See* MTD at 17. But NSO is neither a sovereign nor immune from the Court's exercise of jurisdiction. Nor is NSO's nationality dispositive: "if given controlling weight, it would always prevent suit against a foreign national in a United States court." *See Sinatra*, 854 F.2d at 1199 (discounting defendant's attempt to invoke this factor where defendant had benefited from engagement with the U.S. market).

Fourth, NSO does not seriously dispute California's and Plaintiffs' interests in a California-based resolution of Plaintiffs' claims. *See* MTD at 17-18. California has a "strong interest" in providing residents with "effective means of redress." *Sinatra*, 854 F.2d at 1200. And Plaintiffs' claims are concededly governed by federal and California law. Compl. ¶¶ 49-78; MTD at 20-25. A California-based court is better positioned to apply these laws than an Israeli court.

Finally, NSO is incorrect (MTD at 18) that Plaintiffs bear the burden to show that Israel is inadequate as an alternative forum. *See, e.g.*, *Ballard*, 65 F.3d at 1502 (construing factor against defendant who "present[ed] absolutely no evidence on this issue, erroneously assuming that the burden [was] on [plaintiff]" to show no alternate forum). NSO has offered no evidence on this point, arguing only that Plaintiffs were sued by NSO's employees in Israel. *See* MTD at 18. NSO does not explain how this makes Israel an adequate forum to litigate Plaintiffs' U.S.-law based claims. And of course, NSO does not (and cannot) assert that California is an inadequate forum to hear Plaintiffs' claims.

Thus, the balance of the reasonableness factors favors Plaintiffs. And since Plaintiffs have satisfied each prong of the analysis, the Court has specific jurisdiction over NSO.

3. This Court has jurisdiction under Rule 4(k)(2).

Even if specific jurisdiction were lacking, NSO would still be subject to personal jurisdiction under Federal Rule of Civil Procedure 4(k)(2) because (1) Plaintiffs' CFAA claim arises under federal law; (2) NSO would not be subject to jurisdiction in any state; and (3) exercising jurisdiction comports with due process. *See Hydentra HLP Int'l v. Sagan Ltd.*, 783 F. App'x 663, 665 (9th Cir. 2019).

Here, Plaintiffs assert claims under federal law. And NSO, in resisting jurisdiction in California, has not "alleged that it is subject to the courts of general jurisdiction in any state." *Holland Am. Line Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 461 (9th Cir. 2007) (a court may exercise

jurisdiction over Rule 4(k)(2) if "the defendant contends that [it] cannot be sued in the forum state and refuses to identify any other where suit is possible") (citation omitted). Indeed, the logic of NSO's argument is that *no* state would have personal jurisdiction if California does not. *See* MTD at 17-18.

Critically, NSO's contacts with the U.S. make it fair for NSO to litigate here. *See Axiom*, 874 F.3d at 1072 (Rule 4(k)(2) analysis "is nearly identical to traditional personal jurisdiction analysis"); *Hydentra*, 783 F. App'x at 665 (applying specific jurisdiction analysis to hold that Rule 4(k)(2) was met). NSO's contacts with the United States were substantial, intentional, and essential to the success of the violations that the Complaint alleges.

Numerous facts support that conclusion. NSO extensively used U.S.-based computer servers in the challenged attacks. *See* Compl. ¶ 34; *see also* Gheorghe Decl. ¶¶ 3-5; Mornin Decl. ¶¶ 2-6, Exs. 1-9; *Micron Tech., Inc. v. United Microelectronics Corp.*, 2019 WL 1959487, at *3 (N.D. Cal. May 2, 2019) (finding Rule 4(k)(2) jurisdiction where defendant used U.S.-based servers). NSO "knowingly and with intent to defraud" accessed Plaintiffs' computers and infrastructure in the United States to distribute its malware. *See* Compl. ¶ 54; *see generally Facebook*, 2007 WL 2326090 at *2, *5-6. NSO exploited U.S. financial and commercial markets by relying on a subsidiary marketing arm based and incorporated in the United States and by financing its product via U.S. backers. *See* Compl. ¶ 5, Exs. 2, 3. One of NSO's board members lives in the United States. ECF No. 20-3 ¶ 14, Ex. 12. And NSO's conduct foreseeably caused harm in the United States: WhatsApp, a U.S. company, expended significant engineering resources in the United States to investigate and remediate the attack, including updating the WhatsApp app so that approximately 56.6 million users could download an update to protect the app from NSO's attack. Gheorge Decl. ¶ 2; Nguyen Decl. ¶ 3; Compl. ¶ 44. The totality of NSO's U.S.-directed conduct establishes that, "but for [its] forum-related conduct, the injury would not have occurred." *Craigslist*, 694 F. Supp. 2d at 1053 (citation omitted).

Lastly, NSO has made *no* showing (let alone a compelling one) that requiring it to litigate in the U.S. is unfair. *See* Section III.C.2.d. Thus, personal jurisdiction is appropriate under Rule 4(k)(2).

4. This Court should exercise pendent jurisdiction.

If the Court finds jurisdiction over some, but not all, of Plaintiffs' claims, it should exercise pendent jurisdiction over the remaining claims, which arise "out of a common nucleus of operative

facts." *See Action Embroidery Corp. v. Atl. Embroidery, Inc.*, 368 F.3d 1174, 1180 (9th Cir. 2004). Because NSO's unauthorized use of WhatsApp's computer infrastructure to send malicious code to WhatsApp users in violation of WhatsApp's Terms underpins each of Plaintiffs' claims, this Court should exercise pendent jurisdiction over the remaining claims. *See, e.g.*, Compl. ¶¶ 49-78; *CE Distribution, LLC v. New Sensor Corp.*, 380 F.3d 1107, 1113 (9th Cir. 2004) (exercising pendent jurisdiction over contract claims where personal jurisdiction existed for related tort claims).[13]

D. The Complaint Validly Alleges Violations Of Federal And State Law.

1. Plaintiffs state a claim for a violation of the CFAA.

The Complaint alleges that NSO violated Sections 1030(a)(2), (a)(4), and (b) of the CFAA because it accessed and conspired to access, without authorization, Plaintiffs' servers and WhatsApp users' devices. Compl. ¶¶ 49-57. As detailed below, NSO circumvented WhatsApp technical restrictions in order to access and use the servers, which constitutes unauthorized access under the CFAA. *Id.* ¶¶ 32, 35-39. Because NSO's actions caused Plaintiffs to incur a loss as defined by Section 1030(e)(11), the CFAA authorizes Plaintiffs to pursue civil remedies. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2003) ("The civil remedy extends to '[*a*]*ny person* who suffers damage or loss by reason of a violation of this section.'") (quoting 18 U.S.C. 1030(g)).

a. NSO lacked authorization to access the servers and devices.

NSO does not dispute that its conduct resulted in unauthorized access to victims' devices in violation of the CFAA. Compl. ¶¶ 53–54. In addition, NSO lacked authorization to access Plaintiffs' servers, through which it carried out its malicious hacking activity. NSO argues it is immune from liability under the CFAA because the WhatsApp Terms of Service "authorized" its conduct. MTD at 20-21. But NSO mischaracterizes its conduct and the nature of its unauthorized access.

[13] If this Court is not prepared to exercise jurisdiction, Plaintiffs request jurisdictional discovery before the MTD is resolved. *See Gillespie v. Prestige Royal Liquors Corp.*, 183 F. Supp. 3d 996, 1003 (N.D. Cal. 2016) (broad discretion to permit jurisdictional discovery); *Mitan v. Feeney*, 497 F. Supp. 2d 1113, 1119 (C.D. Cal. 2007) ("some evidence" tending to show personal jurisdiction suffices). Here, Plaintiffs have indisputably proffered evidence tending to show personal jurisdiction. While Plaintiffs respectfully submit that their jurisdictional showing is adequate, if this Court disagrees, further discovery would allow Plaintiffs to present additional evidence bearing on, *e.g.*: Defendants' communications showing they knowingly exploited California-based technology from WhatsApp; evidence that Defendants used funding from California entities to develop Pegasus; and evidence that Defendants used California-based computer systems, including QuadraNet servers, in their attacks.

More specifically, and as alleged in the Complaint (Compl. ¶¶ 32-42): *First*, NSO reverse-engineered the WhatsApp app to create an unauthorized program designed to evade technical restrictions on the access and use of the WhatsApp service. *Second*, using its own program (as opposed to the legitimate WhatsApp app) NSO gained unauthorized access to WhatsApp servers. *Third*, NSO circumvented security measures built into WhatsApp's servers by formatting messages to conceal malicious code and appear like legitimate calls. *Fourth*, NSO further used WhatsApp servers to gain unauthorized access to users' devices. In short, Plaintiffs' CFAA claims are not based on a terms-of-service violation but on NSO's conduct in circumventing Plaintiffs' technological restrictions.

Under the CFAA, whether access is "authorized" depends on actions by the computer owner to grant or deny permission to the system. *United States v. Nosal*, 844 F.3d 1024, 1035–36 (9th Cir. 2016) (*Nosal II*) (observing that all circuits agree on this definition); *see also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133, 1135 (9th Cir. 2009). Courts have "typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user." *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007). Relevant considerations include whether the defendant engaged in "technological gamesmanship" to "aid in access," *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016), and "whether the conduct at issue is analogous to 'breaking and entering,'" *hiQ Labs Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1001 (9th Cir. 2019) (citation omitted).

For example, in *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), the court concluded that a defendant who "exploit[ed] [a] security defect[]" to transmit a virus infecting other computers on his network gained "unauthorized access" to those computers because his use of email and network programs was not "in any way related to their intended function" and instead exploited "holes in both programs that permitted him a special and unauthorized access route into other computers." *Id.* at 505, 510; *see Nosal II*, 844 F.3d at 1037 (citing *Morris* with approval). And in *Phillips*, the court concluded that a user's "'brute-force attack' program" that provided "a 'back door' into [his university's] main server" was "not an intended use" of the network "within the understanding of any reasonable computer user and constitute[d] a method of obtaining unauthorized access to computerized data that he was not permitted to view or use." 477 F.3d at 218, 220.

So too here, NSO gained unauthorized access to WhatsApp's servers by reverse-engineering the app and using that program to evade WhatsApp security features that prevent access to and manipulation of technical call settings. *See United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (*Nosal I*) (observing that the "general purpose" of the CFAA "is to punish hacking—the circumvention of technological access barriers"). WhatsApp has never granted any user permission to access server-side call settings and alter the technical architecture routing calls through its servers. Instead, it employs security measures to protect its servers from abuse and prevent attacks on users. NSO built sophisticated software to circumvent those security measures, engaging in "technological gamesmanship" to access and alter network protocols to transmit malicious code to victims and hack into their devices. *Power Ventures, Inc.*, 844 F.3d at 1067. This abuse lies at the core of the hacking activity the CFAA prohibits. *See, e.g.*, H.R. Rep. 98-894 at 10 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3694–95 (CFAA addresses concern about serious harm caused by "'hackers' who have been able to access (trespass into) both private and public computer systems."). Plaintiffs thus sufficiently allege that NSO accessed protected computers without authorization in violation of the CFAA.

In arguing that this abuse was "authorized," NSO observes that it signed up for WhatsApp accounts and so obtained a license to use WhatsApp's services. MTD at 21. But users are licensed to access WhatsApp services only through the WhatsApp app, which has integrated security measures preventing users from accessing server-side call settings. Compl. ¶ 17; *see also id.* ¶¶ 19–23 (WhatsApp Terms of Service prohibit users from gaining "unauthorized access to [WhatsApp's] Services or systems" and "exploiting [WhatsApp's] Services in impermissible or unauthorized manners"). NSO bypassed those restrictions by using its own program to gain unauthorized entry to the servers and manipulate settings not accessible to any user. NSO did not use WhatsApp's servers "in any way related to their intended function" but instead built sophisticated software that provided "a special and unauthorized access route into other computers." *Morris*, 928 F.2d at 510.

Untenable consequences would flow from accepting NSO's argument that creating an account for a service extinguishes CFAA liability even when the user gains unauthorized access through other means. For example, websites like the New York Times authorize users to sign up for accounts and access servers when reading and commenting on articles. But such access surely would not permit a

user to hack into the New York Times's servers, manipulate normally inaccessible settings, and gain control of other readers' comments. NSO's claim that its access was authorized merely because it created a WhatsApp account would sharply circumscribe the CFAA's scope and has no statutory basis.

NSO's reliance on *Brekka*—the only case it cites to support its "authorization" argument—is misplaced. In *Brekka*, an employee who indisputably had been granted access to his work computer and company materials was alleged to have violated the CFAA by accessing those materials for an improper purpose. 581 F.3d at 1129–30. The Ninth Circuit held that "when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations." *Id.* at 1133. Here, unauthorized access occurred not because WhatsApp messages were sent for an improper purpose but because NSO accessed the servers using its own program, evaded technical restrictions, and then commandeered the network infrastructure to deliver malware to victims.[14] The analysis in *Brekka*—which involved a classic employer-employee dispute and implicated concerns about transforming "arguably innocuous conduct" into federal crimes, *Nosal II*, 844 F.3d at 1038—has never been and should not be applied to malicious hacking activity like NSO's conduct here.[15]

b. NSO's conduct harmed Plaintiffs.

The CFAA provides a private right of action to "[a]ny person who suffers damage or loss by reason of a violation . . . ." 18 U.S.C. § 1030(g), *see also Theofel*, 359 F.3d at 1078. The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its

[14] A pending Supreme Court case raises the question whether an employee who is authorized to view information on a computer for particular purposes violates the CFAA by accessing that information for an improper purpose. *Van Buren v. United States*, No. 19-783 (U.S.). The resolution of that issue will not affect Plaintiffs' CFAA claim because NSO had no authorization to access Plaintiffs' servers through a reverse-engineered program or manipulate server-side settings for *any* purpose.

[15] Even if NSO's creation of WhatsApp accounts sufficed to authorize access to WhatsApp's servers, NSO exceeded any such authorized access by using an illicit, reverse-engineered program to evade security restrictions and gain access to call settings that users are not permitted to view or alter. *Nosal I*, 676 F.3d at 858 (CFAA's prohibition on "exceed[ing] authorized access" applies to "individuals whose initial access to a computer is authorized but who access unauthorized information or files"). If the Court determines that unauthorized access did not occur, Plaintiffs request leave to amend their CFAA claim to allege that NSO exceeded authorized access.

condition prior to the offense." 18 U.S.C. § 1030(e)(11). NSO does not (and cannot) dispute that the Complaint adequately alleges loss based on the costs associated with investigating and remediating NSO's unauthorized access to WhatsApp's servers. Compl. ¶¶ 44, 57. On that basis alone, Plaintiffs' CFAA claim should proceed. *See Flextronics Int'l, Ltd. v. Parametric Tech. Corp*., 2014 WL 2213910, at *3 (N.D. Cal. May 28, 2014) (denying motion to dismiss where plaintiff alleged costs related to investigating and remediating defendant's conduct).

In addition, contrary to NSO's contentions (MTD at 22), the Complaint further alleges loss based on NSO's unauthorized access to users' devices. The Ninth Circuit has held that plaintiffs can be injured under the CFAA by a defendant's access to a third party's device, specifically rejecting any requirement of control or ownership of the device. *Theofel*, 359 F.3d at 1072, 1078. Here, under WhatsApp's Terms of Service, WhatsApp owns "all intellectual property rights" associated with the WhatsApp app and grants users a license "to use" the service when they download the app on their devices. *See id.* ¶ 19 (incorporating terms of service). And the Complaint alleges that NSO accessed WhatsApp computers without authorization to further their unauthorized access of Target Devices. *Id.* ¶¶ 53-54. NSO's conduct impaired the integrity and security of the WhatsApp app on those devices and caused a loss to Plaintiffs within the meaning of Section 1030(e)(11), which included responding to the offense and conducting a damage assessment. *Multiven, Inc. v. Cisco Sys., Inc*., 725 F. Supp. 2d 887, 894–95 (N.D.Cal.2010) ("Costs associated with investigating intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the statute.").

Indeed, to prevent NSO's further unauthorized access to users' devices, Plaintiffs needed to update the WhatsApp app. Compl. ¶¶ 44-45; Gheorge Decl. ¶ 2. Costs incurred when "upgrading a system's defenses to prevent future unauthorized access" constitute a cognizable "loss" under the CFAA. *Ticketmaster L.L.C. v. Prestige Entm't W., Inc*., 315 F. Supp. 3d 1147, 1174 (C.D. Cal. 2018); *Kimberlite Corp. v. John Does 1–20*, 2008 WL 2264485, at *2 (N.D. Cal. June 2, 2008) (plaintiff "set forth a CFAA violation "where it alleged costs associated with "securing" its email system). Thus, the Complaint additionally pleads a valid CFAA claim based on NSO's access to users' devices.

c. Plaintiffs' conspiracy claim is sufficient.

Because Plaintiffs have stated claims for violations of 18 U.S.C. § 1030(a)(2) and (a)(4), the Complaint states a conspiracy claim under § 1030(b) as well (as NSO seems to concede, MTD at 23).

2. Plaintiffs state a claim for trespass to chattels.

a. NSO interfered with the intended operation of Plaintiffs' servers and app.

To state a claim for trespass to chattels, a complaint must allege "some injury to the chattel or to the plaintiff's rights in it," such as impairment of the property's "condition, quality, or value." *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1350, 1357 (2003). In the cyber context, such injury occurs if the defendant interfered with the "intended functioning of the system." *Id.* at 1356.

Here, NSO interfered with the intended functioning of Plaintiffs' servers and the WhatsApp app. Compl. ¶ 46. Plaintiffs' servers are programmed to route encrypted communications between users using established network protocols. *Id.* ¶¶ 17-18. NSO's use of Plaintiffs' servers to covertly transmit malware and fraudulently emulate network protocols plainly interfered with the intended functioning and integrity of the WhatsApp computer system. Compl. ¶¶ 17, 35. Indeed, NSO designed its malware to conceal that it was evading WhatsApp's technical restrictions and interfering with the WhatsApp service by making it appear as if the malicious code originated from WhatsApp's servers and not from NSO. Compl. ¶¶ 32, 36-37. Because the value of Plaintiffs' servers and app derives from their ability to securely and accurately transmit communications between users, NSO's actions impaired the quality and value of Plaintiffs' system. *See CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1022 (S.D. Ohio 1997) (holding that computer system's value was "wholly derived from the extent to which that equipment can serve its subscriber base.").[16]

[16] Courts routinely find cognizable injury to support a trespass-to-chattels claim when the defendant impaired the ability of a plaintiff's equipment to serve customers as intended. *See, e.g.*, *Coupons, Inc. v. Stottlemire*, 2008 WL 3245006, at *6 (N.D. Cal. July 2, 2008) (defendant circumvented server's technical restriction and impaired plaintiff's ability to provide coupons to other customers); *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 980 (N.D. Cal. 2013) (unauthorized access reduced website's "capacity to service its users"); *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1564, 1566 (1996) (hacking of network denied "some subscribers access"); *Jedson Eng'g, Inc. v. Spirit Const. Servs., Inc.*, 720 F. Supp. 2d 904, 926 (S.D. Ohio 2010) (unauthorized access harmed value of "servers as a safe, secure location for project files"); *Skapinetz v. CoesterVMS.com, Inc*, 2019 WL 2579120, at *5 (D. Md. June 24, 2019) (defendant "damaged the value of [plaintiff's] accounts by breaching the security and privacy" of email accounts).

NSO misses the point in focusing on whether the transmission of its messages embedded with malicious code burdened Plaintiffs' services as a quantitative matter. MTD at 24-25 (citing cases in which plaintiffs failed to explain how defendant's use of system interfered with system's operation). The Complaint alleged cognizable harm based not on the *number* of messages sent, but on *the effect* of those transmissions in impairing the integrity, quality, and value of WhatsApp's services. That suffices to allege cognizable injury for a trespass-to-chattels claim. *See Hamidi*, 30 Cal. 4th at 1353.

b. Plaintiffs' loss of goodwill and remediation expenditures are cognizable.

Contrary to NSO's contention, *Hamidi* does not categorically foreclose the loss of goodwill and remediation expenditures as cognizable harms. 30 Cal. 4th at 1357–58. Rather, *Hamidi* acknowledged that courts have found such losses actionable where the harm has a sufficient "connection" to the property at issue, such as when the loss of goodwill stems from the "functioning of the company's [computer system]." *Id*. at 1358 (describing loss of reputation and goodwill in *CompuServe*, 962 F. Supp. at 1023).

Here, Plaintiffs' loss of goodwill resulted directly from NSO's interference with the proper functioning and integrity of the WhatsApp system. *See CompuServe*, 962 F. Supp. at 1023; *Microsoft Corp. v. Does 1–18*, 2014 WL 1338677, at *10 (E.D. Va. Apr. 2, 2014) (defendants' manipulation of Microsoft's search engines caused injury to goodwill). Moreover, Plaintiffs had to expend resources to combat and remediate the attacks. *Twitch Interactive, Inc. v. Does 1 Through 100*, 2019 WL 3718582, at *4 (N.D. Cal. Aug. 7, 2019) (harm where plaintiff "expend[ed] resources to combat [defendant's] attack"); *Hotmail Corp. v. Van$ Money Pie Inc.*, 1998 WL 388389, at *7 (N.D. Cal. Apr. 16, 1998) (harm from "added costs for personnel to sort through and respond to the misdirected emails"); *Summit Entm't, LLC v. Santia*, 2014 WL 12577430, at *5 (C.D. Cal. June 24, 2014) (harm from "expend[ing] time and resources investigating and stopping a breach in the servers' security"). NSO's attack on the trespass-to-chattels claim accordingly lacks merit.

IV. CONCLUSION

Plaintiffs respectfully request that the Court deny NSO's motion to dismiss.

Dated: April 23, 2020

Respectfully submitted,

COOLEY LLP

/s/ Travis LeBlanc
Travis LeBlanc

Michael G. Rhodes
Daniel J. Grooms
Elizabeth B. Prelogar
Bethany C. Lobo
Kyle C. Wong
Joseph D. Mornin
COOLEY LLP

Michael R. Dreeben
O'MELVENY & MYERS LLP

Attorneys for Plaintiffs
WHATSAPP INC. and FACEBOOK, INC.