

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC., et al.,
Plaintiffs,
v.
NSO GROUP TECHNOLOGIES
LIMITED, et al.,
Defendants.

Case No. 19-cv-07123-PJH

**ORDER GRANTING IN PART AND
DENYING IN PART MOTION TO
DISMISS AND DENYING MOTION TO
STAY DISCOVERY**

Re: Dkt. Nos. 45, 95

Before the court is defendants NSO Group Technologies, Ltd. (“NSO”) and Q Cyber Technologies Ltd.’s (“Q Cyber,” and together with NSO, “defendants”) motion to dismiss. The matter is fully briefed and suitable for decision without oral argument. Having read the parties’ papers and carefully considered their arguments and the relevant legal authority, and good cause appearing, the court rules as follows.

BACKGROUND

On October 29, 2019, plaintiffs WhatsApp Inc. (“WhatsApp”) and Facebook, Inc. (“Facebook” and together with WhatsApp, “plaintiffs”) filed a complaint (“Compl.”) alleging that defendants sent malware, using WhatsApp’s system, to approximately 1,400 mobile phones and devices designed to infect those devices for the purpose of surveilling the users of those phones and devices. Dkt. 1, ¶ 1. The complaint alleges four causes of action: (1) violation of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030; (2) violation of the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502; (3) breach of contract; and (4) trespass to chattels.

Plaintiff WhatsApp is a Delaware corporation with its principal place of business in

1 Menlo Park, California and is owned by plaintiff Facebook, which is also a Delaware
 2 corporation with its principal place of business in Menlo Park, California. Compl. ¶¶ 3–4.
 3 WhatsApp provides an encrypted communication service that is accessed through the
 4 WhatsApp application (“app”) that users must download to their personal devices. Id.
 5 ¶ 17. Defendant NSO is an Israeli limited liability company and defendant Q Cyber is an
 6 Israeli corporation and NSO’s only active director and the majority shareholder. Id. ¶¶ 5–
 7 6. Defendants are alleged to manufacture, distribute, and operate surveillance
 8 technology “designed to intercept and extract information and communications from
 9 mobile phones and devices” Id. ¶ 24.

10 In order to use the WhatsApp app and service, WhatsApp users consent to
 11 WhatsApp’s terms of service in which they agree to “use [WhatsApp’s] Services
 12 according to [WhatsApp’s] Terms and policies” and further agree to “access and use
 13 [WhatsApp’s] Services only for legal, authorized, and acceptable purposes.” Id. ¶¶ 19–
 14 20. WhatsApp’s terms prohibit users from using services in ways that “violate,
 15 misappropriate, or infringe the rights of WhatsApp, [its] users, or others,” “are illegal,
 16 intimidating, harassing, . . . or instigate or encourage conduct that would be illegal, or
 17 otherwise inappropriate;” or “involve sending illegal or impermissible communications.”
 18 Id. ¶ 21. Additionally, users are not permitted to:

19 (a) reverse engineer, alter, modify, create derivative works
 20 from, decompile, or extract code from our Services, (b) send,
 21 store, or transmit viruses or other harmful computer code
 22 through or onto our Services; (c) gain or attempt to gain
 23 unauthorized access to our Services or systems; (d) interfere
 with or disrupt the safety, security, or performance of our
 Services; [or] . . . (f) collect the information of or about our users
 in any impermissible or unauthorized manner.

24 Id. ¶ 22.

25 Plaintiffs allege that defendants created a data program, termed Pegasus, that
 26 could “remotely and covertly extract valuable intelligence from virtually any mobile
 27 device.” Id. ¶ 27. Defendants licensed Pegasus and sold support services to customers.
 28 Id. ¶ 29. According to public reporting and as alleged, defendants’ customers include

1 sovereign nations such as the Kingdom of Bahrain, the United Arab Emirates, and
2 Mexico. Id. ¶ 43. Defendants could customize Pegasus for different purposes such that,
3 once installed on a user's device, they could intercept communications, capture
4 screenshots, or exfiltrate browser history and contacts from that user's device. Id. ¶¶ 27,
5 41. Defendants used a network of computers to monitor and update the version of
6 Pegasus implanted on a user's phone as well as control the number of devices that a
7 customer could compromise using Pegasus. Id. ¶ 28.

8 Between January 2018 and May 2019, defendants are alleged to have created
9 WhatsApp accounts that could be used to send malicious code to personal devices in
10 April and May 2019. Id. ¶ 33. Defendants also leased servers and internet hosting
11 services from third parties such as Choopa, QuadraNet, and Amazon Web Service; the
12 leased servers were used to distribute malware and relay commands to users' devices.
13 Id. ¶ 34. Defendants reverse engineered the WhatsApp app and developed Pegasus to
14 emulate legitimate WhatsApp network traffic. Id. ¶ 35.

15 Pegasus is alleged to operate by first routing malicious code through WhatsApp's
16 relay servers to a user's device. Id. ¶ 36. Defendants formatted certain messages
17 containing the malicious code to appear like a legitimate call and concealed the code
18 within the call settings. Id. ¶ 37. To avoid technical restrictions built into the WhatsApp
19 signaling servers, defendants formatted call initiation messages that contained the
20 malicious code to appear as a legitimate call. Id. The call would inject the malicious
21 code into a device's memory whether or not the user answered the call. Id. After the
22 malicious code was delivered to a device, defendants caused encrypted data packets to
23 be sent to a user's device via WhatsApp's relay servers, designed to activate the
24 malicious code residing on the memory of the target devices. Id. ¶ 39. Once activated,
25 the malicious code caused the target device to connect to one of the leased, remote
26 servers hosting defendants' malware, which was then downloaded and installed on the
27 target devices. Id. ¶ 40. The malware would then give defendants and their customers
28 access to information on the target devices. Id. ¶ 41.

1 jurisdiction is raised . . . the court may inquire by affidavits or otherwise, into the facts as
 2 they exist.”). “Once the moving party has converted the motion to dismiss into a factual
 3 motion by presenting affidavits or other evidence properly brought before the court, the
 4 party opposing the motion must furnish affidavits or other evidence necessary to satisfy
 5 its burden of establishing subject matter jurisdiction.” Safe Air for Everyone, 373 F.3d at
 6 1039.

7 **2. Rule 12(b)(2)**

8 A federal court may dismiss an action under Federal Rule of Civil Procedure
 9 12(b)(2) for lack of personal jurisdiction. When resolving a motion to dismiss under Rule
 10 12(b)(2) on written materials, the court accepts uncontroverted facts in the complaint as
 11 true and resolves conflicts in affidavits in the plaintiffs’ favor. Mavrix Photo, Inc. v. Brand
 12 Techs., Inc., 647 F.3d 1218, 1223 (9th Cir. 2011). The party seeking to invoke a federal
 13 court’s jurisdiction bears the burden of demonstrating jurisdiction. Picot v. Weston, 780
 14 F.3d 1206, 1211 (9th Cir. 2015). “Federal courts ordinarily follow state law in determining
 15 the bounds of their jurisdiction over persons.” Daimler AG v. Bauman, 571 U.S. 117, 125
 16 (2014); see Fed. R. Civ. P. 4(k)(1)(a). California’s long arm statute permits exercise of
 17 personal jurisdiction to the fullest extent permissible under the U.S. Constitution,
 18 therefore, the court’s inquiry “centers on whether exercising jurisdiction comports with
 19 due process.” Picot, 780 F.3d at 1211; see Cal. Code Civ. P. § 410.10.

20 The Due Process Clause of the Fourteenth Amendment “limits the power of a
 21 state’s courts to exercise jurisdiction over defendants who do not consent to jurisdiction.”
 22 Martinez v. Aero Caribbean, 764 F.3d 1062, 1066 (9th Cir. 2014). Due process requires
 23 that the defendant “have certain minimum contacts with it such that the maintenance of
 24 the suit does not offend traditional notions of fair play and substantial justice.” Int’l Shoe
 25 Co. v. Washington, 326 U.S. 310, 316 (1945) (internal quotation marks omitted). Under
 26 the “minimum contacts” analysis, a court can exercise either “general or all-purpose
 27 jurisdiction,” or “specific or conduct-linked jurisdiction.” Daimler, 571 U.S. at 121–22
 28 (citing Goodyear Dunlop Tires Operations, S.A. v. Brown, 564 U.S. 915, 919 (2011)).

1 A court may exercise specific jurisdiction over a defendant if its less-substantial
2 contacts with the forum give rise to the claim or claims pending before the court—that is,
3 if the cause of action “arises out of” or has a substantial connection with that activity.

4 Hanson v. Denckla, 357 U.S. 235, 250–53 (1958); see also Goodyear, 564 U.S. at 924–
5 25. The inquiry into whether a forum state may assert specific jurisdiction over a
6 nonresident defendant focuses on the relationship among the defendant, the forum, and
7 the litigation. Walden v. Fiore, 571 U.S. 277, 283–84 (2014) (citation omitted).

8 To determine whether a defendant’s contacts with the forum state are sufficient to
9 establish specific jurisdiction, the Ninth Circuit employs a three-part test:

- 10 (1) The non-resident defendant must purposefully direct his
11 activities or consummate some transaction with the forum or
12 resident thereof; or perform some act by which he purposefully
13 avails himself of the privilege of conducting activities in the
14 forum, thereby invoking the benefits and protections of its laws;
15 (2) the claim must be one which arises out of or relates to the
16 defendant’s forum-related activities; and
17 (3) the exercise of jurisdiction must comport with fair play and
18 substantial justice, i.e. it must be reasonable.

19 Morrill v. Scott Fin. Corp., 873 F.3d 1136, 1142 (9th Cir. 2017). A plaintiff bears the
20 burden of satisfying the first two prongs. Id. If the plaintiff does so, then the burden shifts
21 to the defendant to “set forth a ‘compelling case’ that the exercise of jurisdiction would not
22 be reasonable.” CollegeSource, Inc. v. AcademyOne, Inc., 653 F.3d 1066, 1076 (9th Cir.
23 2011) (quoting Burger King Corp. v. Rudzewicz, 471 U.S. 462, 477–78 (1985)).

24 **3. Rule 12(b)(6)**

25 A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) tests for the
26 legal sufficiency of the claims alleged in the complaint. Ileto v. Glock Inc., 349 F.3d 1191,
27 1199–1200 (9th Cir. 2003). Under Federal Rule of Civil Procedure 8, which requires that
28 a complaint include a “short and plain statement of the claim showing that the pleader is
entitled to relief,” Fed. R. Civ. P. 8(a)(2), a complaint may be dismissed under Rule
12(b)(6) if the plaintiff fails to state a cognizable legal theory, or has not alleged sufficient
facts to support a cognizable legal theory. Somers v. Apple, Inc., 729 F.3d 953, 959 (9th
Cir. 2013).

1 While the court is to accept as true all the factual allegations in the complaint,
2 legally conclusory statements, not supported by actual factual allegations, need not be
3 accepted. Ashcroft v. Iqbal, 556 U.S. 662, 678–79 (2009). The complaint must proffer
4 sufficient facts to state a claim for relief that is plausible on its face. Bell Atl. Corp. v.
5 Twombly, 550 U.S. 544, 555, 558–59 (2007).

6 “A claim has facial plausibility when the plaintiff pleads factual content that allows
7 the court to draw the reasonable inference that the defendant is liable for the misconduct
8 alleged.” Iqbal, 556 U.S. at 678. “[W]here the well-pleaded facts do not permit the court
9 to infer more than the mere possibility of misconduct, the complaint has alleged—but it
10 has not ‘show[n]’—‘that the pleader is entitled to relief.’” Id. at 679 (quoting Fed. R. Civ.
11 P. 8(a)(2)). Where dismissal is warranted, it is generally without prejudice, unless it is
12 clear the complaint cannot be saved by any amendment. In re Daou Sys., Inc., 411 F.3d
13 1006, 1013 (9th Cir. 2005).

14 Review is generally limited to the contents of the complaint, although the court can
15 also consider documents “whose contents are alleged in a complaint and whose
16 authenticity no party questions, but which are not physically attached to the plaintiff’s
17 pleading.” Knievel v. ESPN, 393 F.3d 1068, 1076 (9th Cir. 2005) (quoting In re Silicon
18 Graphics Inc. Sec. Litig., 183 F.3d 970, 986 (9th Cir. 1999), superseded by statute on
19 other grounds as stated in In re Quality Sys., Inc. Sec. Litig., 865 F.3d 1130 (9th Cir.
20 2017)); see also Sanders v. Brown, 504 F.3d 903, 910 (9th Cir. 2007) (“[A] court can
21 consider a document on which the complaint relies if the document is central to the
22 plaintiff’s claim, and no party questions the authenticity of the document.” (citation
23 omitted)). The court may also consider matters that are properly the subject of judicial
24 notice (Lee v. City of Los Angeles, 250 F.3d 668, 688–89 (9th Cir. 2001)), and exhibits
25 attached to the complaint (Hal Roach Studios, Inc. v. Richard Feiner & Co., Inc., 896 F.2d
26 1542, 1555 n.19 (9th Cir. 1989)).

27 **4. Rule 12(b)(7)**

28 Federal Rule of Civil Procedure 12(b)(7) permits a party to move for dismissal for

1 failure to join a party recognized as indispensable by Federal Rule of Civil Procedure 19.
2 Fed. R. Civ. P. 12(b)(7); Quileute Indian Tribe v. Babbitt, 18 F.3d 1459, 1458 (9th Cir.
3 1994). Federal Rule of Civil Procedure 19 “governs compulsory party joinder in federal
4 district courts.” E.E.O.C. v. Peabody W. Coal Co. (“Peabody I”), 400 F.3d 774, 778 (9th
5 Cir. 2005). When determining whether dismissal is appropriate under Rule 12(b)(7), the
6 court undertakes “three successive inquiries.” Id. at 779.

7 “First, the court must determine whether a nonparty should be joined under Rule
8 19(a)—that is, whether a nonparty is “necessary.” Id. A nonparty is “necessary” if
9 joinder is “‘desirable’ in the interests of just adjudication.” Id. (quoting Fed. R. Civ. P. 19
10 Advisory Committee Note (1966)). “There is no precise formula for determining whether
11 a particular nonparty should be joined under Rule 19(a). . . . The determination is heavily
12 influenced by the facts and circumstances of each case.” E.E.O.C. v. Peabody W. Coal
13 Co. (“Peabody II”), 610 F.3d 1070, 1081 (9th Cir. 2010) (quoting N. Alaska Envtl. Ctr. v.
14 Hodel, 803 F.2d 466, 468 (9th Cir. 1986)).

15 A nonparty can be necessary under Rule 19(a)(1)(A) or Rule 19(a)(1)(B). A
16 nonparty is necessary under Rule 19(a)(1)(A) if “in that person’s absence, the court
17 cannot accord complete relief among existing parties.” Fed. R. Civ. P. 19(a)(1)(A). A
18 nonparty is necessary under Rule 19(a)(1)(B) if that person “claims a legally protected
19 interest in the subject of the suit such that a decision in its absence will (1) impair or
20 impede its ability to protect that interest; or (2) expose [an existing party] to the risk of
21 multiple or inconsistent obligations by reason of that interest.” Dawavendewa v. Salt
22 River Project Agr. Imp. & Power Dist., 276 F.3d 1150, 1155 (9th Cir. 2002).

23 Second, if a nonparty is necessary, the court determines “whether it is feasible to
24 order that the absentee be joined.” Peabody I, 400 F.3d at 779. Joinder is not feasible
25 “when venue is improper, when the absentee is not subject to personal jurisdiction, and
26 when joinder would destroy subject matter jurisdiction.” Id. Third, if joinder is not
27 feasible, the court must determine whether the party is “indispensable” under Rule 19(b),
28 that is, whether “in equity and good conscience, the action should proceed among the

1 existing parties or should be dismissed.” Fed. R. Civ. P. 19(b). “The inquiry is a practical
 2 one and fact specific and is designed to avoid the harsh results of rigid application.”
 3 Makah Indian Tribe v. Verity, 910 F.2d 555, 558 (9th Cir. 1990) (citations omitted).

4 When considering a motion to dismiss under Rule 12(b)(7), the court accepts as
 5 true the allegations in the plaintiff’s complaint and draws all reasonable inferences in the
 6 plaintiff’s favor. Paiute-Shoshone Indians of Bishop Cmty. of Bishop Colony, Cal. v. City
 7 of Los Angeles, 637 F.3d 993, 996 n.1 (9th Cir. 2011). But the court may consider
 8 evidence outside of the pleadings. See McShan v. Sherrill, 283 F.2d 462, 464 (9th Cir.
 9 1960). “The moving party has the burden of persuasion in arguing for dismissal” for
 10 failure to join. Makah Indian Tribe, 910 F.2d at 558.

11 **B. Analysis**

12 **1. Subject Matter Jurisdiction**

13 As an initial observation, plaintiffs’ complaint pleads a cause of action under the
 14 Computer Fraud and Abuse Act, 18 U.S.C. § 1030, invoking the court’s federal question
 15 jurisdiction. See Gully v. First Nat’l Bank, 299 U.S. 109, 111 (1936). Defendants’ attack
 16 on the court’s subject matter jurisdiction is, therefore, not facial, but factual.

17 Defendants contend that the court lacks subject matter jurisdiction because the
 18 conduct giving rise to the complaint was performed by foreign sovereigns and the Foreign
 19 Sovereign Immunity Act (“FSIA”), 28 U.S.C. §§ 1602–11, bars any lawsuit on that basis.
 20 *Mtn.* at 8–9. Defendants also assert that the court should extend the doctrine of
 21 derivative sovereign immunity to them because defendants were contractors of the
 22 foreign sovereigns acting within the scope of their employment. *Id.* at 9–10.

23 The FSIA provides that “a foreign state shall be immune from the jurisdiction of the
 24 courts of the United States and of the States” except as provided in the FSIA. 28 U.S.C.
 25 § 1604. The parties agree that defendants, as private foreign entities, do not qualify as
 26 foreign states and cannot directly avail themselves of the FSIA. *Opp.* at 3; *Reply* at 9.
 27 More pertinent is whether defendants may avail themselves of some sort of derivative
 28 sovereign immunity. There are two relevant doctrines implicated by defendants’

1 argument: foreign official immunity and derivative sovereign immunity. The court
2 addresses each in turn.

3 **a. Foreign Official Immunity**

4 In Samantar v. Yousuf, 560 U.S. 305, 308 (2010), the Supreme Court addressed
5 whether the FSIA afforded a former Somali vice president and defense minister with
6 immunity from suit based on actions taken in his official capacity. While the Court
7 ultimately concluded that the FSIA did not extend to foreign officials, the Court separately
8 discussed the common law doctrine of foreign sovereign immunity, which potentially
9 applies to the acts of foreign officials not covered by the FSIA. See id. at 311 (citing
10 Schooner Exchange v. McFaddon, 7 Cranch 116, 3 L.Ed. 287 (1812)). Over time, courts
11 formulated a “two-step procedure developed for resolving a foreign state’s claim of
12 sovereign immunity.” Id. The first step involves requesting a “suggestion of immunity”
13 from the U.S. State Department. Id. If the State Department declines to issue the
14 suggestion, then a district court “ha[s] authority to decide for itself whether all the
15 requisites for immunity exist[.]” Id. (quoting Ex parte Peru, 318 U.S. 578, 587 (1943)).
16 At this second step, the court will grant immunity if “the ground of immunity is one which it
17 is the established policy of the [State Department] to recognize.” Id. at 312 (quoting
18 Republic of Mex. v. Hoffman, 324 U.S. 30, 36 (1945)).

19 At the second step of foreign official immunity, courts distinguish between status-
20 based immunity and conduct-based immunity. “Status-based immunity is reserved for
21 diplomats and heads of state and attaches ‘regardless of the substance of the claim.’”
22 Lewis v. Mutond, 918 F.3d 142, 145 (D.C. Cir. 2019) (quoting Chimène I. Keitner, The
23 Common Law of Foreign Official Immunity, 14 Green Bag 2d 61, 64 (2010)). “Conduct-
24 based immunity is afforded to “any [] [p]ublic minister, official, or agent of the state with
25 respect to acts performed in his official capacity if the effect of exercising jurisdiction
26 would be to enforce a rule of law against the state.” Id. (alterations in original) (quoting
27 Restatement (Second) of Foreign Relations Law § 66(f) (1965) (“Restatement”)); accord
28 Doğan v. Barak, 932 F.3d 888, 894 (9th Cir. 2019). While the Supreme Court “expressed

1 no view on whether Restatement § 66 correctly sets out the scope of common-law
 2 immunity applicable to current or former foreign officials,” Samantar 560 U.S. at 321 n.15,
 3 in Doğan v. Barak, 932 F.3d at 893–94, the Ninth Circuit cited with approval Restatement
 4 § 66 to determine conduct-based immunity. Restatement § 66 provides a three factor
 5 test for such immunity: “First, whether the actor is a public minister, official, or agent of
 6 the foreign state. Second, whether the acts were performed in her official capacity. And
 7 third, whether exercising jurisdiction would serve to enforce a rule of law against the
 8 foreign state.” Lewis, 918 F.3d at 146.

9 Here, defendants do not argue that the U.S. State Department has issued them a
 10 suggestion of immunity or that status-based immunity is available to them. Instead, they
 11 contend that conduct-based foreign sovereign immunity applies to a foreign sovereign’s
 12 private agents when the agent acts on behalf of the state and that this standard applies to
 13 their conduct on behalf of foreign sovereigns.¹ Reply at 10.

14 With respect to the first factor, plaintiffs do not contest that defendants are agents
 15 of foreign governments; indeed, the complaint alleges that defendants’ customers include
 16 the Kingdom of Bahrain, the United Arab Emirates, and Mexico. Compl. ¶ 43. With
 17 respect to the second factor, defendants argue that foreign states used defendants’
 18 technology to fight terrorism and serious crime, which are official public acts. Mtn. at 9
 19 n.9. Plaintiffs do not contend that defendants were acting outside the scope of their
 20 contracts with their customers, though they take issue with the idea that attacks on
 21 journalists and attorneys is consistent with fighting terrorism and crime. Opp. at 4 n.2.
 22 Regardless of the character of the governments’ actions, no argument is made that
 23 defendants operated outside their official capacity.

24 With regard to the third factor, plaintiffs argue that a judgment enjoining NSO from

26 ¹ Defendants suggest that derivative immunity is grounded in the common law of foreign
 27 sovereign immunity and that Butters v. Vance International, Inc., 225 F.3d 462 (4th Cir.
 28 2000), applied the common law of foreign sovereign immunity. Reply at 10. Defendants
 appear to be merging two distinct doctrines, foreign official immunity and derivative
 sovereign immunity. For clarity, the court only addresses foreign official immunity in this
 section and then addresses derivative immunity, as discussed in Butters.

1 creating or using accounts with WhatsApp would bind only NSO and that a monetary
2 judgment would not be paid from a foreign state's coffers. Opp. at 6. Defendants do not
3 directly address whether exercising jurisdiction would enforce a rule of law against a
4 foreign state. However, in the context of their Rule 12(b)(7) motion to dismiss for failure
5 to join necessary parties, defendants argue that, because defendants' customers were
6 the entities that accessed plaintiffs' services, injunctive relief would necessarily bind
7 those sovereign nations. Mtn. at 19.

8 In Lewis, 918 F.3d at 147, the D.C. Circuit, in evaluating the third factor, reasoned
9 that the defendants in that case failed to demonstrate that the plaintiff sought "to draw on
10 the [foreign state's] treasury or force the state to take specific action, as would be the
11 case if the judgment were enforceable against the state. Defendants in this case are
12 being sued in their individual capacities and Plaintiff [did] not seek[] compensation out of
13 state funds." Applying here, defendants have not argued that any of their foreign
14 sovereign customers would be forced to pay a judgment against defendants if plaintiffs
15 were to prevail in this lawsuit. Plaintiffs also request injunctive relief against defendants
16 "and all other persons acting in concert or conspiracy with any of them or who are
17 affiliated with" defendants. Compl., Request for Relief. This issue is addressed in
18 greater depth with respect to defendants' 12(b)(7) motion, but, briefly, the court can craft
19 injunctive relief that does not require a foreign sovereign to take an affirmative action.
20 Thus, plaintiffs do not seek to enforce a rule of law against defendants' customers.

21 For the foregoing reasons, defendants do not qualify as foreign officials under the
22 content-based prong of the foreign official immunity test.

23 **b. Derivative Sovereign Immunity**

24 Next, defendants argue that the court should apply the derivative sovereign
25 immunity doctrine articulated by the Fourth Circuit in Butters v. Vance International, Inc.,
26 225 F.3d at 466. That case involved a suit by a U.S. employee against her employer, a
27 U.S. corporation. Id. at 464. The employer provided "security services to corporations
28 and foreign sovereigns," specifically to the wife of the king of Saudi Arabia while she was

1 undergoing medical treatment in California. Id. The employee was employed to provide
2 security services but, because of the religious beliefs of the Saudi entourage, was not
3 permitted to work in the command post and eventually filed a gender discrimination suit
4 against her employer. Id.

5 On appeal, the Fourth Circuit determined that the U.S. company could assert
6 derivative sovereign immunity. Id. at 466. The court cited Yearsley v. W.A. Ross
7 Construction Co., 309 U.S. 18, 21–22 (1940), for the proposition that “contractors and
8 common law agents acting within the scope of their employment for the United States
9 have derivative sovereign immunity.” Id. (emphasis added). The court then extended the
10 rule of derivative sovereign immunity to American private agents of foreign governments:

11 It is but a small step to extend this privilege to the private agents
12 of foreign governments. All sovereigns need flexibility to hire
13 private agents to aid them in conducting their governmental
14 functions. This is especially true for foreign sovereigns given
15 their lack of human resources while operating within the United
16 States. To abrogate immunity would discourage American
17 companies from entering lawful agreements with foreign
18 governments and from respecting their wishes even as to
19 sovereign acts.

20 Id.

21 Plaintiffs argue that the court should not apply Butters because no court in this
22 circuit has extended derivative domestic sovereign immunity to work performed for
23 foreign sovereigns. Opp. at 4. They also argue that Samantar effectively abrogated
24 Butters’ holding because Butters cited and relied on the FSIA to extend sovereign
25 immunity to a private entity working for a foreign sovereign. Id. at 6. In response,
26 defendants contend that Butters remains good law and compare the facts here to
27 Yearsley where a contractor’s performance was “authorized and directed” by the
28 government. Reply at 10–11 (quoting Yearsley, 309 U.S. at 20).

The court need not decide whether Samantar abrogated Butters because Butters
is neither controlling nor persuasive authority. Significantly, as plaintiffs note, the Ninth
Circuit has not held that the doctrine of derivative sovereign immunity applies to the

1 foreign contractors of foreign sovereigns.² Nor is it clear that the circuit would do so
 2 because, as the district court in Broidy Capital Management LLC v. Muzin, No. 19-CV-
 3 0150 (DLF), 2020 WL 1536350, at *7 (D.D.C. Mar. 31, 2020), pointed out, there are
 4 different rationales underlying domestic and foreign sovereign immunity. Foreign
 5 sovereign immunity is “a matter of grace and comity on the part of the United States, and
 6 not a restriction imposed by the Constitution.” Verlinden B.V. v. Central Bank of Nigeria,
 7 461 U.S. 480, 486 (1983). Conversely, domestic derivative sovereign immunity stems
 8 from a valid exercise of constitutional authority where the contractor does not exceed
 9 such authority. Yearsley, 309 U.S. at 20–21 (“[I]t is clear that if this authority to carry out
 10 the project was validly conferred, that is, if what was done was within the constitutional
 11 power of Congress, there is no liability on the part of the contractor for executing its
 12 will.”). Moreover, the Supreme Court has cautioned that while “government contractors
 13 obtain certain immunity in connection with work which they do pursuant to their
 14 contractual undertakings with the United States[,] . . . [t]hat immunity, . . . unlike the
 15 sovereign’s, is not absolute.” Campbell-Ewald Co. v. Gomez, 136 S. Ct. 663, 672 (2016)
 16 (quoting Brady v. Roosevelt S.S. Co., 317 U.S. 575, 583 (1943)). In light of these
 17 divergent doctrines and the lack of controlling authority, there is no compelling reason to
 18 extend derivative sovereign immunity to a foreign entity working on behalf of a foreign
 19 sovereign.

20 Even if the court were to apply Butters as persuasive authority, defendants fail to
 21 meet its standard because they are not incorporated or formed in the United States. In

23 ² Other circuits are split on the issue of whether Yearsley constitutes a rule of
 24 jurisdictional immunity. Compare Adkisson v. Jacobs Eng’g Grp., Inc., 790 F.3d 641, 647
 25 (6th Cir. 2015) (“Yearsley immunity is, in our opinion, closer in nature to qualified
 26 immunity for private individuals under government contract, which is an issue to be
 27 reviewed on the merits rather than for jurisdiction.” (citing Filarsky v. Delia, 566 U.S. 377,
 28 389–92 (2012)); Ackerson v. Bean Dredging LLC, 589 F.3d 196, 207 (5th Cir. 2009)
 (“Yearsley does not discuss sovereign immunity or otherwise address the court’s power
 to hear the case . . .”), with Cunningham v. Gen. Dynamics Info. Tech., Inc., 888 F.3d
 640, 650 (4th Cir. 2018) (reaffirming holding that “Yearsley doctrine operates as a
 jurisdictional bar to suit and not as a merits defense to liability”). Because the court can
 resolve the derivative sovereign immunity question on other grounds, it need not wade
 into the circuit split concerning whether a Yearsley defense is jurisdictional.

1 Butters, the defendant asserting derivative sovereign immunity was a U.S. corporation
 2 and the Fourth Circuit’s reasoning indicated that the U.S. citizenship of the company was
 3 necessary to its holding. 225 F.3d at 466 (“To abrogate immunity would discourage
 4 American companies from entering lawful agreements with foreign governments and from
 5 respecting their wishes even as to sovereign acts.” (emphasis added)). None of the other
 6 cases cited by defendants involve the application of derivative sovereign immunity to
 7 foreign entities.³ E.g., Ivey for Carolina Golf Dev. Co. v. Lynch, No. 1:17CV439, 2018 WL
 8 3764264, at *7 (M.D.N.C. Aug. 8, 2018) (applying Butters to find that United States
 9 citizen acting as agent of foreign sovereign was immune); see also Broidy Capital Mgmt.
 10 LLC v. Muzin, No. 19-CV-0150 (DLF), 2020 WL 1536350, at *6 (D.D.C. Mar. 31, 2020)
 11 (recognizing Butters, Ivey, and Alicog v. Kingdom of Saudi Arabia, 860 F. Supp. 379, 384
 12 (S.D. Tex. 1994), as cases “in which courts have extended foreign sovereign immunity to
 13 U.S. citizens”).

14 Accordingly, the doctrine of derivative domestic sovereign immunity is not
 15 applicable to defendants. For the foregoing reasons, defendants’ motion to dismiss for
 16 lack of subject matter jurisdiction is DENIED.

17 2. Personal Jurisdiction

18 a. Consent

19 Defendants argue that they have not consented to personal jurisdiction by
 20 accepting WhatsApp’s terms of service. Mtn. at 11. The Ninth Circuit has recognized
 21 that accepting a forum selection clause evidences consent to personal jurisdiction in that
 22 forum. SEC v. Ross, 504 F.3d 1130, 1149 (9th Cir. 2007) (citing Nat’l Equip. Rental, Ltd.
 23 v. Szukhent, 375 U.S. 311, 315–16 (1964); and Dow Chem. Co. v. Calderon, 422 F.3d
 24

25 _____
 26 ³ In a case cited by defendants, Moriah v. Bank of China Ltd., 107 F. Supp. 3d 272, 277
 27 n.4 (S.D.N.Y. 2015), the district court cited Butters while discussing derivative foreign
 28 sovereign immunity as applied to a foreign official. However, the court’s reasoning
 applied the “two-step procedure” to assess common-law claims of foreign sovereign
 immunity” required by Samantar. Id. at 276 & n.27 (quoting Samantar, 560 U.S. at 312).
 Thus, the court’s citation of Butters was not necessary to its finding and did not discuss
 the distinction between derivative sovereign immunity and foreign official immunity.

1 827, 831 (9th Cir. 2005)). Forum selection clauses are presumptively valid, M/S Bremen
 2 v. Zapata Off-Shore Co., 407 U.S. 1, 10 (1972), and courts “apply federal law to the
 3 interpretation of the forum selection clause.” Doe 1 v. AOL LLC, 552 F.3d 1077, 1081
 4 (9th Cir. 2009) (citing Manetti–Farrow, Inc. v. Gucci Am., Inc., 858 F.2d 509, 513 (9th Cir.
 5 1988)).

6 “Contract terms are to be given their ordinary meaning, and when the terms of a
 7 contract are clear, the intent of the parties must be ascertained from the contract itself.
 8 Whenever possible, the plain language of the contract should be considered first.”
 9 Klamath Water Users Protective Ass’n v. Patterson, 204 F.3d 1206, 1210 (9th Cir. 1999).
 10 A contract is interpreted as a whole and each part is interpreted with reference to the
 11 whole. Id. “A primary rule of interpretation is [t]hat the common or normal meaning of
 12 language will be given to the words of a contract unless circumstances show that in a
 13 particular case a special meaning should be attached to it.” Hunt Wesson Foods, Inc. v.
 14 Supreme Oil Co., 817 F.2d 75, 77 (9th Cir. 1987) (quoting 4 Williston, A Treatise on the
 15 Law of Contracts, § 618 (W. Jaeger 3d ed. 1961)).

16 Here, the forum selection clause in WhatsApp’s terms of service that were in effect
 17 at the time of the alleged conduct provided:

18 If you are not subject to the “Special Arbitration Provision for
 19 United States or Canada Users” section below, you agree that
 20 you will resolve any Claim you have with us relating to, arising
 21 out of, or in any way in connection with our Terms, us, or our
 22 Services (each, a “Dispute,” and together, “Disputes”) exclusively in the United States District Court for the Northern
 23 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.

24 Declaration of Joseph N. Akrotirianakis (“Akro. Decl.”), Ex. 6, Dkt. 45-7, at 9; Declaration
 25 of Michael P. Duffy (“Duffy Decl.”), Ex. 1, Dkt. 55-4, at 4. As defined earlier in the terms
 26 of service, “us” is defined as WhatsApp and “you” is not defined but appears to refer to
 27 the counterparty accepting the terms of service, i.e., the user. Duffy Decl., Ex. 1 at 2.

28 Defendants do not argue that the terms of service are unreasonable, unjust, or

1 otherwise inapplicable to them. Instead, they contend that the present litigation does not
2 fall within the defined term “Dispute” because a dispute involves “any Claim you have
3 with us,” which would not apply to claims WhatsApp has with its users. Mtn. at 11–12.
4 Plaintiffs contend that the better reading of that phrase would include any claim between
5 WhatsApp and its users, regardless of who initiated the claim. Opp. at 11.

6 The question here is whether the parties to the terms of service intended for the
7 definition of the term “Dispute” to apply as a one-way street, i.e., a user filing a claim
8 against WhatsApp, or a two-way street, either a user or WhatsApp filing a claim against
9 the other. By creating a parenthetical with the word “Dispute,” WhatsApp defined that
10 term in reference to the sentence preceding the parenthetical. In relevant part, the term
11 “Dispute” means “any Claim you have with us relating to, arising out of, or in any way in
12 connection with our Terms, us, or our Services.” The common or normal meaning of the
13 word “have” in the phrase “any Claim you have with us” is as a transitive verb meaning
14 “to hold or maintain as a possession, privilege, or entitlement.” Merriam-Webster
15 Dictionary, <https://www.merriam-webster.com/dictionary/have> (last visited June 22,
16 2020). In the phrase “any Claim you have with us,” the subject that has “any Claim” is
17 “you,” not “us.” Thus, the entity holding or maintaining the claim as a possession,
18 privilege, or entitlement is the user not WhatsApp. Reading the foregoing together, the
19 ordinary meaning of the term “Dispute” is that a user holds in possession any claim
20 against WhatsApp and not that WhatsApp possesses a claim against a user.

21 Plaintiffs argue that the court should read the choice of law provision to interpret
22 the way in which the term “Dispute” is read in the forum selection clause. The choice of
23 law provision states: “The laws of the State of California govern our Terms, as well as
24 any Disputes, whether in court or arbitration, which might arise between WhatsApp and
25 you, without regard to conflict of law provisions.” Duffy Decl., Ex. 1 at 4. The phrase
26 “any Disputes . . . between WhatsApp and you” indicates that it applies to a dispute
27 shared by or common to the parties. It is notable that WhatsApp chose to use “between”
28 in the choice of law provision but not the forum selection clause. Had WhatsApp

1 intended to provide for claims initiated by either a user or by WhatsApp, WhatsApp could
 2 have (but did not) use the term “between” when defining the term “dispute.” Additionally,
 3 the choice of law provision uses the defined term “Disputes,” which indicates that the
 4 definition from the forum selection clause should simply be applied in the choice of law
 5 provision but not that the term accumulates an additional meaning (i.e., between)
 6 because of the choice of law provision.

7 Accordingly, the terms of service’s forum selection clause do not apply to claims
 8 initiated by WhatsApp against its users and, therefore, defendants did not consent to
 9 personal jurisdiction.

10 **b. Specific Jurisdiction**

11 Plaintiffs contend that the court should exercise specific jurisdiction over
 12 defendants under both a purposeful direction theory (based on their tort claims) and a
 13 purposeful avilment theory (based on their contract claim). Opp. at 12.

14 **i. Purposeful Direction**

15 Under the Calder effects test, plaintiffs must show that defendants (1) committed
 16 an intentional act, (2) expressly aimed at the forum state, (3) caused harm that the
 17 defendant knew was likely to be suffered in the forum state. Calder v. Jones, 465 U.S.
 18 783, 789–90 (1984).

19 With regard to the first element, plaintiffs have identified the intentional act as the
 20 targeting of WhatsApp’s systems and servers by defendants to disseminate malicious
 21 code and malware. Opp. at 14. Defendants contend that they did not commit the
 22 intentional act in question; instead, foreign governments committed the intentional acts
 23 and have submitted a declaration to that effect. Mtn. at 14. Plaintiffs respond that the
 24 court cannot accept defendants’ contention at the pleading stage. Opp. at 14 n.11.

25 For purposes of personal jurisdiction, there does not appear to be any dispute that
 26 someone sent malicious code and malware through WhatsApp’s servers, accessed
 27 WhatsApp’s servers without authorization, and sent unauthorized commands to
 28 WhatsApp’s computers. Rather the dispute concerns whether defendants’ evidence

1 demonstrates that someone other than defendants committed the intentional act.
2 Plaintiffs allege that defendants accessed WhatsApp’s computers and servers and user’s
3 devices without authorization. Compl. ¶¶ 54, 60. To rebut those allegations, defendants
4 offer the declaration of Shalev Hulio, NSO’s CEO and co-founder, wherein he declares
5 that “NSO markets and licenses the Pegasus technology to its sovereign customers,
6 which then operate the technology themselves” Hulio Decl. ¶ 14. “Defendants role
7 is limited to NSO providing advice and technical support to assist customers in setting
8 up—not operating—the Pegasus technology.” Id.

9 Two points limit the persuasiveness of the declaration. First, the declaration itself
10 leaves open the possibility of defendants’ involvement in the intentional act because
11 Hulio qualifies his statement on defendants’ limited advice and technical support role by
12 stating “[w]hen Defendants provide those support services, they do so entirely at the
13 direction of their government customers, and Defendants follow those directions
14 completely.” Id. Thus, it appears defendants retained some role in conducting the
15 intentional act, even if it was at the direction of their customers. Second, the complaint
16 goes beyond the statements in the Hulio declaration because plaintiffs allege that
17 defendants designed and manufactured a program to exploit WhatsApp’s app, servers,
18 and infrastructure. At this stage, the boundary between defendants’ conduct and their
19 clients’ conduct is not clearly delineated or definitively resolved by the Hulio declaration.
20 Because the court resolves conflicts in affidavits in plaintiffs’ favor and plaintiffs only need
21 to demonstrate that they have established a prima facie showing of jurisdictional facts,
22 Mavrix Photo, 647 F.3d at 1223, plaintiffs have sufficiently demonstrated that defendants
23 committed an intentional act.

24 The second element “asks whether the defendant’s allegedly tortious action was
25 ‘expressly aimed at the forum.’” Picot, 780 F.3d at 1214 (quoting Brayton Purcell LLP v.
26 Recordon & Recordon, 606 F.3d 1124, 1129 (9th Cir. 2010), abrogated on other grounds
27 by Walden, 571 U.S. 277). “The ‘express aiming’ analysis depends, to a significant
28 degree, on the specific type of tort at issue.” Schwarzenegger v. Fred Martin Motor Co.,

1 374 F.3d 797, 807 (9th Cir. 2004). The alleged torts in the complaint center on the
2 improper access to and misuse of WhatsApp's application, servers, and network.

3 Defendants advance several arguments why plaintiffs fail to show express aiming,
4 including a lack of allegations that the leased, third-party servers are located in California
5 and, if they are in California, courts have rejected the argument that the mere location of
6 a server may give rise to personal jurisdiction. Mtn. at 14. Further, the complaint does
7 not allege that any of defendants' code was routed through WhatsApp's servers located
8 in California or that they even have California servers. Id. at 14–15. Defendants also
9 argue that the contact created between an out-of-state defendant and a server is de
10 minimis. Id. at 15. In response, plaintiffs argue that defendants' acts targeted a
11 California-based company and used WhatsApp's and third-party QuadraNet's
12 California-based servers. Opp. at 14–15. Plaintiffs distinguish the cases cited by
13 defendants on the grounds that they dealt with incidental access to third-party servers
14 rather than intentional targeting of WhatsApp's California-based servers. Id. at 15.
15 Plaintiffs also point to marketing by a U.S.-based advertising arm that advertised
16 defendants' ability to target WhatsApp. Id.

17 Much of the express aiming argument centers on the role of computer servers.
18 There are two categories of servers at issue in the personal jurisdiction analysis: third-
19 party servers that were leased by defendants for the alleged purpose of transmitting
20 malware from the leased server to a user's phone (Compl. ¶ 34) and WhatsApp's signaling
21 and relay servers through which defendants routed malicious code to a user's phone (id.
22 ¶ 36). The servers leased by defendants were owned by third parties such as Choopa,
23 QuadraNet, and Amazon Web Services and located in different countries, including the
24 United States. Id. ¶ 34. The complaint does not allege any of these third-party servers
25 are located in California, but declarations attached to plaintiffs' opposition brief aver that
26 QuadraNet is a California-based company with California-based servers. Dkt. 55-1 ¶¶ 3–
27 5; Dkt. 55-6 ¶¶ 2–4, Exs. 1–5.

28 With respect to the leased third-party servers, plaintiffs have not demonstrated that

1 defendants expressly aimed their conduct at the forum state. As other district courts
2 have noted, “the mere location of a third party or its servers is insufficient to give rise to
3 personal jurisdiction.” Hungerstation LLC v. Fast Choice LLC, No. 19-CV-05861-HSG,
4 2020 WL 137160, at *5 (N.D. Cal. Jan. 13, 2020) (collecting cases). Plaintiffs have
5 identified one third party, QuadraNet, that allegedly leased servers, located in California,
6 to defendants.⁴ Defendants filed a supplemental declaration⁵ with their reply brief that
7 expressly denies that defendants contracted with QuadraNet for use of servers. Dkt. 62-
8 1, ¶ 3. This supplemental declaration casts doubt on the fact that defendants used the
9 QuadraNet servers in California. Even without the declaration, the connection between
10 defendants and any leased server located in California is fortuitous. Neither party
11 controlled where the third parties placed their servers and the servers were not the
12 ultimate target of the intentional act. The leased servers were utilized to send malware
13 and other commands to users’ devices but not WhatsApp’s servers. Yet, these users are
14 not alleged to be located in California.

15 With respect to the location of WhatsApp’s relay and signaling servers, two critical
16 facts are relevant. First, the servers in question are not owned by third parties but are
17 WhatsApp’s own servers and, contrary to defendants’ contention in their motion, plaintiffs
18 allege that at least some of those servers were located in California. Compl. ¶ 60
19 (“Defendants knowingly and without permission used and caused to be used WhatsApp
20 Signaling Servers and Relay Servers, including servers located in California, in violation
21

22 ⁴ Plaintiffs request the court judicially notice information from nonparty QuadraNet’s
23 website. Dkt. 56. Specifically, plaintiffs request the court notice QuadraNet’s terms of
24 service as it appeared on its website on January 29, 2019 and the current version of the
25 terms of service, which became effective March 4, 2020. Id. at 2–3. The request is
26 unopposed. Generally, when considering whether to grant a request for judicial notice, a
27 court may consider factual information from the internet as long as the facts are not
28 subject to reasonable dispute. See, e.g., Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1190,
1204 (N.D. Cal. 2014). Accordingly, the court **GRANTS** plaintiffs’ request for judicial
notice.

⁵ Civil Local Rule 7-3(c) permits declarations to be submitted with a reply brief. Civil
Local Rule 7-3(d)(1) permits an opposing party to file an objection to “new evidence [that]
has been submitted in the reply” Plaintiffs did not file an objection (timely or
otherwise) to the supplemental declaration.

1 of California Penal Code § 502(c)(3).” (emphasis added)). Defendants have not
 2 controverted the allegation that WhatsApp’s servers were located in California and the
 3 court accepts the allegation as true. Second, defendants are alleged to have targeted
 4 WhatsApp’s signaling and relay servers and caused malicious code to be routed through
 5 those servers. Id. ¶ 36 (“WhatsApp’s Signaling Servers facilitated the initiation of calls
 6 between different devices using the WhatsApp Service. WhatsApp’s Relay Servers
 7 facilitated certain data transmissions over the WhatsApp Service.”). These allegations
 8 indicate that defendants’ program sought out specific servers—including servers in
 9 California—in order to transmit malicious code through those servers.

10 Because defendants are alleged to have targeted WhatsApp’s own servers, this
 11 case is distinguishable from Hungerstation LLC, 2020 WL 137160, at *5, and Rosen v.
 12 Terapeak, Inc., No. CV-15-00112-MWF (EX), 2015 WL 12724071, at *9 (C.D. Cal. Apr.
 13 28, 2015), where the servers in question were incidental to the alleged conduct and
 14 owned by third parties. Instead, this case is similar to Seattle Sperm Bank, LLC v.
 15 Cryobank Am., LLC, No. C17-1487 RAJ, 2018 WL 3769803, at *1 (W.D. Wash. Aug. 9,
 16 2018), where former employees, located in Phoenix, of the Seattle-based plaintiff were
 17 alleged to have “copied 10 folders onto a removable hard drive contain[ing] more
 18 than 1,500 documents These materials were housed on a server in Seattle,
 19 Washington.” The court went on to reason that

20 [d]efendants worked for a company whose principal place of
 21 business in Seattle, Washington, a fact that they had
 22 knowledge of, as Defendants attest that Blaine interviewed for
 23 his job there and Kumar had his initial training there. [The
 24 defendant employees] downloaded the allegedly
 misappropriated information from servers located in Seattle,
 Washington. Not only is Plaintiff headquartered in Seattle, but
 Defendants’ actions allegedly caused harm likely to be suffered
 in Washington.

25 Id. at *2 (citation omitted).

26 Here, similar to Seattle Sperm Bank, defendants sought out and accessed
 27
 28

1 plaintiffs' servers.⁶ Defendants are alleged to have reverse-engineered the WhatsApp
 2 app and developed a program that emulated legitimate WhatsApp network traffic in order
 3 to transmit malicious code over WhatsApp servers. Compl. ¶ 35. This indicates a
 4 knowledge of how WhatsApp's servers worked and where they were located such that
 5 defendants could exploit WhatsApp's servers for their own use and the use of their
 6 customers.

7 In their reply brief, defendants argue that, even if WhatsApp had servers in
 8 California and NSO sent messages through those servers, there is no allegation or
 9 argument that NSO selected the location of the server. Reply at 6. In other words,
 10 defendants contend the location of the server is fortuitous and their claims would have
 11 been the same if the servers were located in Cleveland, Paris, or Timbuktu. *Id.* at 7. The
 12 express aiming prong depends on the type of tort alleged, *Picot*, 780 F.3d at 1214, and
 13 here plaintiffs allege that defendants targeted and accessed WhatsApp's servers without
 14 authorization. The location of the servers is, therefore, not a fortuity but central to the
 15 alleged tortious conduct. For example, courts have analogized a CFAA cause of action
 16 to digital "breaking and entering" and a "trespass offense" *hiQ Labs, Inc. v. LinkedIn*
 17 *Corp.*, 938 F.3d 985, 1001 (9th Cir. 2019) (citations omitted), similar to the common law
 18 trespass to chattels offense alleged. By sending malicious code to the California based
 19 servers, defendants allegedly caused a digital transmission to enter California, which
 20 then effectuated a breaking and entering of a server in California. *Cf. Picot*, 780 F.3d at
 21 1215 (concluding personal jurisdiction not appropriate in California where the defendant
 22 interfered with a contract "without entering California, contacting any person in California,
 23 or otherwise reaching out to California").

24
 25 _____
 26 ⁶ Defendants would distinguish *Seattle Sperm Bank* on the grounds that the plaintiff in
 27 that case intentionally stole data from the servers, which defendants are not alleged to
 28 have done here. Reply at 7 n.9. The difference between the misappropriation of trade
 secrets tort alleged in *Seattle Sperm Bank*, 2018 WL 3769803, at *2, and the trespass to
 chattels and unauthorized access torts alleged here is not material for purposes of
 express aiming. Both cases involve an intentional tort that seeks access to a computer
 system without permission.

1 Finally, defendants argue that even if defendants targeted plaintiffs and knew
 2 plaintiffs to be California residents, plaintiffs have not shown defendants targeted
 3 California. Mtn. at 13–14. Defendants are correct to note that plaintiffs cannot rely on a
 4 theory of individualized targeting. Prior to Walden v. Fiore, courts in this circuit found the
 5 express aiming element to be satisfied where a defendant knew of the plaintiff’s
 6 connection to the forum and there was a foreseeable harm to the plaintiff. See, e.g.,
 7 Amini Innovation Corp. v. JS Imports, Inc., 497 F. Supp. 2d 1093, 1105 (C.D. Cal. 2007).
 8 As the Ninth Circuit’s opinion in Axiom Foods, Inc. v. Acerchem International, Inc., 874
 9 F.3d 1064, 1069–70 (9th Cir. 2017), held, Walden requires more than knowledge of a
 10 plaintiff’s forum connections combined with the foreseeable harm that plaintiffs suffered in
 11 the forum. This holding effectively abrogated any individualized targeting theory. Rather,
 12 a court “must look to the defendant’s ‘own contacts’ with the forum, not to the defendant’s
 13 knowledge of a plaintiff’s connections to a forum.” Id. at 1070 (quoting Walden, 571 U.S.
 14 at 289). “Calder made clear that mere injury to a forum resident is not a sufficient
 15 connection to the forum. . . . The proper question is not where the plaintiff experienced a
 16 particular injury or effect but whether the defendant’s conduct connects him to the forum
 17 in a meaningful way.”⁷ Walden, 571 U.S. at 290.

18 Applying here, it is clear that the alleged conduct goes beyond defendants’
 19 knowledge that plaintiffs are located in California and would suffer harm in California.
 20 The complaint avers that defendants sought out WhatsApp’s California-based servers for
 21 the purpose of routing malicious code through those servers to ultimately reach individual
 22 users’ phones. By sending the malicious code, defendants electronically entered the

23 _____
 24 ⁷ While Walden reaffirmed that a defendant’s conduct remains the touchstone of specific
 25 jurisdiction, the Court expressly reserved deciding the amount of minimum contacts
 26 “where intentional torts are committed via the Internet or other electronic means (e.g.,
 27 fraudulent access of financial accounts or ‘phishing’ schemes).” Walden, 571 U.S. at 290
 28 n.9. The Court characterized intentional torts committed using electronic means as
 “present[ing] the very different questions whether and how a defendant’s virtual
 ‘presence’ and conduct translate into ‘contacts’ with a particular State.” Id. This footnote
 reinforces the court’s conclusion that where a defendant enters a forum state with
 malicious code and seeks out servers owned by a plaintiff in that forum state and then
 commits an intentional tort, such conduct is sufficient to find personal jurisdiction.

1 forum state seeking out plaintiffs' servers, which were a necessary component to transmit
2 the malicious code to the users. Defendants created a connection with the forum beyond
3 an individualized targeting theory. Accordingly, plaintiffs have demonstrated that
4 defendants expressly aimed their intentional act at the forum state.

5 The third element of the Calder effects test is whether the defendants caused
6 harm that they knew would likely be suffered in the forum state. Defendants do not offer
7 any argument as to this element. Plaintiffs have alleged that defendants harmed them by
8 interfering with the WhatsApp service and burdening their network and have injured
9 plaintiffs' reputation, public trust, and goodwill. Compl. ¶¶ 46–47. If defendants did
10 access plaintiffs' servers without authorization (or exceeded authorized access), then
11 they would have known they were harming plaintiffs. See id., Ex. 10 at 33 (product
12 description naming Facebook and WhatsApp as applications to be monitored).

13 Defendants also knew that such harm would be suffered in California; for example, the
14 Hulo declaration states that Facebook contacted NSO to inquire about certain
15 capabilities of Pegasus, indicating that defendants were well aware of plaintiffs and their
16 principal place of business in California. Hulo Decl. ¶ 10. Therefore, plaintiffs have
17 demonstrated the purposeful direction element of specific jurisdiction. For that reason,
18 the court does not reach plaintiffs' argument that the court has jurisdiction under
19 Rule 4(k)(2).

20 ii. Purposeful Availment

21 A prima facie showing of purposeful availment “typically consists of evidence of
22 the defendant’s actions in the forum, such as executing or performing a contract there.
23 By taking such actions, a defendant ‘purposefully avails itself of the privilege of
24 conducting activities within the forum State, thus invoking the benefits and protections of
25 its laws.’” Schwarzenegger, 374 F.3d at 802 (quoting Hanson, 357 U.S. at 253). When
26 analyzing purposeful availment, the court must “use a highly realistic approach that
27 recognizes that a contract is ordinarily but an intermediate step serving to tie up prior
28 business negotiations with future consequences which themselves are the real object of

1 the business transaction.” Burger King, 471 U.S. at 479 (internal quotation marks and
2 citation omitted). Generally, an individual’s contract with an out-of-state party alone
3 cannot establish sufficient minimum contacts. Id. at 478. “To have purposefully availed
4 itself of the privilege of doing business in the forum, a defendant must have ‘performed
5 some type of affirmative conduct which allows or promotes the transaction of business
6 within the forum state.’” Boschetto v. Hansing, 539 F.3d 1011, 1016 (9th Cir. 2008)
7 (quoting Sher v. Johnson, 911 F.2d 1357, 1362 (9th Cir. 1990)). Courts examine the
8 “prior negotiations and contemplated future consequences, along with the terms of the
9 contract and the parties’ actual course of dealing” that “determin[e] whether the
10 defendant purposefully established minimum contacts with the forum.” Burger King, 471
11 U.S. at 479.

12 Defendants argue that plaintiffs cannot demonstrate purposeful availment because
13 defendants did not take any actions in the forum, such as executing or performing a
14 contract in California. Mtn. at 16. While defendants acknowledge they accepted the
15 terms of service, they contend a contract alone does not establish minimum contacts and
16 there are no other allegations of affirmative conduct in California. Id. Plaintiffs argue that
17 defendants purposefully availed themselves of California’s benefits for three reasons.
18 First, the terms of service included a California choice-of-law clause, which shows an
19 intent by defendants to avail themselves of California law. Opp. at 12. Second,
20 defendants continuously performed under the terms of service. Id. at 12–13. Third,
21 defendants engaged in activities directed at California such as developing Pegasus with
22 financing from a California-based private equity firm and contracting with a California-
23 based technology company, QuadraNet. Id. at 13.

24 Beginning with prior negotiations, there is no allegation or evidence that the parties
25 engaged in prior negotiations. Nor would one expect there to be any negotiations
26 because terms of service are contracts of adhesion that users choose to either accept or
27 reject based on whether they desire to use a company’s service. Next, the contemplated
28 performance does not center on California. WhatsApp’s terms of service apply to every

1 user no matter where they are located. As plaintiffs point out, the terms of service
2 committed defendants to continuously perform under the contract, but nothing about that
3 performance had anything to do with California—especially in this instance where
4 defendants are not alleged to have traveled to or otherwise performed in California after
5 they agreed to the terms of service.

6 With respect to the terms of the contract, plaintiffs point to the choice-of-law
7 provision in the terms of service. That provision stated: “[t]he laws of the State of
8 California govern our Terms, as well as any Disputes, whether in court or arbitration,
9 which might arise between WhatsApp and you, without regard to conflict of law
10 provisions.” Duffy Decl., Ex. 1. WhatsApp’s choice of law provision would be relevant if it
11 were combined with other facts to demonstrate that defendants purposefully availed
12 themselves of California law. In Google, Inc. v. Eolas Technologies Inc., No. 13-cv-
13 05997-JST, 2014 WL 2916621, at *3 (N.D. Cal. June 24, 2014), the court found the
14 choice of law provision persuasive in the context of a 20-year licensing agreement
15 whereby the defendant entered into the agreement in California, was formerly a California
16 entity, and agreed to ongoing marketing, litigation, and bookkeeping obligations as part of
17 a patent royalty agreement. Similarly, in Facebook, Inc. v. Rankwave Co., No. 19-cv-
18 03738-JST, 2019 WL 8895237, at *6 (N.D. Cal. Nov. 14, 2019), the court assumed that
19 the defendant, as a “sophisticated entity . . . consented to the [terms of service] and its
20 choice-of-law provision for seven of the years during which it created and operated apps
21 on Facebook’s platform.” Thus, the choice of law provision may be relevant but only
22 when combined with other facts that defendants intended to avail themselves of
23 California law.

24 There are no such facts here. This case involves a contract of adhesion where
25 defendants, despite being sophisticated entities, had no ability to negotiate the terms of
26 service. Unlike Eolas (licensing agreement) and Rankwave (creating apps), defendants
27 were only using WhatsApp’s service as any individual consumer might. If the court were
28 to accept plaintiffs’ argument, then any user simply by accepting the terms of service and

1 otherwise having no interaction with California could be said to have purposefully availed
2 him or herself of California's laws.

3 Plaintiffs advance a few other arguments that involve conduct outside the four
4 corners of the terms of service. First, defendants are alleged to have received financing
5 from a California-based private equity firm. From 2014 to February 2019, a San
6 Francisco-based entity owned a controlling interest in NSO. Compl. ¶ 5 & Ex. 4. This
7 fact represents a potential connection with California, but plaintiffs have not connected it
8 to the WhatsApp terms of service, the alleged conduct (which occurred after Q Cyber
9 acquired NSO), or that the funding was instrumental to the alleged conduct. Second,
10 plaintiffs argue that defendants intentionally exploited WhatsApp's California-based
11 infrastructure. This allegation is relevant to the purposeful direction test but is not
12 relevant to purposeful avilment. Third, plaintiffs point to defendants' contract with
13 QuadraNet to use QuadraNet's servers to direct malware to WhatsApp's users.
14 Defendants have denied this fact in a supplemental declaration. Nor is it clear how a
15 contract with a third party informs the purposeful avilment analysis concerning the terms
16 of service agreed to by WhatsApp and defendants.

17 In sum, plaintiffs have not met their burden to demonstrate purposeful avilment.
18 Because, however, plaintiffs have met their burden with respect to purposeful direction,
19 the court turns to whether exercising personal jurisdiction would comport with fair play
20 and substantial justice.

21 **iii. Reasonableness and Pendent Jurisdiction**

22 The factors that are relevant to the fair play and substantial justice evaluation are:
23 "(1) the extent of the defendants' purposeful injection into the forum state's affairs; (2) the
24 burden on the defendant of defending in the forum; (3) the extent of the conflict with the
25 sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the
26 dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of
27 the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence
28 of an alternative forum." CollegeSource, 653 F.3d at 1079. No one factor is dispositive

1 and the court must balance all of the factors. Core-Vent Corp. v. Nobel Indus., AB, 11
 2 F.3d 1482, 1488 (9th Cir. 1993). The more attenuated the contacts with the forum state,
 3 the less a defendant must show in terms of unreasonableness to defeat the court's
 4 exercise of jurisdiction. Id. At this step of the specific jurisdiction analysis, the burden
 5 shifts to defendants to present a compelling case that jurisdiction would be unreasonable.
 6 Burger King, 471 U.S. at 477.

7 First, the purposeful injection factor is analogous to the purposeful direction
 8 analysis. Corp. Inv. Bus. Brokers v. Melcher, 824 F.2d 786, 790 (9th Cir. 1987) ("Ninth
 9 Circuit cases give the 'purposeful interjectment' factor no weight once it is shown that the
 10 defendant purposefully directed its activities to the forum state" (citations omitted)).
 11 Because plaintiffs demonstrated purposeful direction, defendants injected themselves
 12 into the forum state.

13 Second, courts "examine the burden on the defendant in light of the corresponding
 14 burden on the plaintiff." Sinatra v. Nat'l Enquirer, Inc., 854 F.2d 1191, 1199 (9th Cir.
 15 1988) (quoting Brand v. Menlove Dodge, 796 F.2d 1070, 1075 (9th Cir. 1986)). Here, the
 16 burden on defendants to litigate in California is substantial given that their witnesses and
 17 evidence are located in Israel. However, the burden on plaintiffs to litigate in Israel would
 18 be similarly burdensome as their witnesses and evidence are located in California.
 19 Defendants have also secured U.S.-based outside counsel and a U.S.-based public
 20 relations firm for the express purpose of this lawsuit (Dkt. 20-6), which indicates the
 21 burden is somewhat mitigated. Further, given the advances in technology, it is not clear
 22 that the burden of litigating is so great as to violate due process. See Sinatra, 796 F.2d
 23 at 1199 (observing, in 1988, that "modern advances in communications and
 24 transportation have significantly reduced the burden of litigating in another country"
 25 (citations omitted)). In sum, this factor is in equipoise.

26 Third, "conflict with the sovereignty of the defendant's state 'is not dispositive
 27 because, if given controlling weight, it would always prevent suit against a foreign
 28 national in a United States court.'" Id. (quoting Gates Learjet Corp. v. Jensen, 743 F.2d

1 1325, 1333 (9th Cir. 1984)). “The Supreme Court, though, has cautioned against
 2 extending state long arm statutes in an international context.” Id. (citing Asahi Metal
 3 Indus. Co. v. Superior Ct. of Cal., Solano Cty., 480 U.S. 102, 115 (1987)). Here, while
 4 defendants have presented no evidence as to a particular interest, the state of Israel has
 5 some presumable interest in adjudicating conflicts concerning their corporate citizens.
 6 See Harris Rutsky & Co. Ins. Servs. v. Bell & Clements Ltd., 328 F.3d 1122, 1133 (9th
 7 Cir. 2003) (“While [defendant] has presented no evidence of the United Kingdom’s
 8 particular interest in adjudicating this suit, we may presume for present purposes that
 9 there is such an interest.”). This factor cuts in favor of defendants.

10 Fourth, California maintains a strong interest in providing an effective means of
 11 redress for its residents tortuously injured in California. Sinatra, 854 F.2d at 1200. Here,
 12 plaintiffs’ principal places of business are Menlo Park, California and they were allegedly
 13 harmed in California. This factor militates in favor of exercising jurisdiction.

14 Fifth, in considering which forum could most efficiently resolve this dispute, courts
 15 “focus on the location of the evidence and witnesses.” Harris Rutsky, 328 F.3d at 1133
 16 (citing Caruth v. Int’l Psychoanalytical Ass’n, 59 F.3d 126, 129 (9th Cir. 1995)). Here,
 17 defendants’ evidence and witnesses are located in Israel and plaintiffs’ evidence and
 18 witnesses are in California. This factor is neutral especially given the advances of
 19 modern technology. See Panavision Int’l v. Toeppen, 141 F.3d 1316, 1323 (9th Cir.
 20 1998) (noting factor is “no longer weighed heavily given the modern advances in
 21 communication and transportation” (citation omitted)).

22 Sixth, “[i]n evaluating the convenience and effectiveness of relief for the plaintiff,
 23 we have given little weight to the plaintiff’s inconvenience.” Id. at 1324 (citing Ziegler v.
 24 Indian River Cty., 64 F.3d 470, 476 (9th Cir. 1995)). Here, the maintenance of this suit in
 25 a foreign country would be inconvenient for plaintiffs. This factor tips in plaintiffs’ favor,
 26 though only slightly.

27 Seventh, the parties dispute which party has the burden to show Israel is
 28 inadequate as an alternative forum. Defendants cite Ballard v. Savage, 65 F.3d 1495,

1 1502 (9th Cir. 1995), where the Ninth Circuit stated that the defendant “Royal claims that
2 an Austrian court could hear [the plaintiff’s] claims, but it presents absolutely no evidence
3 on this issue, erroneously assuming that the burden is on [the plaintiff] to prove the lack
4 of an alternate forum.” Ballard cites no authority for the proposition that the defendant
5 must prove lack of alternate forum. In contrast, defendants cite Amoco Egypt Oil Co. v.
6 Leonis Navigation Co., where the court stated that the plaintiff “Amoco has the burden of
7 proving the unavailability of an alternative forum.” 1 F.3d 848, 853 (9th Cir. 1993) (citing
8 Pac. Atl. Trading Co. v. M/V Main Exp., 758 F.2d 1325, 1331 (9th Cir. 1985)). Both
9 Sinatra, 854 F.2d at 1201, and Harris Rutsky, 328 F.3d at 1134, cases decided before
10 and after Ballard, hold that the burden is on plaintiffs to prove unavailability. The weight
11 of authority holds that plaintiffs have the burden on this factor and they have not cited any
12 evidence that Israel is not an available alternative forum whereas defendants cite several
13 cases finding Israel to be an available forum. E.g., Israel Discount Bank Ltd. v. Schapp,
14 505 F. Supp. 2d 651, 659 (C.D. Cal. 2007). This factor points towards defendants.

15 In sum, some factors tip in defendants’ favor and others tip in plaintiffs’ favor. The
16 Ninth Circuit has indicated that, in such an instance, a defendant has not carried its
17 burden to present a compelling case that exercising jurisdiction would be unreasonable.
18 See Harris Rutsky, 328 F.3d at 1134 (“The balance is essentially a wash, since some of
19 the reasonableness factors weigh in favor of [defendant], but others weigh against it.”);
20 see also Roth v. Garcia Marquez, 942 F.2d 617, 625 (9th Cir. 1991) (finding exercise of
21 jurisdiction was reasonable even though only two reasonableness factors favored
22 plaintiff, while three favored defendant). Accordingly, exercising personal jurisdiction
23 over defendants comports with fair play and substantial justice.

24 Finally, plaintiffs argue that, if the court finds personal jurisdiction is appropriate
25 over some but not all claims, the court should exercise pendent jurisdiction over the
26 remaining claims. Opp. at 18. They contend that NSO’s unauthorized use of
27 WhatsApp’s infrastructure underpins each of plaintiffs’ claims. Id. at 19. Defendants do
28 not address pendent jurisdiction.

1 “Personal jurisdiction must exist for each claim asserted against a defendant.”⁸
 2 Action Embroidery Corp. v. Atl. Embroidery, Inc., 368 F.3d 1174, 1180 (9th Cir. 2004)
 3 (citing Data Disc, Inc. v. Sys. Tech. Assocs., Inc., 557 F.2d 1280, 1289 n.8 (9th Cir.
 4 1977)). “[A] court may assert pendent personal jurisdiction over a defendant with respect
 5 to a claim for which there is no independent basis of personal jurisdiction so long as it
 6 arises out of a common nucleus of operative facts with a claim in the same suit over
 7 which the court does have personal jurisdiction.” Id. In this case, the breach of contract
 8 claim involves the same common nucleus of operative facts as the tort claims and
 9 pendent jurisdiction is appropriate.

10 For the foregoing reasons, defendants’ motion to dismiss the complaint for lack of
 11 personal jurisdiction is DENIED.

12 3. Failure to Join Necessary Parties

13 Defendants move to dismiss the complaint because plaintiffs failed to join
 14 defendants’ foreign sovereign customers under Rule 19. Mtn. at 18. As an initial matter,
 15 defendants argue only that their customers are required parties under Rule 19(a)(1)(A),
 16 (id. at 19), and the court focuses its analysis on that provision.

17 Finding a party to be necessary under Rule 19(a)(1)(A) requires the court to
 18

19 ⁸ The court uses the term “pendent personal jurisdiction” to distinguish the concept from
 20 the supplemental jurisdiction statute, 28 U.S.C. § 1367. As explained by a leading
 21 treatise:

22 In recent years, there has been some debate about whether
 23 Section 1367 of Title 28, the supplemental jurisdiction statute,
 24 should be read to include the doctrine of pendent personal
 25 jurisdiction. Neither the plain meaning of this statute, which
 26 shows it to be a subject matter jurisdiction provision, nor its
 27 legislative history supports the conclusion that Congress
 28 intended Section 1367 to include personal jurisdiction [I]f
 pendent personal jurisdiction exists, it must be properly
 understood to be a federal common law doctrine. For the sake
 of clarity, this section will refer to “pendent personal jurisdiction”
 rather than “supplemental personal jurisdiction” to highlight the
 fact that Section 1367 should not be read to subsume personal
 as well as subject matter jurisdiction.

4A Wright & Miller, Federal Practice & Procedure, § 1069.7 (4th ed. 2020).

1 determine that “complete relief” cannot be accorded between the existing parties absent
2 the joinder of the nonparty. “This factor is concerned with consummate rather than partial
3 or hollow relief as to those already parties, and with precluding multiple lawsuits on the
4 same cause of action.” Northrop Corp. v. McDonnell Douglas Corp., 705 F.2d 1030,
5 1043 (9th Cir. 1983) (citing Advisory Committee’s Note, 39 F.R.D. 89, 91 (1966)). In
6 conducting a Rule 19(a)(1)(A) analysis, courts ask whether the absence of the nonparty
7 party would preclude the court from fashioning meaningful relief as between the parties.
8 Id. at 1044. This prong only concerns current parties to the action. Disabled Rights
9 Action Comm. v. Las Vegas Events, Inc., 375 F.3d 861, 879 (9th Cir. 2004); see also
10 NGV Gaming, Ltd. v. Upstream Point Molate, LLC, 355 F. Supp. 2d 1061, 1068 (N.D.
11 Cal. 2005) (“The effect a decision may have on the absent party is not material.” (internal
12 quotation marks and citation omitted)).

13 Here, the parties focus on whether the court can issue an injunction that would
14 afford plaintiffs complete relief. The complaint requests the following: “[t]hat the Court
15 enter a permanent injunction enjoining and restraining Defendants and their agents,
16 servants, employees, successors, and assigns, and all other persons acting in concert
17 with or conspiracy with any of them or who are affiliated with Defendants from” various
18 actions including accessing or attempting to access WhatsApp’s service or platform.
19 Compl., Request for Relief. There are two possible readings of the underlined language.
20 On the one hand “all other persons acting in concert with or conspiracy with any of them”
21 could be read as seeking an injunction against defendants’ customers who both parties
22 acknowledge are sovereign nations. On the other hand, the language could be read as
23 standard boilerplate drawn from Rule 65(d)(2)(C) that does not necessarily bind the
24 sovereign nations by requiring them to take an affirmative action.

25 In EEOC v. Peabody Western Coal Co., 610 F.3d 1070, 1079 (9th Cir. 2010), the
26 Ninth Circuit encountered a similar Rule 19 challenge concerning the scope of potential
27 injunctive relief. There, the defendant argued that a sovereign entity (previously a
28 defendant to the suit but dismissed by an earlier appellate decision) was a necessary

1 party because of the plaintiff's request for injunctive relief, using language drawn from
2 Rule 65. Id. The court reasoned that the "better reading of the boilerplate language in
3 the complaint" was that the plaintiff was not seeking injunctive relief against a non-party
4 sovereign entity. This reasoning indicates that the better reading of plaintiffs' relief, which
5 involves similar boilerplate language from Rule 65, is that plaintiffs are not seeking
6 injunctive relief against defendants' foreign sovereign customers. Such reasoning is not
7 a complete answer because Peabody Western relied, in part, on the fact that an earlier
8 Ninth Circuit opinion in that case determined that the sovereign entity could not be sued.
9 No such finding has been made in this case.

10 More importantly, defendants' customers are not required parties because the
11 court can craft injunctive relief that excludes or carves out any sovereign nation.
12 Peabody Western recognized as much stating, "the district court nonetheless erred in
13 dismissing EEOC's suit. Because we had held in Peabody II that joinder of the Nation
14 was feasible despite the unavailability of injunctive relief against it, the proper response of
15 the district court would have been simply to deny EEOC's request for injunctive relief.
16 610 F.3d at 1080 (emphasis added). The district court in Broidy Capital Management,
17 LLC v. Qatar, No. CV 18-2421-JFW(Ex), 2018 WL 6074570, at *10 (C.D. Cal. Aug. 8,
18 2018), arrived at a similar conclusion in a CFAA case involving the sovereign nation of
19 Qatar. The district court determined that Qatar was a necessary party under Rule
20 19(a)(1)(A) because "[p]laintiffs seek injunctive relief prohibiting all defendants including
21 Qatar, from accessing Plaintiffs' protected computers without authorization" Id. at
22 *9. However, the court determined that Qatar was not an indispensable party because
23 relief could be effected without Qatar. Id. at *10 ("[A]ny potential prejudice by Qatar's
24 absence from this action can be lessened or avoided entirely by crafting injunctive relief
25 that would affect only the remaining defendants, and not Qatar."). Though the court
26 resolved the Rule 19 analysis at the subdivision (b) step, the reasoning is applicable to
27 the Rule 19(a) analysis.

28 Defendants rely on the holding from Republic of Philippines v. Pimentel, 553 U.S.

1 851, 867 (2008), that “[a] case may not proceed when a required-entity sovereign is not
 2 amenable to suit.” In Pimentel, “[t]he application of subdivision (a) of Rule 19 [was] not
 3 contested” and the foreign sovereigns in that case were “required entities.” Id. at 863–64.
 4 Pimentel’s analysis proceeds from the starting point that the sovereign is a necessary (or
 5 required party) under Rule 19(a). Thus, Pimentel is distinguishable because Rule 19(a)
 6 is contested in this case and Peabody Western controls the Rule 19(a)(1)(A) analysis and
 7 outcome. Because defendants’ foreign sovereign customers are not necessary parties,
 8 Pimentel’s holding does not apply.

9 For the foregoing reasons, defendants’ motion to dismiss the complaint for failure
 10 to join necessary parties is DENIED.

11 **4. Failure to State a Claim**

12 **a. First Claim: CFAA**

13 “The CFAA prohibits acts of computer trespass by those who are not authorized
 14 users or who exceed authorized use.” Facebook, Inc. v. Power Ventures, Inc., 844 F.3d
 15 1058, 1065 (9th Cir. 2016). “It creates criminal and civil liability for whoever “intentionally
 16 accesses a computer without authorization or exceeds authorized access, and thereby
 17 obtains . . . information from any protected computer.” Id. at 1065–66 (alteration in
 18 original) (quoting 18 U.S.C. § 1030(a)(2)(C)). “The statute thus provides two ways of
 19 committing the crime of improperly accessing a protected computer: (1) obtaining access
 20 without authorization; and (2) obtaining access with authorization but then using that
 21 access improperly.” Musacchio v. United States, 136 S. Ct. 709, 713 (2016). “[T]he
 22 CFAA is best understood as an anti-intrusion statute and not as a ‘misappropriation
 23 statute.’” hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1000 (9th Cir. 2019) (quoting
 24 United States v. Nosal (“Nosal I”), 676 F.3d 854, 857–58 (9th Cir. 2012) (en banc)). The
 25 operative question is whether “the conduct at issue is analogous to ‘breaking and
 26 entering.’” Id. at 1001 (citation omitted).

27 **i. WhatsApp’s Servers**

28 Defendants argue that the allegations in the complaint are analogous to LVRC

1 Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), because, as WhatsApp users,
2 they had authorization, pursuant to the terms of service, to access WhatsApp's
3 computers and servers to send messages over the WhatsApp app. Mtn. at 21. Plaintiffs
4 respond that whether access to a computer is "authorized" depends on actions by the
5 computer's owner to grant or deny permission. Opp. at 20. In this case, no WhatsApp
6 user had permission to access the technical call settings or evade WhatsApp's security
7 and, thus, there was no authorization. Id. at 21.

8 In Brekka, 581 F.3d at 1129, an employee was given permission by his employer
9 to access the employer's website using an administrative login that gave the employee
10 broad access to the data on the website. During this time, the employee emailed
11 documents he obtained to his personal computer. Id. The employee eventually ceased
12 working for the employer but continued to use his administrative login, which had not
13 been revoked by the employer, to access the employer's website. Id. at 1130.

14 The court first determined that because the employer gave the employee
15 permission to access a company computer, the employee could not have been acting
16 "without authorization." Id. at 1133. Further, an employee is not acting "without
17 authorization" simply because the "employee resolves to use the computer contrary to
18 the employer's interest." Id. In support of that conclusion, the court examined the
19 difference between the "without authorization" and "exceeds authorized access" prongs
20 of the CFAA. The CFAA defines the term "exceeds authorized access" as meaning "to
21 access a computer with authorization and to use such access to obtain or alter
22 information in the computer that the accesser is not entitled so to obtain or alter." 18
23 U.S.C. § 1030(e)(6).

24 As this definition makes clear, an individual who is authorized
25 to use a computer for certain purposes but goes beyond those
26 limitations is considered by the CFAA as someone who has
27 "exceed[ed] authorized access." . . . In other words, for
28 purposes of the CFAA, 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.

1 Brekka, 581 F.3d at 1133 (first alteration in original). The court then summarized the two
2 prongs as follows: “a person who ‘intentionally accesses a computer without
3 authorization,’ accesses a computer without any permission at all, while a person who
4 ‘exceeds authorized access,’ has permission to access the computer, but accesses
5 information on the computer that the person is not entitled to access.” Id. (citing 18
6 U.S.C. § 1030(a)(2), (a)(4)).

7 Applying here, the complaint confirms that “[d]efendants created WhatsApp
8 accounts that they used and caused to be used to send malicious code to Target Devices
9 in April and May 2019.” Compl. ¶ 33. By creating WhatsApp accounts and accepting the
10 terms of service, defendants, as is true of any WhatsApp user, had authorization to send
11 messages using the WhatsApp app, which would be transmitted over WhatsApp’s
12 servers. For that reason, this case is similar to the Brekka employee’s conduct prior to
13 his termination because defendants here had at least some level of authorized access to
14 the protected computers in question. Therefore, the facts alleged are not an instance
15 where a person accesses a computer without any permission at all. With regard to the
16 WhatsApp servers, plaintiffs have not stated a claim for a violation of 18 U.S.C.
17 § 1030(a)(2) and (a)(4) by intentionally accessing information on a protected computer
18 “without authorization.”

19 This is not the end of the inquiry because the factual allegations detail conduct that
20 meets the “exceeds authorized access” prong of 18 U.S.C. § 1030(a)(2) and (a)(4).
21 WhatsApp imposes certain limitations on accessing portions of its servers, such as
22 prohibiting access to the technical call settings. Defendants are alleged to have created
23 a program that went beyond those restrictions by evading WhatsApp’s security features
24 and manipulating the technical call settings. For example, plaintiffs allege that
25 defendants used their program to “avoid the technical restrictions built into WhatsApp
26 Signaling Servers” and “formatted call initiation messages containing malicious code to
27 appear like a legitimate call and concealed the code within call settings.” Compl. ¶ 37.
28 Defendants’ program would then use “WhatsApp servers to route malicious code, which

1 masqueraded as a series of legitimate calls and call settings, to a Target Device using
 2 telephone number (202) XXX-XXXX.” Id. ¶ 38. Defendants also are alleged to have
 3 used “WhatsApp’s Relay Servers without authorization to send encrypted data packets
 4 designed to activate the malicious code injected into the memory of the Target Devices.”
 5 Id. ¶ 39. These factual allegations meet the definition of exceeds authorized access
 6 because defendants had permission to access a portion of the computer in question (the
 7 WhatsApp servers) but did not have permission to access other portions. See Nosal I,
 8 676 F.3d at 857 (“[A]ssume an employee is permitted to access only product information
 9 on the company’s computer but accesses customer data: He would “exceed []
 10 authorized access” if he looks at the customer lists.” (second alteration in original)).

11 Defendants offer two rejoinders to the exceeds authorized access prong. Neither
 12 is persuasive. First, defendants argue that even if the court applies the “exceeds
 13 authorized access” prong of the CFAA, the Ninth Circuit has held that the CFAA does not
 14 apply to “violations of corporate computer use restrictions.” Mtn. at 21–22 (quoting
 15 Nosal I, 676 F.3d at 862. Defendants are correct that “a violation of the terms of use of a
 16 website—without more—cannot establish liability under the CFAA.” Power Ventures, 844
 17 F.3d at 1067. Plaintiffs’ allegations go beyond any restrictions imposed by WhatsApp’s
 18 terms of service because they allege that defendants’ program “avoid[ed] the technical
 19 restrictions built into WhatsApp Signaling Servers.” Compl. ¶ 37. Avoiding technical
 20 restrictions goes beyond any contractual limits imposed by the terms of service. See
 21 Nosal I, 676 F.3d at 863 (purpose of CFAA is “to punish hacking—the circumvention of
 22 technological access barriers”).

23 Second, defendants cite hiQ Labs for the proposition that technical restrictions
 24 imposed by plaintiffs cannot state a “without authorization” theory. Reply at 13. That
 25 case involved a data scraping company that scraped LinkedIn’s servers for information
 26 that was publicly available. hiQ Labs, 938 F.3d at 992. The court summarized:

27 it appears that the CFAA’s prohibition on accessing a computer
 28 “without authorization” is violated when a person circumvents a
 computer’s generally applicable rules regarding access

1 permissions, such as username and password requirements,
 2 to gain access to a computer. It is likely that when a computer
 3 network generally permits public access to its data, a user's
 4 accessing that publicly available data will not constitute access
 without authorization under the CFAA. The data hiQ seeks to
 access is not owned by LinkedIn and has not been demarcated
 by LinkedIn as private using such an authorization system.

5 Id. at 1003–04. hiQ Labs turned on the fact that the data in question was publicly
 6 available, not owned by LinkedIn, and the servers in question were not protected by
 7 generally applicable access permissions. Those facts are not present here. The
 8 information defendants are alleged to have accessed is private and WhatsApp's servers
 9 are protected from access by generally applicable access permissions.

10 In sum, plaintiffs have stated a claim for violation of 18 U.S.C. § 1030(a)(2) and
 11 (a)(4) under the exceeds authorized access prong.

12 **ii. Harm Based on Access to Users' Devices**

13 Next, defendants argue that, with regard to alleging a claim based on accessing
 14 individual users' devices without authorization, plaintiffs did not suffer a loss as defined
 15 by the CFAA. This argument stems from plaintiffs' allegations that defendants accessed
 16 "Target Devices" (i.e., individual user's devices) without authorization. Compl. ¶¶ 53–54.
 17 As plaintiffs point out, the Ninth Circuit has held that a plaintiff can recover for violation of
 18 the CFAA when a defendant accesses a third party's device as long as the plaintiff is
 19 harmed by such an act, particularly if the plaintiff has a right to data stored on the third
 20 party device. Theofel v. Farey-Jones, 359 F.3d 1066, 1078 (9th Cir. 2004).

21 With respect to harm, "[t]he statute permits a private right of action when a party
 22 has suffered a loss of at least \$5,000 during a one-year period." Power Ventures, 844
 23 F.3d at 1066 (citing 18 U.S.C. § 1030(c)(4)(A)(i)(I)). CFAA defines "loss" as "any
 24 reasonable cost to any victim, including the cost of responding to an offense, conducting
 25 a damage assessment, and restoring the data, program, system, or information to its
 26 condition prior to the offense, and any revenue lost, cost incurred, or other consequential
 27 damages incurred because of interruption of service." § 1030(e)(11).

28 Here, plaintiffs' alleged losses include the expenditure of resources to investigate

1 and remediate defendants' conduct. This type of loss is described by the statute's
 2 reference to "the cost of responding to an offense." 18 U.S.C. § 1030(e)(11).
 3 Defendants do not quarrel with this interpretation but instead contend that plaintiffs' loss
 4 derived from responding to a vulnerability in the WhatsApp system and not to the
 5 accessing of information on individual users' devices. Mtn. at 22. Citing Theofel,
 6 defendants argue that a plaintiff would be injured by a defendant's access to a third
 7 party's device if the plaintiff had rights to data stored on the device. Id.

8 However, as plaintiffs point out, they have alleged rights to at least some data on
 9 users' devices.⁹ Moreover, they have alleged that they incurred costs responding to the
 10 unauthorized access to users' phones by upgrading the WhatsApp system in response to
 11 defendants' intrusion. See Multiven, Inc. v. Cisco Sys., Inc., 725 F. Supp. 2d 887, 895
 12 (N.D. Cal. 2010) ("It is sufficient to show that there has been an impairment to the
 13 integrity of data . . . and the rightful computer owner must take corrective measures "to
 14 prevent the infiltration and gathering of confidential information." (quoting Shurgard
 15 Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126–27 (W.D.
 16 Wash. 2000))). These allegations are sufficient to state a claim for loss based on
 17 responding to an offense on a third party's device.

18 Finally, assuming the court determines that plaintiffs' CFAA § 1030(a)(2) and
 19 (a)(4) claims survive the motion to dismiss, then the conspiracy claim under § 1030(b)
 20 would also survive because the only argument defendants make as to the conspiracy
 21 claim is that plaintiffs cannot state a claim under § 1030(a)(2) or (a)(4).

22 For the foregoing reasons, defendants' motion to dismiss plaintiffs' first cause of
 23 action for violation of the Computer Fraud and Abuse Act is DENIED.

24 **b. Fourth Claim: Trespass to Chattels**

25 "Under California law, trespass to chattels 'lies where an intentional interference
 26

27 _____
 28 ⁹ Plaintiffs assert that the WhatsApp terms of service, which are referenced in the
 complaint, provide for WhatsApp to retain intellectual property rights on a user's device.
 Opp. at 23 (citing Compl. ¶ 19). Defendants do not appear to contest this point.

1 with the possession of personal property has proximately caused injury.” Intel Corp. v.
 2 Hamidi, 30 Cal. 4th 1342, 1350–51 (2003) (emphasis omitted) (quoting Thrifty-Tel, Inc. v.
 3 Bezenek, 46 Cal. App. 4th 1559, 1566 (Ct. App. 1996)). A plaintiff may only recover “the
 4 actual damages suffered by reason of the impairment of the property or the loss of its
 5 use.” Id. (emphasis omitted) (quoting Zaslow v. Kroenert, 29 Cal. 2d 541, 551 (1946)).
 6 To state a trespass to chattels claim, a plaintiff must plead that “(1) the defendant
 7 intentionally and without authorization interfered with plaintiff’s possessory interest in the
 8 computer system; and (2) defendant’s unauthorized use[] proximately caused damage.”
 9 Brodsky v. Apple Inc., — F. Supp. 3d —, No. 19-CV-00712-LHK, 2020 WL 1694363, at
 10 *6 (N.D. Cal. Apr. 7, 2020) (alteration in original) (quoting In re Facebook Internet
 11 Tracking Litig., 263 F. Supp. 3d 836, 842 (N.D. Cal. 2017)).

12 In this case, defendants argue that plaintiffs cannot state a claim for trespass to
 13 chattels because they have not alleged that defendants’ conduct caused actual damage
 14 to plaintiffs’ servers. Mtn. at 23. Defendants contend that plaintiffs’ allegations
 15 concerning investigating and remediation of defendants’ conduct is not harm to their
 16 servers. Id. While plaintiffs allege that the conduct burdened plaintiffs’ computer
 17 network, defendants argue that such an allegation is unsupported by any factual
 18 allegations. Id. at 24. Plaintiffs respond that trespass to chattels includes claims that a
 19 defendant interfered with the intended functioning of a system and defendants have done
 20 so in here. Opp. at 24. Plaintiffs aver that the value of their system is based on their
 21 ability to securely and accurately transmit communications between users and argue that
 22 NSO’s misuse of that system interfered with its intended functioning. Id. Plaintiffs focus
 23 not on the quantity of messages sent but the effect of those messages in impairing the
 24 integrity, quality, and value of WhatsApp’s services. Id. at 25.

25 The leading California case on electronic trespass to chattels is Intel Corp. v.
 26 Hamidi, 30 Cal. 4th at 1347, where the California Supreme Court held that trespass to
 27 chattels “does not encompass . . . an electronic communication that neither damages the
 28 recipient computer system nor impairs its functioning.” In Hamidi, Intel alleged that the

1 defendant used Intel's email system to send six mass email to Intel's employees that
2 criticized Intel's employment practices, urged Intel's employees to find other employment,
3 and other anti-Intel messaging. Id. at 1348–49. The mass emails did not involve the
4 defendant breaching Intel's security and did not damage, slow, or impair Intel's computer
5 system. Id. at 1349. The court reasoned that “the undisputed evidence revealed no
6 actual or threatened damage to Intel's computer hardware or software and no
7 interference with its ordinary and intended operation.” Id. at 1352–53.

8 The following passage from the opinion succinctly summarizes the key issues
9 relevant here:

10 [W]e conclude that under California law the tort does not
11 encompass, and should not be extended to encompass, an
12 electronic communication that neither damages the recipient
13 computer system nor impairs its functioning. Such an
14 electronic communication does not constitute an actionable
15 trespass to personal property, i.e., the computer system,
16 because it does not interfere with the possessor's use or
17 possession of, or any other legally protected interest in, the
18 personal property itself. The consequential economic damage
19 Intel claims to have suffered, i.e., loss of productivity caused by
20 employees reading and reacting to Hamidi's messages and
21 company efforts to block the messages, is not an injury to the
22 company's interest in its computers—which worked as
23 intended and were unharmed by the communications—any
24 more than the personal distress caused by reading an
25 unpleasant letter would be an injury to the recipient's mailbox,
26 or the loss of privacy caused by an intrusive telephone call
27 would be an injury to the recipient's telephone equipment.

28 Id. at 1347 (citations omitted).

21 This case is similar to Hamidi because the alleged actions did not degrade or
22 damage WhatsApp's servers. Nor do plaintiffs advance the argument that approximately
23 1,400 messages out of the 1.5 billion people in 180 countries who use the WhatsApp
24 service (Compl. ¶ 17) impaired the physical functioning of WhatsApp's servers. In fact,
25 defendants' program was reliant on WhatsApp's servers to function exactly as intended.
26 Defendants' program is alleged to emulate legitimate WhatsApp network traffic in order to
27 transmit malicious code, undetected, to a user's device over WhatsApp's servers. Id.
28 ¶ 35.

1 Nonetheless, plaintiffs contend that defendants impaired the value and quality of
 2 WhatsApp’s servers by designing a program that concealed malicious code and made it
 3 appear that WhatsApp, rather than defendants, sent the code. Opp. at 24. This
 4 argument conflates the impairment of the value and quality of WhatsApp’s servers with
 5 the impairment to “the integrity, quality, and value of WhatsApp’s services.” Id. at 25
 6 (emphasis added). Plaintiffs have not alleged that the value of the servers were
 7 degraded as a result defendants’ actions. Instead, they only plead consequential
 8 economic damages, such as the expenditure of resources¹⁰ responding to the breach,
 9 and the loss of goodwill in WhatsApp’s business due to a perceived weakness in
 10 WhatsApp’s encryption or its services. Compl. ¶ 78. Hamidi forecloses consequential
 11 economic damages, 30 Cal. 4th at 1347, and questioned whether the “loss of business
 12 reputation and customer goodwill” is cognizable under an action for trespass to chattels.
 13 Id. at 1358. Arguing that goodwill is cognizable, plaintiffs only cite out of circuit cases that
 14 did not apply Hamidi, Microsoft Corp. v. Does 1–18, No. 13cv139 (LMB/TCB), 2014 WL
 15 1338677, at *10 (E.D. Va. Apr. 2, 2014); CompuServe Inc. v. Cyber Promotions, Inc., 962
 16 F. Supp. 1015, 1023 (S.D. Ohio 1997), but district courts applying Hamidi and addressing
 17 similar financial injuries have found that a financial injury resulting from a trespass to a
 18 computer is not an actual harm actionable, see Hiossen, Inc. v. Kim, No.
 19 CV1601579SJOMRWX, 2016 WL 10987365, at *11 (C.D. Cal. Aug. 17, 2016); Fields v.
 20 Wise Media, LLC, No. C 12-05160 WHA, 2013 WL 5340490, at *4 (N.D. Cal. Sept. 24,
 21 2013).

22 Plaintiffs are correct in pointing out that Hamidi did not explicitly foreclose a
 23 goodwill argument and the court considered such economic injuries as an alternative
 24

25 ¹⁰ In support of harm due to responding to a digital attack, plaintiffs cite Twitich Interactive,
 26 Inc. v. Does 1 Through 100, No. 19-CV-03418-WHO, 2019 WL 3718582, at *4 (N.D. Cal.
 27 Aug. 7, 2019), where the plaintiff asserted that the “defendants’ breach caused it lost
 28 profits and led it to expend resources to combat the attack.” Twitich is not persuasive
 because the court cited that harm in its analysis concerning the plaintiff’s breach of
 contract claim, not its trespass to chattels claim. Further, due to the procedural posture
 of that case, the court did not engage at length with the actual harm argument advanced
 by defendants in this case.

1 argument. 30 Cal. 4th at 1358. The court went on to reject such an argument because
2 the complaint did not concern the functioning of the computer system, but the content of
3 the emails. Id. Even if this court were to follow a similar course and consider plaintiffs'
4 allegations concerning goodwill, plaintiffs have not alleged that they have lost goodwill or
5 customers because of the impairment to WhatsApp's servers as opposed to impairment
6 of WhatsApp's service. Cf. CompuServe Inc., 962 F. Supp. at 1023 ("Many subscribers
7 have terminated their accounts specifically because of the unwanted receipt of bulk e-
8 mail messages. Defendants' intrusions into CompuServe's computer systems, insofar as
9 they harm plaintiff's business reputation and goodwill with its customers, are actionable
10 under Restatement § 218(d).") (emphasis added) (citations omitted)).

11 Finally, plaintiffs cite several cases, including Craigslist Inc. v. 3Taps Inc., 942 F.
12 Supp. 2d 962, 981 (N.D. Cal. 2013), Coupons, Inc. v. Stottlemire, No. CV 07-03457 HRL,
13 2008 WL 3245006, at *6 (N.D. Cal. July 2, 2008), and Thrifty-Tel, 46 Cal. App. 4th at
14 1564, 1566, for the proposition that courts routinely find cognizable injury when the
15 defendant impaired the ability of a plaintiff's equipment to serve customers as intended.
16 Craigslist and Coupons, Inc. only stand for the proposition that whether the defendants
17 caused actual damage or impairment to the computer systems was a question of fact
18 more appropriate for summary judgment or trial than for a motion to dismiss. This point is
19 true, assuming plaintiffs can allege actual harm. Thrifty-Tel, 46 Cal. App. 4th at 1564,
20 involved a computer hack that "den[ied] some subscribers access to phone lines."
21 Plaintiffs in this case have not alleged that any WhatsApp customer was deprived or
22 denied access to the WhatsApp system. The lack of an allegation similar to Thrifty-Tel
23 only reinforces the conclusion that, as currently alleged, the complaint does not detail any
24 actual harm caused by defendants' program or access to WhatsApp's computers or
25 servers.

26 For the foregoing reasons, plaintiffs' fourth cause of action for trespass to chattels
27 is DISMISSED WITH LEAVE TO AMEND.

28 ///

