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

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

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

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

Id. ¶ 22.

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

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

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

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

Between April 29, 2019 and May 10, 2019, defendants caused their malicious code to be transmitted over WhatsApp's servers reaching approximately 1,400 devices used by "attorneys, journalists, human rights activists, political dissidents, diplomats, and other senior foreign government officials." Id. ¶ 42. On May 13, 2019, Facebook announced that it had investigated the vulnerability and WhatsApp and Facebook closed the vulnerability around that time. Id. ¶ 44.

DISCUSSION

A. Legal Standard

1. Rule 12(b)(1)

A federal court may dismiss an action under Federal Rule of Civil Procedure 12(b)(1) for lack of federal subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). Because "[a] federal court is presumed to lack jurisdiction in a particular case unless the contrary affirmatively appears," the burden to prove its existence "rests on the party asserting federal subject matter jurisdiction." Pac. Bell Internet Servs. v. Recording Indus. Ass'n of Am., Inc., No. C03-3560 SI, 2003 WL 22862662, at *3 (N.D. Cal. Nov. 26, 2003) (quoting Gen. Atomic Co. v. United Nuclear Corp., 655 F.2d 968, 969 (9th Cir. 1981); and citing Cal. ex rel. Younger v. Andrus, 608 F.2d 1247, 1249 (9th Cir. 1979)). A jurisdictional challenge may be facial or factual. Safe Air for Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004) (citing White v. Lee, 227 F.3d 1214, 1242 (9th Cir. 2000)). When the attack is facial, the court determines whether the allegations contained in the complaint are sufficient on their face to invoke federal jurisdiction. Id. Where the attack is factual, however, "the court need not presume the truthfulness of the plaintiff's allegations." Id.

When resolving a factual dispute about its federal subject matter jurisdiction, a court may review extrinsic evidence beyond the complaint without converting a motion to dismiss into one for summary judgment. McCarthy v. United States, 850 F.2d 558, 560 (9th Cir. 1988) (holding that a court "may review any evidence, such as affidavits and testimony, to resolve factual disputes concerning the existence of jurisdiction"); see also Land v. Dollar, 330 U.S. 731, 735 n.4 (1947) ("[W]hen a question of the District Court's

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

2. Rule 12(b)(2)

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

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

A court may exercise specific jurisdiction over a defendant if its less-substantial contacts with the forum give rise to the claim or claims pending before the court—that is, if the cause of action "arises out of" or has a substantial connection with that activity. Hanson v. Denckla, 357 U.S. 235, 250–53 (1958); see also Goodyear, 564 U.S. at 924–25. The inquiry into whether a forum state may assert specific jurisdiction over a nonresident defendant focuses on the relationship among the defendant, the forum, and the litigation. Walden v. Fiore, 571 U.S. 277, 283–84 (2014) (citation omitted).

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

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

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

3. Rule 12(b)(6)

A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) tests for the legal sufficiency of the claims alleged in the complaint. Ileto v. Glock Inc., 349 F.3d 1191, 1199–1200 (9th Cir. 2003). Under Federal Rule of Civil Procedure 8, which requires that 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).

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

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

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

4. Rule 12(b)(7)

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

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

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

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

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

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

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

B. Analysis

1. Subject Matter Jurisdiction

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

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

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

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

a. Foreign Official Immunity

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

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

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

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

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

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

[1] Defendants suggest that derivative immunity is grounded in the common law of foreign sovereign immunity and that Butters v. Vance International, Inc., 225 F.3d 462 (4th Cir. 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.

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

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

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

b. Derivative Sovereign Immunity

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

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

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

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

Id.

Plaintiffs argue that the court should not apply Butters because no court in this circuit has extended derivative domestic sovereign immunity to work performed for foreign sovereigns. Opp. at 4. They also argue that Samantar effectively abrogated Butters' holding because Butters cited and relied on the FSIA to extend sovereign immunity to a private entity working for a foreign sovereign. Id. at 6. In response, defendants contend that Butters remains good law and compare the facts here to Yearsley where a contractor's performance was "authorized and directed" by the 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

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

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

---

[2] Other circuits are split on the issue of whether Yearsley constitutes a rule of jurisdictional immunity. Compare Adkisson v. Jacobs Eng'g Grp., Inc., 790 F.3d 641, 647 (6th Cir. 2015) ("Yearsley immunity is, in our opinion, closer in nature to qualified immunity for private individuals under government contract, which is an issue to be reviewed on the merits rather than for jurisdiction." (citing Filarsky v. Delia, 566 U.S. 377, 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.

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

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

2. Personal Jurisdiction

a. Consent

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

[3] In a case cited by defendants, Moriah v. Bank of China Ltd., 107 F. Supp. 3d 272, 277 n.4 (S.D.N.Y. 2015), the district court cited Butters while discussing derivative foreign 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.

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

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

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

> If you are not subject to the "Special Arbitration Provision for United States or Canada Users" section below, you agree that you will resolve any Claim you have with us relating to, arising out of, or in any way in connection with our Terms, us, or our Services (each, a "Dispute," and together, "Disputes") exclusively in the United States District Court for the Northern District of California or a state court located in San Mateo County in California, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such Disputes.

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

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

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

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

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

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

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

b. Specific Jurisdiction

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

i. Purposeful Direction

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

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

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

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

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

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

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

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

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

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

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

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

[4] Plaintiffs request the court judicially notice information from nonparty QuadraNet's website. Dkt. 56. Specifically, plaintiffs request the court notice QuadraNet's terms of service as it appeared on its website on January 29, 2019 and the current version of the terms of service, which became effective March 4, 2020. Id. at 2–3. The request is unopposed. Generally, when considering whether to grant a request for judicial notice, a court may consider factual information from the internet as long as the facts are not 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.

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

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

> [d]efendants worked for a company whose principal place of business in Seattle, Washington, a fact that they had knowledge of, as Defendants attest that Blaine interviewed for his job there and Kumar had his initial training there. [The 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.

Id. at *2 (citation omitted).

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

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

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

[6] Defendants would distinguish Seattle Sperm Bank on the grounds that the plaintiff in that case intentionally stole data from the servers, which defendants are not alleged to 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.

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

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

[7] While Walden reaffirmed that a defendant's conduct remains the touchstone of specific jurisdiction, the Court expressly reserved deciding the amount of minimum contacts "where intentional torts are committed via the Internet or other electronic means (e.g., fraudulent access of financial accounts or 'phishing' schemes)." Walden, 571 U.S. at 290 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.

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

The third element of the Calder effects test is whether the defendants caused harm that they knew would likely be suffered in the forum state. Defendants do not offer any argument as to this element. Plaintiffs have alleged that defendants harmed them by interfering with the WhatsApp service and burdening their network and have injured plaintiffs' reputation, public trust, and goodwill. Compl. ¶¶ 46–47. If defendants did access plaintiffs' servers without authorization (or exceeded authorized access), then they would have known they were harming plaintiffs. See id., Ex. 10 at 33 (product description naming Facebook and WhatsApp as applications to be monitored). Defendants also knew that such harm would be suffered in California; for example, the Hulio declaration states that Facebook contacted NSO to inquire about certain capabilities of Pegasus, indicating that defendants were well aware of plaintiffs and their principal place of business in California. Hulio Decl. ¶ 10. Therefore, plaintiffs have demonstrated the purposeful direction element of specific jurisdiction. For that reason, the court does not reach plaintiffs' argument that the court has jurisdiction under Rule 4(k)(2).

ii. Purposeful Availment

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

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

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

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

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

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

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

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

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

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

iii. Reasonableness and Pendent Jurisdiction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Failure to Join Necessary Parties

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

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

---

[8] The court uses the term "pendent personal jurisdiction" to distinguish the concept from the supplemental jurisdiction statute, 28 U.S.C. § 1367. As explained by a leading treatise:

> In recent years, there has been some debate about whether Section 1367 of Title 28, the supplemental jurisdiction statute, should be read to include the doctrine of pendent personal jurisdiction. Neither the plain meaning of this statute, which shows it to be a subject matter jurisdiction provision, nor its legislative history supports the conclusion that Congress 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).

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

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

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

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

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

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

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

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

4. Failure to State a Claim

a. First Claim: CFAA

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

i. WhatsApp's Servers

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

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

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

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

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

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

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

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

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

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

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

> it appears that the CFAA's prohibition on accessing a computer "without authorization" is violated when a person circumvents a computer's generally applicable rules regarding access

> permissions, such as username and password requirements, to gain access to a computer. It is likely that when a computer network generally permits public access to its data, a user's 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.

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

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

ii. Harm Based on Access to Users' Devices

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

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

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

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

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

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

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

b. Fourth Claim: Trespass to Chattels

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

[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.

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

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

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

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

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

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

Id. at 1347 (citations omitted).

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

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

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

[10] In support of harm due to responding to a digital attack, plaintiffs cite Twitch Interactive, Inc. v. Does 1 Through 100, No. 19-CV-03418-WHO, 2019 WL 3718582, at *4 (N.D. Cal. Aug. 7, 2019), where the plaintiff asserted that the "defendants' breach caused it lost profits and led it to expend resources to combat the attack." Twitch 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.

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

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

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

/ / /

5. Motion to Stay Discovery

While the present motion to dismiss was pending, defendants subsequently filed a motion to stay discovery pending final resolution of their motion to dismiss. Dkt. 95. Defendants argue that because their motion is based in part on a foreign sovereign immunity argument, they should be free from all burdens of litigation. Id. at 2. They also argue that good cause exists to stay discovery pending disposition of the motion beyond the sovereign immunity argument. Id. at 3–4.

Defendants advance no reason to stay discovery other than the pending motion to dismiss. Because this order adjudicates their pending motion, defendants' request to stay discovery is moot. Accordingly, the court DENIES AS MOOT defendants' motion to stay discovery.

CONCLUSION

For the foregoing reasons, the court GRANTS defendants' Rule 12(b)(6) motion to dismiss plaintiffs' fourth cause of action for trespass to chattels but DENIES their motion in all other respects. The court further DENIES AS MOOT defendants' motion to stay discovery. Because plaintiffs have not alleged actual harm, the court is skeptical that the fourth cause of action can be amended to state a claim. That said, it is not clear that amendment would be futile. Plaintiffs shall file any amended complaint within 21 days of the date of this order to amend only the fourth cause of action. No new parties or causes of action may be pleaded without leave of court or the agreement of defendants. Upon the filing of any amended complaint, plaintiffs must also file a redline clearly demarcating their changes from the existing complaint.

IT IS SO ORDERED.

Dated: July 16, 2020

/s/ Phyllis J. Hamilton
PHYLLIS J. HAMILTON
United States District Judge