JOSEPH N. AKROTIRIANAKIS (Bar No. 197971)
jakro@kslaw.com
AARON S. CRAIG (Bar No. 204741)
acraig@kslaw.com
KING & SPALDING LLP
633 West Fifth Street, Suite 1700
Los Angeles, CA 90071
Telephone: (213) 443-4355
Facsimile: (213) 443-4310

Attorneys for Defendants
NSO GROUP TECHS. LTD. and Q CYBER TECHS. LTD.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

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

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No. 4:19-cv-07123-PJH

DEFENDANTS' NOTICE OF MOTION AND MOTION TO DISMISS OR FOR SUMMARY JUDGMENT FOR LACK OF PERSONAL JURISDICTION AND FOR PARTIAL SUMMARY JUDGMENT; POINTS AND AUTHORITIES

Date: November 1, 2024
Time: 1:30 p.m.
Place: Courtroom 3, Ronald V. Dellums Federal Building & U.S. Courthouse, 1301 Clay Street, Oakland, California

Action Filed: 10/29/2019

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

PLEASE TAKE NOTICE that on November 1, 2024, at 1:30 p.m., Defendants NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. (collectively "NSO") will bring on for hearing before the Honorable Phyllis J. Hamilton, United States District Judge, in the United States Courthouse, 1301 Clay Street, Courtroom 3, Oakland, California, a motion to dismiss or for summary judgment for lack of personal jurisdiction and for partial summary judgment. The motion is based on the following Points and Authorities; the Declarations of Yaron Shohat, Terrence McGraw, and Joseph N. Akrotirianakis (and the exhibits to those Declarations); the pleadings, papers, and records on file in this case; and such oral argument as may be presented.

First, NSO moves to dismiss under Rule 12(b)(2), or for summary judgment under Rule 56, because the Court lacks personal jurisdiction over NSO. Courts have treated such motions both as motions for summary judgment, *Stoliarov v. Marshmello Creative, LLC*, 2021 WL 1781870 (C.D. Cal. Apr. 7, 2021), and as motions to dismiss, *Kiwijet, LLC v. Mena Technics Co.*, 2022 WL 20401312 (C.D. Cal. Dec. 16, 2022).[1] However the Court characterizes this motion, it should "make any necessary factual findings and decide the jurisdictional issue" as a matter of law. *Berardinelli v. Castle & Cooke Inc.*, 587 F.2d 37, 39 (9th Cir. 1978). ***Second***, NSO moves for partial summary judgment under Rule 56 on: (1) all of Plaintiffs' claims based on the *use* of Pegasus; (2) Plaintiffs' Computer Fraud and Abuse Act ("CFAA") claim; and (3) Plaintiffs' California Comprehensive Computer Data Access and Fraud Act ("CDAFA") claim.

POINTS AND AUTHORITIES

Plaintiffs' claims challenge actions Israeli corporations took in Israel to design a technology licensed to foreign governments to use to investigate foreign crimes. The only connection this case has to California (or even the United States) is that Plaintiffs, like nearly every other large tech company, placed their headquarters in the Bay Area. For that reason, California has never had any basis to exercise personal jurisdiction over NSO. To argue otherwise, Plaintiffs told this Court that NSO's "Pegasus" technology "*sought out specific* [WhatsApp] servers—including servers *in California*—in order to transmit malicious code through those servers." (Dkt. 111 at 22 (emphases

[1] When a defendant moves to dismiss pre-trial for lack of personal jurisdiction, "the mode of [the motion's] determination is left to the trial court." *Data Disc, Inc. v. Sys. Tech. Assocs., Inc.*, 557 F.2d 1280, 1285 (9th Cir. 1977).

added).) The Court denied NSO's motion to dismiss and allowed this action to proceed on the basis of that assertion. But that assertion was false. And instead of correcting it, Plaintiffs have engaged in an abusive fishing expedition—plumbing NSO's most sensitive documents for something, *anything*, that could tie NSO to California. They found nothing.

So now, after more than four and a half years, the record proves what Plaintiffs must have known all along: NSO did not and could not target *any* specific WhatsApp server, much less servers in California. Almost none of WhatsApp's servers were even in California. And wherever they were, neither NSO nor its government customers targeted any server based on its location. Nor could they have—*WhatsApp* alone chose which servers would handle Pegasus messages. So if WhatsApp's own decisions about how to design its system caused any Pegasus message to pass through servers in California, that reflected Plaintiffs' "unilateral activity," which cannot support jurisdiction over NSO. *Walden v. Fiore*, 571 U.S. 277, 286 (2014). Plaintiffs cannot identify any other proper basis for personal jurisdiction over NSO. Therefore, the Court should dismiss all of Plaintiffs' claims for lack of personal jurisdiction.

NSO is also entitled to partial summary judgment on the merits of most claims. ***First***, NSO is entitled to summary judgment on all of Plaintiffs' claims to the extent they rest on the *use* of Pegasus to monitor WhatsApp *users'* devices. NSO *never* operated Pegasus on any nonconsenting WhatsApp user's device. Only NSO's government customers did so, and Plaintiffs have no evidence otherwise. Moreover, the "act of state" doctrine bars Plaintiffs from "question[ing] the legality" of a foreign government's "sovereign act" of using Pegasus. *IAM v. OPEC*, 649 F.2d 1354, 1359 (9th Cir. 1981). ***Second***, NSO is entitled to summary judgment on Plaintiffs' claim under the Computer Fraud and Abuse Act ("CFAA"). This Court already held that Plaintiffs cannot pursue a claim under CFAA's "without authorization" prong (Dkt. 111 at 37), and there is no basis for Plaintiffs to revive that claim now. Nor can Plaintiffs pursue a claim under CFAA's "exceeds authorized access" prong, because NSO never "obtain[ed] or alter[ed] information in" WhatsApp's servers that it was "not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). And in all events, Plaintiffs cannot challenge any of NSO's research and development ("R&D") for Pegasus after December 2018 because it was authorized by the FBI, a "law enforcement agency of the United

States." *Id.* § 1030(f). ***Third***, NSO is entitled to summary judgment on Plaintiffs' claim under the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"). CDAFA does not apply to conduct outside of California, and Plaintiffs have no evidence that NSO took any actions prohibited by CDAFA within California.

Background

A. NSO's business. NSO is an Israeli technology company that designs and markets to government agencies a highly regulated technology only for use in investigating crimes and terrorism. (Shohat Decl. ¶¶ 3-4.) This case involves an NSO product called "Pegasus." NSO licenses Pegasus exclusively to select government agencies approved by the Government of Israel, never to any private customer. (Shohat Decl. ¶ 9; Akro. Exh. H at 138:12-15; Akro. Exh. I at 93:13-19.)[2]

A Pegasus license includes a year of "support[] and maintenance," including software updates and "new[] versions" of Pegasus. (Shohat Exhs. A & B at 9, 14-15.) Maintaining and updating Pegasus requires continuous R&D. (Shohat Decl. ¶ 15; Akro. Exh. H at 104:3-13.) NSO, however, *never operates* Pegasus—only its government customers may do so. (Shohat Decl. ¶¶ 14-16, Exh. A ¶ 2.4, Exh. B ¶ 2.4; Akro. Exh. H at 234:8-236:10, Exh. I at 316:11-317:2.) NSO requires its government customers to agree that they will (1) "fully comply with all privacy and national security related laws and regulations, international standards, and any other laws and regulations that are applicable to the use of [Pegasus], including by way of obtaining all judicial warrants . . . to the extent required by law," (2) use Pegasus "only for the prevention and investigation of crimes and terrorism and ensure that [Pegasus] will not be used for human rights violations," and (3) "immediately notify" NSO of any "misuse or potential misuse." (Shohat Exh. A ¶ 18.5, Exh. B ¶ 19.5.) NSO can suspend or terminate service to customers that misuse its technology, and it has done so. (Shohat Decl. ¶ 12; Akro. Exh. H at 21:16-25, 26:23-31:17, 181:10-15.)

NSO has no presence or operations in the United States. (Shohat Decl. ¶ 4; Akro. Exh. H at 87:14-89:1.) In the past, an independent Delaware company called Westbridge Technologies

[2] Israel strictly regulates Pegasus and must approve each request for a license. (Shohat Decl. ¶¶ 5-7.) Israel requires NSO's government customers to execute end-use certificates on a government-to-government basis, promising to use Pegasus only for the "[c]ollection of data from mobile devices for the prevention and investigation of crimes and terrorism, in compliance with privacy and national security laws." (Akro. Exh. N; Shohat Decl. ¶ 6.)

Inc. marketed NSO's products to potential U.S. government customers. Westbridge was within the same broad corporate family as NSO and Q Cyber but was not a parent or subsidiary of either entity. (Shohat Exh. C; Akro. Exh. H at 81:9-14; Akro. Exh. G at 123:5-14.) NSO's and Westbridge's interactions were governed by a contract that identified Westbridge as "an independent contractor" rather than an "agen[t]." (Shohat Exh. D ¶ 12.) NSO did not control or direct any of Westbridge's marketing efforts. (Akro. Exh. G at 155:14-20, 287:4-17, 290:2-7, Exh. J at 288:9-293:1, 314:14-315:5, 333:7-12, Exh. H at 140:6-141:6; Shohat Decl. ¶ 20.) Westbridge had its own operations, employees, executives, offices, bank accounts, and other corporate formalities. (Akro. Exh. G at 84:20-21, 270:2-271:14, 272:17-275:14, Exh. J at 32:6-33:21, 273:6-277:19; Shohat Decl. ¶ 20.) NSO was not Westbridge's "exclusive" supplier (Shohat Exh. D ¶ 2.1), and Westbridge also marketed products designed by a separate company called CS Circles Solutions Ltd. (Shohat Exh. E at 8; Akro. Exh. G at 158:16-159:10, 242:15-243:8).

Westbridge's marketing efforts for Pegasus were largely unsuccessful. (Akro. Exh. G at 177:2-13; Akro. Exh. J at 64:22-25.) In 2016 Westbridge unsuccessfully marketed Pegasus to a few local law-enforcement agencies in California. (Akro. Exh. J at 211:4-10, 318:22-319:5.) Westbridge alone made the decision to market to these agencies, with no input from NSO. (Akro. Exh. J at 288:9-290:24, 315:2-5.) No California entity ever licensed Pegasus. (Akro. Exh. G at 236:16-22.) Westbridge did successfully market Pegasus to the FBI in December 2018. (Akro. Exh. G at 264:7-18, Exh. O.) The FBI purchased a Pegasus license, which required NSO to provide continuous "maintenance" and updates. (Akro. Exh. N, Exh. G at 332:3-333:21.)

B. NSO's Pegasus technology. Pegasus includes (1) an "agent" designed to reside on a target device and collect information from that device, and (2) various delivery mechanisms (or "vectors") for delivering the agent to target devices. (McGraw Decl. ¶¶ 38, 45; Akro. Exh. I at 30:7-23, 42:23-43:5.) The Pegasus "agent" cannot function on any device that is in the United States or has a U.S. phone number. (Shohat Decl. ¶ 13; Akro. Exh. I at 316:3-7, 327:11-328:14.)

Between April 2018 and May 2020, NSO licensed three delivery "vectors" for the Pegasus agent—known as "Heaven," "Eden," and "Erised," and collectively as "Hummingbird"—that

operated by messaging target devices through WhatsApp. (Akro. Exh. I at 67:15-24.)[3] All three vectors used WhatsApp to send messages to target devices that, if successful, would cause the target devices to download the Pegasus agent from a third-party "payload server" controlled by Pegasus's government operator. (McGraw Decl. ¶¶ 30-39.) As Plaintiffs admitted, "WhatsApp servers were not compromised by" the vectors' use of the WhatsApp service to send WhatsApp messages. (Akro. Exh. P at 4.) Pegasus did not damage, alter, or impair WhatsApp's servers or the servers' code in any way. (McGraw Decl. ¶¶ 80-85; Akro. Exh. L at 183:1-184:7.) Nor had NSO "introduce[d]" any "vulnerability into [WhatsApp's] code base." (Akro. Exh. K at 200:25-201:10.) The messages Pegasus sent simply traveled through WhatsApp servers like any other WhatsApp message would have—akin to mail sent through the postal service. (McGraw Decl. ¶ 74).

Due to how WhatsApp designed its own infrastructure, WhatsApp messages sent by any WhatsApp user, including a governmental Pegasus operator, passed through "signaling" and "relay" servers controlled by WhatsApp. (*Id.* ¶¶ 20-28, 41-54.) WhatsApp alone, not NSO or its government customers, chose how to route messages Pegasus sent over WhatsApp's servers. (*Id.*)

Signaling Servers. WhatsApp signaling servers (also called "chatd" servers) create the initial connection between two callers. (McGraw Decl. ¶ 20.) In 2019, all of WhatsApp's signaling servers were in data centers in Iowa, Oregon, and North Carolina. (Akro. Exh. L at 184:21-185:9.) When any WhatsApp user, including a governmental Pegasus operator, initiated a WhatsApp call, WhatsApp sent a call request to a domain name identified solely as "chat.whatsapp.com." (Akro. Exh. L at 86:1-19.) At that point, WhatsApp unilaterally chose the signaling server that would be involved in the call. (McGraw Decl. ¶ 21; Akro. Exh. L at 89:4-90:6, 96:25-98:16, 102:4-104:15, 129:15-20.) WhatsApp chose the signaling server according to its own internal algorithms, to balance server loads across its infrastructure. (*Id.*)

Relay Servers. WhatsApp's relay servers convey audio and video data during a call. (McGraw Decl. ¶¶ 14, 26.) In 2019, WhatsApp's relay servers were located in over 100 "edge locations" worldwide, only two of which were in California. (Akro. Exh. L at 82:15-17, 132:22-133:10.)

[3] NSO does not now have any "installation vector for Pegasus . . . that uses [Plaintiffs'] technology in any way." (Akro. Exh. H at 51:23-52:3.)

WhatsApp's "signaling server is the one that actually pick[ed] the relay servers involved in [a] call," using an algorithm designed by WhatsApp. (Akro. Exh. L at 81:17-82:21.) The signaling server picked the relay servers for any call (including calls initiated with Pegasus) by generating a short list of URLs associated with the relay servers that WhatsApp's algorithm determined had the best performance. (Akro. Exh. L at 117:21-121:20; McGraw Decl. ¶¶ 28, 47.) The signaling server then provided callers (including Pegasus users) "tokens" authorizing them to access those relay servers; as Plaintiffs' corporate designee testified, "as long as you have a valid token, you can use the relay." (Akro. Exh. L at 118:19-119:25; McGraw Decl. ¶¶ 28, 47.) The WhatsApp application would then reach out to those URLs, and WhatsApp would again decide which relay servers to use based on an algorithmic assessment of server performance. (Akro. Exh. L at 120:1-121:2, Exh. I at 319:7-19; McGraw Decl. ¶¶ 28, 50.) Just like the WhatsApp application, the Eden and Erised installation vectors used whichever relay server happened to have the best performance, without considering the server's location. (McGraw Decl. ¶¶ 48-54; Akro. Exh. I at 323:9-325:22.)[4] Thus, it was always WhatsApp that chose the servers any message Pegasus sent was passed through.

As designed, *every message* Pegasus sent through WhatsApp servers complied fully with every technical requirement imposed by those servers—otherwise, the servers would have rejected the message. (McGraw Decl. ¶¶ 65-79.) Pegasus did not execute any foreign code on the WhatsApp servers or introduce any vulnerability into WhatsApp's code. (*Id.* ¶¶ 34, 37, 39, 69; Akro. Exh. K at 200:25-201:10, 202:10-18.) Nor did Pegasus access any server information that was off-limits to any other WhatsApp user, let alone breach any code-based access barriers protecting such information. (McGraw Decl. ¶¶ 65-79.) Pegasus merely invoked messaging functions that WhatsApp servers made available to it (*id.* ¶¶ 39, 65-79), and thus accessed only those parts of the server that WhatsApp programmed those functions to access (Akro. Exh. L at 129:15-130:23). The only difference between Pegasus's use of servers and other WhatsApp users' use of the same servers was the *content* of the messages Pegasus passed through them. Plaintiffs may not have liked the content of those messages, but they were not prohibited by anything in WhatsApp's server code. (McGraw Decl. ¶ 67.)

[4] Heaven did not use WhatsApp relay servers at all. (McGraw Decl. ¶ 45; Akro. Exh. I at 258:17-260:2.)

C. The Court's motion to dismiss order. Plaintiffs filed their complaint in October 2019. NSO moved to dismiss on multiple grounds, including that it is not subject to personal jurisdiction in California and that Plaintiffs did not plead a CFAA violation. In opposing NSO's personal jurisdiction argument, Plaintiffs argued (among other things) that NSO (1) targeted California by using third-party servers located there and (2) deliberately "sought out specific [WhatsApp signaling and relay] servers . . . in California." (Dkt. 111 at 21-22.) With respect to third-party servers, Plaintiffs submitted declarations asserting that Pegasus's code "included" the "IP address of a remote server" to which Pegasus "cause[d] a WhatsApp user's mobile device to connect." (Dkt. 55-2 ¶ 3.) Plaintiffs said this IP address "was located in Los Angeles, California." (Dkt. 55-6 ¶ 2.)

This Court denied NSO's motion in part. As to personal jurisdiction, the Court held that any use of third-party servers in California could not create personal jurisdiction. (Dkt. 111 at 20-21.) But the Court found that Plaintiffs had adequately alleged that NSO specifically "*sought out* WhatsApp's California-based servers," which was sufficient to support personal jurisdiction at the pleadings stage. (*Id.* at 24.) Discovery has proven false Plaintiffs' allegations about WhatsApp's California-based servers.[5] As to CFAA, the Court held Plaintiffs had *not* stated a claim under CFAA's "without authorization" prong because WhatsApp's TOS "authorized" NSO "to send messages using the WhatsApp app." (*Id.* at 37.) The Court found that Plaintiffs had adequately pleaded a violation of CFAA's "exceeds authorized access" prong by alleging that NSO "evad[ed] WhatsApp's securities features" to "access a portion" of WhatsApp's servers that NSO "did not have permission to access." (*Id.* at 37-38.) Discovery has proven that allegation untrue as well.

Argument

The Court should dismiss Plaintiffs' claims. Plaintiffs cannot meet their burden of proving NSO is subject to personal jurisdiction in California. Although this Court held at the motion to dismiss stage that Plaintiffs had adequately *pleaded* jurisdictional facts, the Court's ruling depended

[5] It seems clear that Plaintiffs must have known, when they filed their complaint, that none of WhatsApp's signaling servers were in California and that WhatsApp's servers were configured so that users could not direct messages to any particular relay server. Plaintiffs' failure to correct the false impression their allegations created is consistent with other of their conduct in this litigation. (*E.g.*, Dkt. 377.) The Court need not find that Plaintiffs acted deliberately, however; it need only conclude Plaintiffs have not proven the truth of their allegations.

on an untrue allegation—that NSO deliberately "sought out specific [WhatsApp] servers" in California (Dkt. 111 at 22). Plaintiffs then conducted a yearslong fishing expedition that confirmed, contrary to Plaintiffs' allegations, that NSO did not and could not purposefully target any California-based WhatsApp servers. Because Plaintiffs cannot prove NSO purposefully directed its alleged conduct at California servers, their primary theory of personal jurisdiction collapses. Their backup theories fare no better. This Court thus lacks personal jurisdiction over NSO.

The Court need go no further to adjudicate this case. But if the Court chooses to address issues beyond jurisdiction, it should also grant NSO partial summary judgment on: (1) all claims based on the *use* of Pegasus by NSO's customers, because Plaintiffs cannot attribute that conduct to NSO and the act of state doctrine bars any such claim; (2) Plaintiffs' CFAA claim, because they cannot prove that NSO accessed WhatsApp's servers "without authorization" or in a way that "exceed[ed] authorized access," and NSO's R&D after December 2018 was all "lawfully authorized investigative, protective, or intelligence activity" of the FBI, 18 U.S.C. § 1030(a)(2), (f); and (3) Plaintiffs' CDAFA claim, because they cannot prove NSO targeted any California computer.

I. Plaintiffs cannot prove that NSO is subject to personal jurisdiction in California.

Plaintiffs "bear the burden" to prove that the Court may exercise personal jurisdiction over NSO at all stages of the case, including "on [a] motion for summary judgment." *Vista v. USPlabs, LLC*, 2014 WL 5507648, at *4 (N.D. Cal. Oct. 30, 2014); *see Data Disc, Inc. v. Sys. Tech. Assocs., Inc.*, 557 F.2d 1280, 1289 n.6 (9th Cir. 1977). Plaintiffs must "prov[e] jurisdiction by a preponderance of the evidence." *Stoliarov, LLC*, 2021 WL 1781870, at *2 n.3; *see Haisten v. Grass Valley Med. Reimb. Fund, Ltd.*, 784 F.2d 1392, 1396 n.1 (9th Cir. 1986). Because Plaintiffs cannot do so, the Court should dismiss their claims.

As a matter of federal due process, personal jurisdiction exists only if NSO's contacts with California support either general or specific personal jurisdiction. *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 801-02 (9th Cir. 2004). Plaintiffs have never argued that NSO, an Israeli corporation, is subject to general jurisdiction in California. *Daimler AG v. Bauman*, 571 U.S. 117, 137 (2014). Therefore, Plaintiffs must prove *specific* jurisdiction by proving that NSO "either 'purposefully direct[ed] [its] activities' toward the forum or 'purposefully avail[ed] [it]self of the

privileges of conducting activities in the forum.'" *Axiom Foods, Inc. v. Acerchem Int'l, Inc.*, 874 F.3d 1064, 1068 (9th Cir. 2017). The "purposeful direction analysis" applies in cases, like this one, based on allegations that a defendant "engaged in tortious conduct from a location outside of the United States by remotely accessing servers located in the United States." *Hungerstation LLC v. Fast Choice LLC*, 857 F. App'x 349, 351 (9th Cir. 2021).[6]

A. NSO did not purposefully direct any case-related conduct toward California.

To satisfy the purposeful direction test, also known as the "effects" test, Plaintiffs must prove that NSO "expressly aimed" case-related conduct "at the forum state." *Axiom Foods*, 874 F.3d at 1069 (cleaned up). This analysis focuses on "the defendant's contacts with the forum State itself, not the defendant's contacts with persons who reside there." *Walden*, 571 U.S. at 285. "Due process requires that a defendant be haled into court in a forum State based on his own affiliation with the State, not based on the 'random, fortuitous, or attenuated' contacts he makes by interacting with other persons affiliated with the State." *Id.* at 286. So Plaintiffs may not establish personal jurisdiction simply by claiming that NSO targeted *them*—they must prove that NSO targeted *California*. *Id.*; *Axiom Foods*, 874 F.3d at 1069-70; (Dkt. 111 at 24). They cannot do so.

1. NSO did not target WhatsApp's California servers.

At the motion to dismiss stage, this Court found Plaintiffs had adequately pleaded specific jurisdiction by alleging that NSO "sought out specific [WhatsApp] servers—including servers in California—in order to transmit malicious code through those servers." (Dkt. 111 at 22.) But discovery has exposed that allegation as false. The undisputed record proves that NSO did not *and could not* target specific WhatsApp signaling or relay servers anywhere, much less in California.

First, NSO could not have targeted WhatsApp signaling servers in California because *there were no* WhatsApp signaling servers in California. At the relevant times, all of WhatsApp's signaling servers were in Oregon, Iowa, or North Carolina. (Akro. Exh. L at 184:21-185:9.)

Second, NSO did not purposefully use California relay servers as opposed to servers located anywhere else. At the relevant times, WhatsApp had "a very large number" of relay servers

[6] This Court previously held Plaintiffs could not establish purposeful availment (Dkt. 111 at 26-27), and Plaintiffs have no evidence supporting a different conclusion now.

"geographically distributed" across more than 100 locations worldwide, only two of which were in California. (Akro. Exh. L at 82:15-17, 134:11-19.) And which relay server any particular WhatsApp call passes through was *entirely up to WhatsApp*. The WhatsApp signaling server generated a small list of available relay servers, based on an algorithm *WhatsApp* designed to select servers based on server traffic. (Akro. Exh. L at 119:3-121:2.) That list identified relay servers through URL addresses, which WhatsApp in its sole discretion routed to servers that could change over time. (McGraw Decl. ¶¶ 47, 51-52.) A WhatsApp user had no advance knowledge of or control over which relay servers the signaling server chose; the "signaling server is the one that actually picks the relay servers involved in the call." (Akro. Exh. L at 82:3-5.) And once the signaling server created the list of relay servers, the WhatsApp *application*—not any user—chose which relay server to use, again based solely on an algorithmic assessment of server performance. (Akro. Exh. L at 82:3-21, 120:21-122:20; McGraw Decl. ¶¶ 28, 50.)

Pegasus worked the same way. (McGraw Decl. ¶¶ 48-54.) Because WhatsApp's own signaling servers generate the list of URLs for available relay servers based on WhatsApp's own algorithm, Pegasus *could not* control which relay servers a signaling server chose, much less specifically target California servers. (*Id*. ¶¶ 50-52.) And once the signaling server generated the list of URLs, nothing in Pegasus directed calls to the URLs associated with California relay servers as opposed to relay servers anywhere else in the world. (*Id*.) To the contrary, Plaintiffs' own evidence shows that Pegasus used whichever WhatApp relay servers happened to have the best performance, exactly as the WhatsApp application did. (*Id*.) That makes perfect sense: NSO's only motivation would be to use whichever servers would perform best, without regard to location. (McGraw Decl. ¶¶ 43, 48, 53.) A server's presence in California could not have made any difference to NSO (Akro. Exh. I at 325:9-22), and Plaintiffs have no evidence suggesting otherwise.

These undisputed facts confirm that NSO did *not* "s[eek] out WhatsApp's California-based servers," as Plaintiffs falsely told the Court. (Dkt. 111 at 24.) When NSO designed Pegasus, and when NSO's government customers used Pegasus, they did not direct their actions toward any particular WhatsApp server, much less specific servers in California. Rather, the identity and location of WhatsApp servers accessed by NSO or a Pegasus user were due *entirely* to WhatsApp's

own decisions. In these circumstances, where "there is no . . . evidence that the defendants played any role in selecting the server's location," a "server's location" cannot "establish personal jurisdiction." *GreatFence.com, Inc. v. Bailey*, 726 F. App'x 260, 261 (5th Cir. 2018).

That is true even when the defendant is accused of accessing the plaintiff's own servers. As long as a defendant, like NSO, has no control over where the plaintiff's servers are located and does not purposefully target specific servers based on their location, the servers' location is due entirely to the plaintiff's own "unilateral activity," *Walden*, 571 U.S. at 286 (cleaned up), and is thus too "'random,' 'fortuitous,' [and] 'attenuated'" to support specific jurisdiction, *Broidy Cap. Mgmt., LLC v. Qatar*, 2018 WL 9943551, at *7 (C.D. Cal. Aug. 22, 2018); *Karp v. Buchem*, 2018 WL 4944995, at *3 (C.D. Cal. Mar. 23, 2018).[7]

Here too, the California location of a tiny minority of WhatsApp's relay servers is purely "fortuitous" and does not show that NSO purposefully directed any conduct toward California. To the extent that NSO or its customers ever sent a message that passed through a California-based relay server, that was not because of any decision *by NSO*. It was because *WhatsApp* designed its own system in a way that just happened to choose to use a California server for the message at issue. Such "'unilateral activity' of a plaintiff" cannot support specific jurisdiction over NSO in California. *Walden*, 571 U.S. at 286.

2. NSO's alleged use of third-party servers cannot support jurisdiction.

In this Court's motion to dismiss order, the Court rejected Plaintiffs' argument that NSO "expressly aimed [its] conduct at [California]" by allegedly "leas[ing] third-party servers" there. (Dkt. 111 at 20-21.) Despite that ruling, Plaintiffs appear to continue to argue that NSO targeted California by leasing third-party servers that other companies decided to place in California. But the evidence does not support the assertion that NSO used any California-based third-party servers,

[7] *See also Hungerstation*, 857 F. App'x at 351 (defendant's access to plaintiff's data on U.S. servers did not support jurisdiction because "the location of the servers was fortuitous"); *X Corp. v. Ctr. for Countering Digital Hate Ltd.*, 2024 WL 1245993, at *10 (same, when "there [was] no support for the notion that [defendant] specifically sought out any particular servers within the forum"); *Guar. Rate, Inc. v. Conn*, 264 F. Supp. 3d 909, 921-22 (N.D. Ill. 2017) (access to plaintiff's servers inadequate because the "role [the] servers play in [plaintiff's] network is the result of conduct by [plaintiff]"); *cf. Hasson v. FullStory, Inc.*, 114 F.4th 181, 191 (3d Cir. 2024) ("transmitting computer code to a browser that happens to be in [the forum]" is not "sufficient to establish express aiming").

and even if it did, "'the mere location of a third party or its servers is insufficient to give rise to personal jurisdiction.'" (Dkt. 111 at 21 (quoting *Hungerstation LLC v. Fast Choice LLC*, 2020 WL 137160, at *5 (N.D. Cal. Jan. 13, 2020), *aff'd*, 857 F. App'x 349).)

Plaintiffs contend that each installation of Pegasus was configured to instruct the target device to download certain information from one of 38 third-party IP addresses. (Dkt. 55-2; McGraw Decl. ¶ 56.) Plaintiffs contend that *one* of those IP addresses was registered to a company called QuadraNet, which listed its address as being in Los Angeles, California. (*Id.*) Plaintiffs infer from QuadraNet's location that the QuadraNet *server* was located in California.

As a factual matter, that conclusion does not follow. The IP address's supposed association with California means only that the server *owner* (QuadraNet) is based in California, not that the physical *server* is in California. (McGraw Decl. ¶¶ 60-61.) Cloud providers and web hosts often use *virtual* IP addresses, which do not relate to any specific piece of hardware.[8] (*Id.*) Requests to the address can be routed to any one of numerous servers in any number of locations. (*Id.*) For example, Google has a single virtual IP address that routes communications to hundreds of servers around the world. (*Id.*) WhatsApp similarly uses virtual IP addresses that are not associated with any particular physical server. (*Id.* ¶¶ 21, 42, 52; Akro. Exh. L at 91:25-92:25.) For that reason, Plaintiffs cannot prove the QuadraNet IP address was associated with an actual server in California. (*See* Akro. Exh. L at 203:22-205:20.) That alone dooms Plaintiffs' argument.[9]

Even if Plaintiffs could prove that one QuadraNet server was in California, this Court already held that would not support specific jurisdiction over NSO. (Dkt. 111 at 20-21.) In opposition to NSO's motion to dismiss, Plaintiffs submitted the same evidence on which they now appear to rely. They submitted a declaration that Pegasus "was designed to cause a WhatsApp user's mobile device

[8] This is also why Plaintiffs initially thought there were two third-party servers in the United States: the QuadraNet server and the AWS server that has been the subject of much motion practice in this case. (Akro. Exh. W at 3.) Plaintiffs have subsequently acknowledged that they were mistaken as to the AWS server, which was located in Germany. (Dkt. No. 331 at 1:21-22.)

[9] *42 Ventures, LLC v. Mav*, 2021 WL 5985018, at *1 (9th Cir. Dec. 16, 2021) (third-party servers could not support personal jurisdiction when plaintiff "did not allege that the servers were in fact located in the United States, as opposed to merely operated by U.S.-based companies"); *Freeman v. 3Commas Techs. OU*, 2024 WL 1880147, at *2 (N.D. Cal. Mar. 25, 2024) (same, where it was "not clear whether . . . the data server provider is located in California, or the server itself is located in California").

to connect to" the QuadraNet IP address (Dkt. 55-2 ¶¶ 3-4), which Plaintiffs claimed "was located in Los Angeles, California" (Dkt. 55-6 ¶ 2). The Court held that evidence could not support specific jurisdiction because "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 [NSO's alleged] intentional act." (Dkt. 111 at 21.)

That conclusion remains correct. Courts agree that personal jurisdiction does not exist "over a private foreign entity solely because that entity engaged in tortious conduct from a location outside of the United States by remotely accessing servers located in the United States." *Hungerstation*, 857 F. App'x at 351. "Likewise, no authority supports the proposition that the act of using a third-party company's server in the United States to host illegally-obtained information, without more, is sufficient to convey personal jurisdiction." *Id.* Numerous courts had so held when this Court issued its earlier decision,[10] and that consensus has only grown stronger since.[11]

Those cases govern here because Plaintiffs have no evidence that NSO "made a deliberate decision to locate [any] server in California." *Freeman*, 2024 WL 1880147, at *2. "There is no [evidence] that [NSO] agreed that [QuadraNet] would host the data in California, or even knew where the data would be hosted." *Id.* The record reflects only that QuadraNet leased servers to a Vietnamese company called 365 Online Technology JSC with the email address admin@greencloudvps.com. (Akro. Exh. Q.) There is no evidence that NSO had any contract or communications with QuadraNet, any control over which servers QuadraNet used, any knowledge of where any QuadraNet server was located, or even any communications with QuadraNet's

[10] *E.g., Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs.,* 334 F.3d 390, 402 (4th Cir. 2003); *Kazakhstan v. Ketebaev*, 2017 WL 6539897, at *6-7 (N.D. Cal. Dec. 21, 2017); *Sonterra Cap. Master Fund Ltd. v. Credit Suisse Grp. AG*, 277 F. Supp. 3d 521, 590 (S.D.N.Y. 2017); *Rosen v. Terapeak, Inc.*, 2015 WL 12724071, at *9 (C.D. Cal. Apr. 28, 2015); *Man-D-Tec, Inc. v. Nylube Prods. Co.*, 2012 WL 1831521, at *2 (D. Ariz. May 18, 2012).

[11] *E.g.*, *Doe v. Yardi Sys. Inc.*, 2024 WL 1601787, at *3 (C.D. Cal. Mar. 27, 2024); *Zarif v. Hwareh.com, Inc.*, 2024 WL 1268167, at *5 (S.D. Cal. Mar. 25, 2024); *Alhathloul v. DarkMatter Grp.*, 2023 WL 2537761, at *6-7 (D. Or. Mar. 16, 2023); *GeoSolutions B.V. v. Sina.com Online*, 700 F. Supp. 3d 821, 828-29 (N.D. Cal. Oct. 27, 2023); *Ross v. Abbott Vascular Inc.*, 2022 WL 20275185, at *6 (N.D. Cal. Mar. 3, 2022); *Prevail Legal, Inc. v. Gordon*, 2021 WL 1947578, at *5-6 (N.D. Cal. May 14, 2021); *CrossFit, Inc. v. Fitness Trade sp. z o.o.*, 2020 WL 6449155, at *5-6 (S.D. Cal. Nov. 2, 2020).

customer 365 Online Technology/Greencloud. (Akro. Decl. ¶ 12; Shohat Decl. ¶ 22; McGraw Decl. ¶¶ 57-59.) Therefore, the presence of a QuadraNet server in California would be entirely "fortuitous." (Dkt. 111 at 21); *see Zarif*, 2024 WL 1268167, at *5 (defendant did not "target" California by using web host's California servers because web host, "not [d]efendant, chose to locate its servers in California," so the servers' location "was merely 'random' or 'fortuitous'").

Furthermore, "the level of contact created by the connection between an out-of-state defendant and a web server located within a forum" is "de minimis." *Carefirst*, 334 F.3d at 402. NSO never operated any third-party server. (Akro. Exh. I at 285:7-9.) Plaintiffs claim only that NSO *leased* them and that NSO's government customers used them "to send malware and other commands to users' devices but not WhatsApp's servers," so the servers were mere waypoints between governmental Pegasus users and foreign targets with no connection to California. (Dkt. 111 at 21.) Even if Plaintiffs could prove (and they cannot) that Pegasus transferred some data through third-party servers in California, such transient contacts with California would still be too insignificant to establish purposeful direction. (*Id.*); *Carefirst*, 334 F.3d at 402. A contrary ruling would create a dangerous precedent, moreover, under which "the Northern District of California always would have jurisdiction in any case where a party hosts its data with a Silicon Valley company." *Hungerstation*, 2020 WL 137160, at *6. This District "is not an international court of internet law," and Plaintiffs should not be permitted to treat it like one. *Id.* (cleaned up).

3. Westbridge's actions cannot support specific jurisdiction over NSO.

Unable to support specific jurisdiction with NSO's own conduct, Plaintiffs appear to seek to rely on *Westbridge*'s marketing activities in California. But Westbridge was a distinct entity from NSO, and Plaintiffs have no evidence that could justify attributing Westbridge's conduct to NSO for purposes of personal jurisdiction.

To begin, Plaintiffs cannot attribute Westbridge's conduct to NSO unless Westbridge and NSO were alter egos. *Am. Tel. & Tel. Co. v. Compagnie Bruxelles Lambert*, 94 F.3d 586, 591 (9th Cir. 1996). Before the Supreme Court's decision in *Daimler*, the Ninth Circuit allowed courts to exercise "general jurisdiction . . . under an agency theory." *Williams v. Yamaha Motor Co.*, 851 F.3d 1015, 1021 (9th Cir. 2017). But *Daimler* "invalidated [that] 'agency' test," *id.*, a holding that

"applies no less in the context of specific jurisdiction," *id.* at 1024. Accordingly, "the agency test cannot be the basis of this Court's exercise of specific jurisdiction," and Plaintiffs must prove that Westbridge and NSO were alter egos. *MSP Recovery Claims, Series LLC v. Actelion Pharms. US, Inc.*, 2024 WL 3408221, at *4 (N.D. Cal. July 12, 2024).[12] Plaintiffs cannot do so.

To prove that two entities are alter egos, a plaintiff must prove "that there is such unity of interest and ownership that the separate personalities of the two entities no longer exist." *Williams*, 851 F.3d at 1021. That requires proof of the parent company's "pervasive control over the subsidiary, such as when a parent corporation *dictates every facet* of the subsidiary's business—from broad policy decisions to routine matters of day-to-day operation." *Ranza v. Nike, Inc.*, 793 F.3d 1059, 1073 (9th Cir. 2015) (emphasis added). Under this test, no reasonable jury could find that NSO and Westbridge were alter egos. Even "a parent-subsidiary relationship is insufficient, on its own, to justify imputing one entity's contacts with a forum state to another for the purpose of establishing personal jurisdiction," *Ranza*, 793 F.3d at 1070, and NSO was not Westbridge's parent. They were "distinct business entities" within a sprawling corporate family, reflecting mere "common ownership" that "is insufficient to disregard the corporate form." *Apple Inc. v. Allan & Assocs. Ltd.*, 445 F. Supp. 3d 42, 53 (N.D. Cal. 2020).[13] In addition, Plaintiffs cannot prove that NSO and Westbridge "failed to respect corporate formalities." *Id*. Among other things, Westbridge and NSO had separate employees and offices, "maintained separate bank accounts and never comingled assets or funds," and kept "separate corporate records." *Apple*, 445 F. Supp. 3d at 53; (*see* Akro. Exh. G at 270:2-271:14, 272:17-275:14, Exh. J at 273:6-277:19; Shohat Decl. ¶ 20). "This evidence establishes that [NSO and Westbridge] are not alter egos." *Apple*, 445 F. Supp. 3d at 53.

Additionally, Plaintiffs cannot prove, as they would have to, that NSO "dictate[d] every facet of" Westbridge's "day-to-day operation." *Ranza*, 793 F.3d at 1073-74. Westbridge "negotiate[d] its own contracts and licenses" and made its own decisions about where and how to market Pegasus. *Id.* at 1074; (*see* Akro. Exh. G at 290:2-7, Exh. J at 288:9-293:1, 314:14-315:5).

[12] *Accord Aldrich v. NCAA*, 484 F. Supp. 3d 779, 794 (N.D. Cal. 2020); *Corcoran v. CVS Health Corp.*, 169 F. Supp. 3d 970, 982 (N.D. Cal. Mar. 14, 2016); *Los Gatos Mercantile, Inc. v. E.I. DuPont De Nemours & Co.*, 2015 WL 4755335, at *5 (N.D. Cal. Aug. 11, 2015).

[13] *Ranza*, 793 F.3d at 1073 ("Total ownership and shared management personnel are alone insufficient to establish the requisite level of control."); *GeoSolutions*, 700 F. Supp. 3d at 828 (same).

Therefore, the mere fact that Westbridge "market[ed] products on [NSO's] behalf" is insufficient as a matter of law to attribute its conduct to NSO. *Ranza,* 793 F.3d at 1075.

The same would be true even if specific jurisdiction could be based on agency after *Daimler*. "[U]nder any standard for finding an agency relationship, the parent company must have the right to substantially control its subsidiary's activities." *Williams*, 851 F.3d at 1024-25; *accord Bluestar Genomics v. Song*, 2023 WL 4843994, at *23 (N.D. Cal. May 25, 2023). In practice, this "agency analysis" is "identical" to the test for "alter-ego liability" because it requires "parental control of the subsidiary's internal affairs or daily operations." *Apple*, 445 F. Supp. 3d at 56 (cleaned up); *see In re Dynamic Access Memory*, 2005 WL 2988715, at *7-8 (N.D. Cal. Nov. 7, 2005) (Hamilton, J.) (rejecting specific jurisdiction based on agency when "each foreign parent defendant who maintains an American subsidiary also maintains an independent and separate existence, controls its own day to day activities, controls its own books, and maintains its own revenues"). Plaintiffs cannot prove any such control by NSO over Westbridge. Westbridge was an independent contractor rather than an agent, and Plaintiffs have "no evidence [NSO] directed [Westbridge] to sell [Pegasus] in California," *Tangle, Inc. v. Buffalo Games, LLC*, 2023 WL 5672178, at *6 (N.D. Cal. Sept. 1, 2023), or that NSO "ordered or required" any of Westbridge's activities, *CZ Servs., Inc. v. Anthem Ins. Cos.*, 2022 WL 4126281, at *2 (N.D. Cal. Sept. 9, 2022). Without such evidence that NSO "actively directed [Westbridge's] advertising and sales efforts," NSO cannot be subject to specific jurisdiction based on those efforts. *Williams*, 851 F.3d at 1023 n.3.

Finally, Westbridge's marketing cannot support specific jurisdiction because Plaintiffs' claims do not "arise out of or relate to" it. *Yamashita v. LG Chem, Ltd.*, 62 F.4th 496, 503 (9th Cir. 2023) (cleaned up). The "'effects test' can only be satisfied if the plaintiff can point to contacts which demonstrate that the defendant *expressly aimed its tortious conduct* at the forum, and thereby made the forum the focal point of *the tortious activity.*" *Hasson*, 114 F.4th at 192 (cleaned up). Westbridge's marketing is not the "tortious activity" Plaintiffs challenge, *id.*, and neither of the former Westbridge-employee witnesses testified that they *used* Pegasus during any marketing in California. (*See* Akro. Exh. J at 202:6-20, 205:19-206:1; *cf.* Akro. Exh. H at 155:10-24, 171:23-172:1.) And Westbridge's marketing to California local law enforcement agencies failed, so no

California-based potential customer ever used Pegasus either. That marketing, therefore, has no connection to the conduct that Plaintiffs claim to be unlawful and lacks the "close relation" to Plaintiffs' claims necessary to support specific jurisdiction. *Yamashita*, 62 F.4th at 506.

B. NSO is not subject to nationwide jurisdiction under Rule 4(k)(2).

Plaintiffs also previously argued that NSO is subject to nationwide jurisdiction under Rule 4(k)(2). But "[t]he Ninth Circuit has urged cautious application of Rule 4(k)(2)," *Hungerstation*, 2020 WL 137160, at *7, which permits jurisdiction only if a defendant has "significant" and "extensive contacts" with the United States as a whole, *Holland Am. Line Inc. v. Wartsila N.A., Inc.*, 485 F.3d 450, 462 (9th Cir. 2007). NSO lacks such contacts.

First, Courts routinely reject Rule 4(k)(2) jurisdiction based on a defendant's alleged use of U.S.-based servers. *Hungerstation*, 857 F. App'x at 350-51; *X Corp.*, 2024 WL 1245993, at *6-11; *Alhathloul*, 2023 WL 2537761, at *6-8; *CrossFit*, 2020 WL 6449155, at *9-10; *Sonterra*, 2020 WL 137160, at *7. As with NSO's alleged use of California servers, Plaintiffs have no evidence that NSO purposefully targeted either WhatsApp or third-party servers based on their location in the United States, so any contacts between NSO and U.S.-based servers "are too weak to satisfy the due process demands of personal jurisdiction." *Ross*, 2022 WL 20275185, at *6.

Second, Plaintiffs cannot attribute Westbridge's U.S. marketing to NSO because Westbridge was not NSO's alter ego or agent for purposes of personal jurisdiction. If NSO *were* Westbridge's alter ego, then NSO would be subject to *general* jurisdiction in Westbridge's home state of Delaware. *Williams*, 851 F.3d at 1021. NSO would then be "subject to jurisdiction in an[other] state's courts of general jurisdiction," Fed. R. Civ. P. 4(k)(2)(A), and Rule 4(k)(2) would not apply, *Cargnani v. Pewag Austria G.m.b.H.*, 2007 WL 415992, at *10 (E.D. Cal. Feb. 5, 2007).

That aside, Westbridge's marketing activities in the United States are neither substantial enough nor closely enough related to Plaintiffs' claims to support jurisdiction under Rule 4(k)(2), even if they were attributed to NSO. Plaintiffs do not challenge Westbridge's marketing standing alone, and they do not claim any U.S. government agency violated the law by licensing and using Pegasus. (Nor could Plaintiffs , since CFAA does not apply to U.S. law-enforcement activities. 18 U.S.C. § 1030(f).) Moreover, Westbridge's marketing and selling of NSO's products do not

constitute "extensive contacts" with the United States because NSO "also marketed in other countries." *Good Job Games Bilism Yazilim Ve Pazarlama A.S. v. SayGames LLC*, 458 F. Supp. 3d 1202, 1212 (N.D. Cal. 2020), *rev'd on other grounds*, 2021 WL 5861279 (9th Cir. Dec. 10, 2021). Out of all of NSO's Pegasus contracts, the FBI was the only U.S. government agency to ever use Pegasus. (Akro. Exh. H at 148:16-21.) That one sale is too limited a contact with the United States to support jurisdiction "on a national scale." *Glencore Grain Rotterdam B.V. v. Shivnath Rai Harnarain Co.*, 284 F.3d 1114, 1127 (9th Cir. 2002) ("seven East Cost shipments" were too "few in number" to trigger Rule 4(k)(2)).[14] And again, if contacts between NSO and the FBI *were* sufficient to create personal jurisdiction, then NSO would be subject to specific jurisdiction in Washington, D.C., and Rule 4(k)(2) would not apply. *Platinum Performance, Inc. v. Pro Dev., GmbH*, 2009 WL 10676261, at *6 (C.D. Cal. Jun 3, 2009).

II. NSO is entitled to summary judgment on all claims based on the operational use of Pegasus by NSO's government customers.

Plaintiffs alleged in their Complaint that NSO itself operates Pegasus, another claim that discovery proved to be untrue. Plaintiffs, however, continue to assert claims based on the use of Pegasus to monitor the targets of governmental investigations. NSO is entitled to summary judgment on all of these claims. As a threshold matter, Plaintiffs have no evidence that NSO ever operated Pegasus to access any target user's device. Even if Plaintiffs had such evidence, the act of state doctrine would bar any claim challenging foreign governments' use of Pegasus.

A. Plaintiffs have no evidence NSO ever unlawfully used Pegasus.

Plaintiffs' claims against NSO related to the use of Pegasus fail for the simple reason that they cannot attribute any use of Pegasus to NSO. NSO's government customers alone operate Pegasus and make all decisions about how to do so. (Shohat Exh. A ¶ 2.4, Exh. B ¶ 2.4.) Plaintiffs

[14] *Holland*, 485 F.3d at 462 ("isolated incident" in Florida insufficient under Rule 4(k)(2)); *accord Michael Grecco Prods. Inc. v. ImageSelect B.V.*, 2024 WL 1640911, at *9-10 (C.D. Cal. Mar. 11, 2024); *St Andrews Links Ltd. v. Source & Design Int'l (UK) LTD*, 2022 WL 11902199, at *4-5 (N.D. Cal. Oct. 20, 2022); *Travelers Prop. Cas. Co. of Am. v. Apex Shipping Co. (NYC)*, 2020 WL 5608476, at *6 (N.D. Cal. Aug. 31, 2020).

know that the users of Pegasus are "nation states" (Akro. Exh. R[15]), and they have no evidence from which a reasonable jury could find that *NSO*, rather than its government customers, ever used Pegasus to access a nonconsenting WhatsApp user's device. Without evidence of any such conduct *by* NSO, Plaintiffs cannot pursue a claim *against* NSO for the use of Pegasus.

B. The act of state doctrine bars Plaintiffs' claims based on the operational use of Pegasus by NSO's government customers.

Even if Plaintiffs could attribute governments' use of Pegasus to NSO, the act of state doctrine prohibits U.S. courts from resolving any claim based on that conduct. The act of state doctrine bars lawsuits that "question the legality of the sovereign acts of foreign states." *IAM*, 649 F.2d at 1359. It applies, at a minimum, when "(1) there is an official act of a foreign sovereign performed within its own territory; and (2) the relief sought or the defense interposed in the action would require a court in the United States to declare invalid the foreign sovereign's official act." *Sea Breeze Salt, Inc. v. Mitsubishi Corp.*, 899 F.3d 1064, 1069 (9th Cir. 2018) (cleaned up). The "doctrine is to be applied pragmatically and flexibly, with reference to its underlying considerations." *In re Philippine Nat'l Bank*, 397 F.3d 768, 773 (9th Cir. 2005) (cleaned up). "Thus, even when an act of a foreign state affects property outside of its territory, the considerations underlying the act of state doctrine may still be present" when justified by an "underlying governmental interest." *Id.* at 773-74 (cleaned up).[16] A "private litigant may raise the act of state doctrine, even when no sovereign state is a party to the action." *IAM*, 649 F.2d at 1359.

The act of state doctrine applies to foreign governments' use of Pegasus. NSO exclusively licensed Pegasus to governments and government agencies, and a government's use of Pegasus is an "official, sovereign act[]." *Sea Breeze Salt*, 899 F.3d at 1069. When a government engages in "clandestine surveillance and espionage," it "employ[s] powers that . . . are peculiar to sovereigns." *Broidy Cap. Mgmt., LLC v. Qatar*, 982 F.3d 582, 594 (9th Cir. 2020) (cleaned up). Even though Plaintiffs contend that some uses of Pegasus occasionally sent messages through WhatsApp servers

[15] *See, e.g.*, Akro. Exh. S ("MX government[]"), Exh. T ("Saudi Arabian government[]"), Exh. U ("Uzbekistan's government[]"), Exh. V ("UAE government[]").

[16] *See AdvanFort Co. v. Cartner*, 2015 WL 12516240, at *7 (E.D. Va. Oct. 30, 2015) ("the fact that a government entity acted outside the physical boundaries of the sovereign will not automatically defeat the doctrine's application where the decision . . . is 'governmental' in nature").

in the United States, only WhatsApp—not NSO or its customers—controlled which servers any message passed through. The fortuity that *WhatsApp* potentially may have caused some Pegasus messages sent *by* foreign governments *to* foreign devices to pass through U.S. servers does not rob those governments' actions of their sovereign nature or eliminate their "governmental interest" in not having those actions questioned in U.S. courts. *Philippine Nat'l Bank*, 397 F.3d at 773; *cf. Broidy*, 982 F.3d at 594 (nation's "surveillance and espionage against a national of another nation in that other nation" is sovereign conduct).

Plaintiffs' claims would improperly require this Court to "question the legality of . . . sovereign acts" by finding that governments' uses of Pegasus were illegal. *IAM*, 649 F.2d at 1359. The district court's decision in *Du Daobin v. Cisco Sys.*, 2 F. Supp. 3d 717 (D. Md. 2014), is instructive. There, the plaintiffs sued Cisco for allegedly designing and selling a "surveillance program" that China "used to detect, monitor, detain, suppress, and torture dissidents." *Id.* at 720. The court held the act of state doctrine barred the lawsuit. Although the plaintiffs sued only Cisco, they "effectively ask[ed] the [c]ourt to decide that the Chinese government, with substantial assistance from Cisco, has engaged in multiple violations of international law." *Id.* at 726. The act of state doctrine prohibited such "judicial interference" in the "official actions of the Chinese government." *Id.* Likewise here, Plaintiffs "ask[] the Court to decide the extent to which" NSO's "technology can be used . . . by foreign governments." *Id.* The act of state doctrine forbids that result.

III. NSO is entitled to summary judgment on Plaintiffs' CFAA claim.

In addition to the other defects identified above, Plaintiffs' CFAA claim cannot proceed for other reasons. First, as this Court already held, Plaintiffs cannot prove a claim under CFAA's "without authorization" prong because NSO's alleged agreement to WhatsApp's TOS establishes that NSO *had* authorization to access WhatsApp's servers. (Dkt. 111 at 37.) Second, Plaintiffs cannot prove a claim under CFAA's "exceeds authorized access" prong because they have no evidence that NSO circumvented any technical restrictions on WhatsApp's servers to "obtain or alter information in" the servers that NSO was "not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Third, NSO's R&D after December 2018 was all "lawfully authorized investigative, protective, or intelligence activity of" the FBI, which CFAA does not prohibit. *Id.* § 1030(f).

A. Plaintiffs cannot pursue a "without authorization" claim or a claim based on WhatsApp's terms of service.

CFAA prohibits certain forms of computer access either "without authorization" or in a way that "exceed[s] authorized access." 18 U.S.C. § 1030(a). In this Court's motion to dismiss order, the Court dismissed Plaintiffs' CFAA claims to the extent they alleged that NSO accessed WhatsApp's servers "without authorization" because Plaintiffs contend that NSO agreed to WhatsApp's TOS, which gave NSO "authorization to send messages . . . over WhatsApp's servers." (Dkt. 111 at 37.) The Court limited Plaintiffs to proceeding under CFAA's "exceeds authorized access prong." (*Id.* at 39.) Plaintiffs did not amend their complaint.

Despite this, Plaintiffs and their experts continue to assert that NSO accessed WhatsApp servers "without authorization." This Court's order forecloses that claim. When a court dismisses a claim and the plaintiff does not amend its complaint, the plaintiff "cannot simply resurrect [that] claim[]" after discovery. *Chronic Tacos Enters., Inc. v. Chronic Tacos Huntington Beach, Inc.*, 2011 WL 6010265, at *2 (C.D. Cal. Nov. 28, 2011).[17] Nor may a plaintiff "amend [its] complaint through an opposition to a motion for summary judgment." *Id.*; *accord City of L.A. v. Bank of Am. Corp.*, 2015 WL 4880511, at *5 (C.D. Cal. May 11, 2015). Thus, this Court's motion to dismiss order limits Plaintiffs to an "exceeds authorized access" claim; without having amended their complaint, they may not reassert the "without authorization" claim this Court rejected.

That aside, this Court's reasoning remains fatal to any "without authorization" claim. The Court correctly applied Ninth Circuit law holding that "a person uses a computer 'without authorization'" only "when the person has not received permission to use the computer *for any purpose*." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009) (emphasis added). As long as a defendant "is authorized to use a computer for certain purposes," its access to the computer cannot be "without authorization"—even if the defendant violates limits the computer's owners placed on the defendant's access. *Id.* at 1133. Plaintiffs have pleaded that NSO agreed to WhatsApp's TOS, which authorized NSO to access WhatsApp's servers. (Dkt. 111 at 37.)

[17] *Accord Natkin v. Am. Osteopathic Ass'n*, 2024 WL 3510926, at *4 (D. Or. July 23, 2024); *Bagdasaryan v. City of L.A.*, 2018 WL 6113104, at *14-15 (C.D. Cal. Oct. 22, 2018).

Accordingly, Plaintiffs cannot claim NSO "access[ed] a computer without any permission at all," and NSO is entitled to summary judgment on Plaintiffs' "without authorization" claim to the extent that it survived the motion to dismiss. (*Id.*)

Indeed, Plaintiffs cannot pursue *any* CFAA claim based on NSO's alleged breach of WhatsApp's TOS. Even the "exceeds authorized access" prong does not apply to "violations of corporate computer use restrictions." *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (en banc); *accord Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) ("violation of the terms of use of a website—without more—cannot establish liability under the CFAA"). NSO is entitled to summary judgment on any claim that it violated CFAA by accessing a computer in violation of WhatsApp's TOS.

B. Plaintiffs cannot pursue an "exceeds authorized access" claim.

Plaintiffs also cannot prove that NSO violated CFAA's "exceeds authorized access" prong because they have no evidence that NSO used its "access" to Plaintiffs' servers "to obtain or alter information" on the servers that NSO was "not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

Pegasus did not "obtain" or "alter" *any* information on WhatsApp's servers. Pegasus used WhatsApp's servers *only* to send messages to WhatsApp users. Although Pegasus allowed NSO's customers to obtain information from *target users' devices*, Plaintiffs admit NSO did not "corrupt," "alter," "impair the availability of," or "delete any of WhatsApp's data from WhatsApp's servers." (Akro. Exh. L at 183:7-184:7, 250:22-251:24, Exh. K at 249:7-250:10.) Nor did NSO "introduce" a "vulnerability into [WhatsApp's] code base." (Akro. Exh. K at 200:25-201:10.) Instead, Plaintiffs argue that Pegasus sent a *kind* of message that WhatsApp users are not allowed to send. But CFAA does not apply to computer users that merely "misuse [their] access" to a computer. *Van Buren v. United States*, 593 U.S. 374, 381 (2021). It prohibits only "the unauthorized *procurement* or *alteration* of information." *Nosal*, 676 F.3d at 863 (emphasis added). NSO did not take or alter information on WhatsApp's servers, so it did not "exceed[] authorized access" even if WhatsApp did not authorize NSO to send the *kinds* of messages Pegasus sent.

More than that, Plaintiffs cannot prove that NSO ever "entere[d] a part of the [servers] to which [it] lack[ed] access privileges." *Van Buren*, 593 U.S. at 388. The messages Pegasus sent

passed through the exact same areas of WhatsApp's servers as any other WhatsApp message. (Akro. Exh. L at 129:15-130:23; McGraw Decl. ¶¶ 68-70, 73.) And messages Pegasus sent complied with *every* technological restriction WhatsApp's servers placed on such messages—otherwise, the servers would have rejected the messages, and they never would have reached target users' devices. (McGraw Decl. ¶¶ 65-79.) The fact that WhatsApp's "computer code allow[ed]" Pegasus to send those messages proves that WhatsApp's "system authorize[d] the access." *Abu v. Dickson*, 107 F.4th 508, 515 (6th Cir. 2024).

Plaintiffs contend that NSO, by *complying* with WhatsApp's technological restrictions, was somehow *circumventing* them. That makes no sense (McGraw Decl. ¶ 79), and it exposes the fatal flaw in Plaintiffs' theory. At bottom, Plaintiffs' claim is that because they did not *want* WhatsApp users to send messages like those sent by Pegasus, NSO *must have* exceeded its authorized access to WhatsApp servers by sending them. But CFAA enforces only "technological access barriers" on particular *areas* of a computer, *Nosal*, 676 F.3d at 863, not "purpose-based limits" on the *use* of a computer, *Van Buren*, 593 U.S. at 396. Because NSO was allowed to "enter a particular area of the [servers] for some purpose"—sending ordinary WhatsApp messages—it was equally "authorized" under CFAA to use that same area of the servers for any other purpose, even if Plaintiffs believe that "purpose [was] improper." *Abu*, 107 F.4th at 518-19. Because NSO did not access any area of WhatsApp's servers that was unavailable to any other WhatsApp user, Plaintiffs' subjective opposition to the *way* NSO used WhatsApp's servers cannot support a CFAA claim.

C. CFAA's law-enforcement exception shields NSO's R&D after December 2018.

NSO is entitled to summary judgment on any CFAA claim based on its R&D activities after December 2018 because those activities were "lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States." 18 U.S.C. § 1030(f). When the FBI purchased a Pegasus license in December 2018, one of the services it contracted for was "maintenance," which required NSO to maintain Pegasus in an operational state for use by the FBI. (Akro. Exh. N.) Moreover, 10% of every Pegasus contract is earmarked for NSO to provide "updates and upgrades" to Pegasus. (Akro. Exh. M at 212:1-15.) Accordingly, NSO's R&D activities after December 2018 were required, authorized, and paid for by the FBI, which qualifies

them for CFAA § 1030(f)'s "exception for law enforcement activity." *Naicom Corp. v. Dish Network Corp.*, 2024 WL 1363462, at *29 (D.P.R. Mar. 29, 2024).

In *Naicom*, private defendants "assisted federal law enforcement" by "penetrat[ing]" the plaintiff's "servers and computers" and assisting with the execution of search warrants on the plaintiff's computers. *Id.* at *1, 5-6. The plaintiff claimed these actions violated CFAA, but the court dismissed the CFAA claim under § 1030(f), finding that the defendants' "conduct was 'lawfully authorized investigative . . . activity.'" *Id.* at *29. The court rejected the plaintiff's argument that the defendants were acting for their own private motives, holding that "the relevant inquiry is whether the [private] [d]efendants had authorization to access the information" from the federal government. *Id.* at *29 n.17. Here too, NSO's licensing agreement with the FBI authorized NSO's R&D activities after December 2018, making them lawful under § 1030(f).

IV. NSO is entitled to summary judgment on Plaintiffs' CDAFA claim because Plaintiffs cannot prove NSO knowingly took any action in California.

Finally, NSO is entitled to summary judgment on Plaintiffs' CDAFA claim, which requires Plaintiffs to prove NSO intentionally and unlawfully accessed a computer *located in California*. California recognizes a "presumption against extraterritorial application," under which California statutes cannot apply "to occurrences outside the state" unless a contrary intent is "clearly expressed or reasonably to be inferred from the language of the act or from its purpose, subject matter or history." *Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1207 (2011) (cleaned up). The Due Process Clause of the U.S. Constitution also prohibits California from regulating foreign conduct. *Phillips Petrol. Co. v. Shutts*, 472 U.S. 797, 818 (1985); *Churchill Vill., LLC v. Gen. Elec. Co.*, 169 F. Supp. 2d 1119, 1126-27 (N.D. Cal. 2000). For those reasons, California law does not apply when "the liability-creating conduct occurs outside of California." *Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018).

Because CDAFA contains no express language suggesting it applies extraterritorially, it does not govern conduct outside of California. *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *6 (N.D. Cal. Nov. 20, 2020); *Terpin v. AT&T Mobility, LLC*, 399 F. Supp. 3d 1035, 1047-48 (C.D. Cal. 2019); *M Seven Sys. Ltd. v. Leap Wireless Int'l, Inc.*, 2013 WL 12072526, at *3 (S.D. Cal. June 26, 2013).

And while CDAFA covers several forms of computer-related misconduct, the minimum requirement for its prohibitions is "knowing[]" access to a computer. Cal. Penal Code § 502(c). For that conduct to occur within California, the defendant must knowingly access a computer *in California*. Otherwise, "the liability-creating conduct" would "occur[] outside of California," and CDAFA would not apply. *Oman*, 889 F.3d at 1079.[18] That is true even when the plaintiff lives in California, because "the concept of extraterritoriality . . . concerns legislation that regulates *conduct* that occurs in a foreign jurisdiction—regardless of the plaintiff's residency." *English v. Gen. Dynamics Mission Sys.*, 2019 WL 2619658, at *6 (C.D. Cal. May 8, 2019) (cleaned up).[19]

This rule dooms Plaintiffs' CDAFA claim because they cannot prove NSO knowingly accessed any California-based WhatsApp server. As discussed above, WhatsApp had no signaling servers in California, and NSO had no advance knowledge or control of which relay servers any Pegasus message passed through. Accordingly, any access to California servers by NSO would not have been "knowing[]," as CDAFA requires. Moreover, any connection between NSO and California-based WhatsApp servers would be purely fortuitous, and such incidental contact with California would not "show a sufficient nexus between California and [NSO's] alleged wrongful conduct" to permit application of California law. *Nowak*, 2020 WL 6822888, at *6 (CDAFA did not apply to hacking of plaintiff's Bitcoin account even though account was in California); *see Sajfr v. BBG Comms., Inc.*, 2012 WL 398991, at *4 (S.D. Cal. Jan. 10, 2012) (California law did not apply to foreign calls "routed through switches in the United States" and "rated and billed from San Diego").

Conclusion

The Court should grant NSO's motion and enter judgment in NSO's favor.

Dated: September 27, 2024

KING & SPALDING LLP

By: *Joseph N. Akrotirianakis*
JOSEPH N. AKROTIRIANAKIS
AARON S. CRAIG
Attorneys for Defendants

[18] *See Terpin*, 399 F. Supp. 3d at 1047 (dismissing CDAFA claim because plaintiff did "not allege that the hacks . . . occurred in California"); *M Seven*, 2013 WL 12072526, at *3 (CDAFA did not apply to hacking of Korean computer).

[19] *See Allergan, Inc. v. Athena Cosmetics*, 738 F.3d 1350, 1358-59 (Fed. Cir. 2013) (California law did not apply to foreign sales, even if sales "cause[d] [plaintiff] an injury . . . in California").