Greg D. Andres
Antonio J. Perez-Marques
Craig T. Cagney
Gina Cora
Luca Marzorati
(admitted *pro hac vice*)
DAVIS POLK & WARDWELL LLP
450 Lexington Avenue
New York, New York 10017
Telephone: (212) 450-4000
Facsimile: (212) 701-5800
Email: greg.andres@davispolk.com
antonio.perez@davispolk.com
craig.cagney@davispolk.com
gina.cora@davispolk.com
luca.marzorati@davispolk.com

Micah G. Block (SBN 270712)
DAVIS POLK & WARDWELL LLP
1600 El Camino Real
Menlo Park, California 94025
Telephone: (650) 752-2000
Facsimile: (650) 752-2111
Email: micah.block@davispolk.com

Attorneys for Plaintiffs
WhatsApp LLC and Meta Platforms, Inc.

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

WHATSAPP LLC and META PLATFORMS, INC., a Delaware corporation, Plaintiffs, v. NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED, Defendants.	Case No. 4:19-cv-07123-PJH **PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT OR PARTIAL SUMMARY JUDGMENT** Date: November 7, 2024 Time: 1:30 p.m. Ctrm: 3 Judge: Hon. Phyllis J. Hamilton Action Filed: October 29, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

PAGE(S)

STATUTES & RULES

OTHER AUTHORITIES

Plaintiffs' Motion for Partial Summary Judgment established NSO's liability under the Computer Fraud and Abuse Act ("CFAA"), California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), and for contractual breaches of WhatsApp's Terms of Service. NSO admits its Pegasus spyware was used to carry out the attacks described in the complaint, and worked exactly as Plaintiffs alleged. NSO also admits that it created WhatsApp accounts for itself and customers to use with NSO's spyware. NSO even admitted that it circumvented Plaintiffs' security measures both *before* and *after* the May 2019 attacks in order to continue using WhatsApp as an installation vector, even while this litigation was pending. NSO disputes none of those facts, but attempts to avoid liability by challenging personal jurisdiction and asserting various defenses under the CFAA and CDAFA. None has merit, and NSO's motion should be denied.

Discovery has established that personal jurisdiction over NSO exists for several independent reasons. *First*, discovery proves NSO consented to jurisdiction by accepting the amended forum selection clause in WhatsApp's 2020 Terms of Service. *Second*, contrary to NSO's contentions, the undisputed evidence shows that NSO did intentionally target WhatsApp's servers, including by hardcoding the domain names into NSO's source code and designing the means to use WhatsApp's servers to circumvent Plaintiffs' security upgrades in 2018. There is no dispute that those servers were located in the United States, including California, and the Court has already rejected NSO's argument that NSO needed to have selected those particular servers *based on their location*. Dkt No. 111 at 23. *Finally*, NSO purposefully availed itself of the privilege of doing business in California. Not only did NSO enter into a contract with WhatsApp governed by California law, but it leased a California server (through an intermediary) that it hardcoded into more than 700 malicious messages sent during the attack. NSO also partnered with a California private equity firm, which provided millions of dollars in funding that NSO used to develop its WhatsApp-based technology, and which also helped NSO to create a market for Pegasus in California through an NSO-controlled affiliate.

NSO's other arguments are similarly unavailing. NSO is still liable even if (as it claims) it used its spyware only against devices that it owned, because NSO admits it still accessed WhatsApp's servers without authorization. NSO is solely responsible for designing and installing Pegasus via WhatsApp, and thus is liable for all installations requested by its customers, for conspiring with its

customers, and for trafficking in "password or similar information." 18 U.S.C. § 1030(a)(6) & (b).

The act of state doctrine does not apply. NSO has produced no evidence that any (let alone all) its customers were foreign sovereigns, and finding NSO liable does not require invalidating any sovereign's official action taken within its own borders, which makes the doctrine inapplicable.

The undisputed evidence shows that NSO accessed WhatsApp's servers without authorization and exceeded any authorization it purportedly had to obtain information NSO was "not entitled so to obtain." *Id.* § 1030(e)(6). NSO's argument that the FBI sanctioned its activity is meritless. There is no evidence that its independent development of Pegasus was, in fact, directed or authorized by the FBI or part of the FBI's "lawfully authorized investigative" activity. *Id.* § 1030(f).

Finally, to the extent NSO's motion is based on a claim of lack of evidence, that argument should be rejected for the reasons Plaintiffs explained in its Motion for Sanctions. *See* Dkt. No. 406. Accordingly, NSO's motion for summary judgment should be denied.

BACKGROUND

To use WhatsApp, users must install the legitimate WhatsApp client application ("Official Client"), and agree to the WhatsApp Terms of Service ("Terms"). *See* Ex. 1 (Lee Dep.) at 174:4-179:18; *see also* Ex. 2 (Woog Dep.) at 177:7-23; Youssef Decl., Ex. B at 26-27.[1] During registration, an encrypted key is created on the Official Client, which it uses to gain access to the signaling servers, and obtain from them a temporary token used to access the relay servers. Ex. 3 (Gheorghe Dep.) at 117:21-119:25, 136:5-137:13. WhatsApp's signaling servers start the call, and the relay servers support the "realtime traffic" during the call. *Id.* at 31:14-17, 33:10-21. WhatsApp's signaling servers are all located in the United States, although none are in California. Ex. 4 (Palau Dep.) at 89:7-93:14. WhatsApp's relay servers are located in the United States and around the world, including in Los Angeles and San Jose, California. Ex. 3 (Gheorghe Dep.) at 206:8-17.

Pegasus consists of an "agent" that runs on the target devices, Ex. 5 (Gazneli Dep.) at 42:23-43:5, and the software vectors used to install it, *id.* at 30:3-31:13; Ex. 6 (Defs.' Supp. Resps. to Pls.'

[1] Citations to "Br." refer to NSO's motion, Dkt. No. 396, and citations to "Ex." refer to the Exhibits to the Declaration of Micah G. Block submitted herewith. All emphases have been added unless otherwise indicated.

First Interrogs.) at 9-13. Some installation vectors used WhatsApp (the "Malware Vectors"), but did not use the Official Client; instead, NSO designed a modified client application called the "WhatsApp Installation Server" (or "WIS") to send messages that the Official Client could not. Ex. 5 (Gazneli Dep.) at 157:7-164:9, 237:10-238:16, 278:16-279:6. NSO created WhatsApp accounts to use with the WIS because NSO could not access WhatsApp's servers without misappropriating the authentication keys from an Official Client. *Id.* at 278:16-23. NSO also set up WhatsApp accounts and server infrastructure for its customers. *See* Ex. 7 (Eshkar Dep.) at 39:15-17, 151:3-153:8.

An early Malware Vector, called Heaven, used the WIS to manipulate WhatsApp's signaling servers to force them to direct target devices to an external relay server controlled by NSO. *See* Ex. 5 (Gazenli Dep.) at 189:25-196:6; Ex. 3 (Gheorghe Dep.) at 103:14-104:7. Heaven was permanently disabled by security updates that Plaintiffs made to WhatsApp's servers in 2018. *See* Youssef Decl., Ex. B at 38; Ex. 5 (Gazneli Dep.) at 254:14-17; Ex. 8 (PX2007). NSO then developed a new Malware Vector called Eden to circumvent those security updates. Ex. 5 (Gazneli Dep.) at 256:16-258:5. Unlike Heaven, Eden "need[ed] to go through WhatsApp relay servers." *Id.* at 258:17-22; *see* Ex. 6 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 8. NSO admits Eden was responsible for the attacks described in the Complaint. *See* Ex. 9 (Shohat Dep.) at 69:13-18.

After detecting those May 2019 attacks, Plaintiffs implemented security updates for their servers and the Official Client, which permanently disabled Eden. *See* Ex. 3 (Gheorghe Dep.) at 29:22-25; Trexler Decl., Ex. B at 21-31; Ex. 10 (PX2058) at -513; Ex. 11 (PX2039). Plaintiffs also disabled NSO's accounts, *see, e.g.*, Ex. 12 (SHANER_WHATSAPP_00001480), and filed this lawsuit. Dkt. No. 1. NSO then developed a new Malware Vector called Erised that continued using WhatsApp through at least May 2020, while this litigation was pending, until WhatsApp's security updates eventually disabled Erised, too. Ex. 5 (Gazneli Dep.) at 45:15-46:16, 267:2-10.

LEGAL STANDARD

The moving party is entitled to summary judgment only if, after viewing the evidence and drawing all reasonable inferences in the light most favorable to the non-moving party, there are no genuine disputes of material fact. *See* Fed. R. Civ. P. 56(a); *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). When a defendant moves based on a lack of jurisdiction, the court still must construe

the evidence "in the light most favorable to the party opposing the motion," and find jurisdiction "if no genuine issue of material fact remains that [the plaintiff] has established personal jurisdiction by a preponderance of the evidence." *Medimpact Healthcare Sys., Inc. v. IQVIA Inc.*, 2022 WL 6281793, at *11 (S.D. Cal. Oct. 7, 2022) (citation omitted). Any material disputed facts must be resolved "either at a hearing on the issue of jurisdiction or in the course of trial on the merits." *Dorchester Fin. Sec., Inc. v. Banco BRJ, S.A.*, 722 F.3d 81, 85 (2d Cir. 2013) (citation omitted).

ARGUMENT

I. NSO IS SUBJECT TO PERSONAL JURISDICTION

The undisputed evidence demonstrates jurisdiction over NSO. Specific jurisdiction exists if (1) NSO purposefully directed its activities toward the forum or purposely availed itself of the privileges of conducting activities in the forum, and (2) Plaintiffs' claims arise out of or relate to those activities. *Axiom Foods, Inc. v. Acerchem Int'l, Inc.*, 874 F.3d 1064, 1068 (9th Cir. 2017).[2] The undisputed evidence shows several independent bases for jurisdiction. First, NSO consented to jurisdiction by accepting the 2020 amendments to the Terms. *See infra* § I.A. Second, NSO purposefully directed its conduct at California because its "program sought out specific servers—including servers in California—in order to transmit malicious code through those servers." Dkt. No. 111 at 22; *see infra* § I.B. Finally, NSO purposefully availed itself by leasing and repeatedly using a California server, by securing millions of dollars in investment capital from a California private equity firm, and by creating a market for its spyware products in California. *See infra* § I.C.

A. NSO Consented to Jurisdiction

NSO consented to jurisdiction by continuing to use WhatsApp after learning that WhatsApp amended the forum selection clause in its Terms in January 2020.[3] NSO admits its employees created WhatsApp accounts, *see, e.g.*, Ex. 7 (Eshkar Dep.) at 17:13-23, 21:13-24, which required agreeing to the Terms, *see* Ex. 1 (Lee Dep.) at 174:4-179:18. NSO is therefore bound by at least the 2016

[2] The Court has twice concluded exercising jurisdiction is reasonable. Dkt. No. 111 at 31; Dkt. No. 233 at 7-8. NSO makes no further arguments about reasonableness, and waives any it might have.

[3] Plaintiffs preserve for appeal their contention that the forum selection clause in the 2016 Terms also covered this dispute. *See, e.g.*, Dkt. No. 55 at 10-12.

Terms, *see AWR Corp. v. ZTE, Corp.*, 2011 WL 13217534, at *2–3 (C.D. Cal. June 13, 2011); Dkt. No. 401 at 6-8, which NSO does not deny (Br. at 21). The 2016 Terms permitted WhatsApp to amend them and provided that "continued use of [WhatsApp's] Services confirms [the user's] acceptance of [the] Terms, as amended." Ex. 13 (WA-NSO-00014825) at -832. Such provisions are routinely enforced. *See Ghazizadeh v. Coursera, Inc.*, 2024 WL 3455255, at *13 (N.D. Cal. June 20, 2024) (using services after email notice is "sufficient to demonstrate manifestation of consent to the updated terms"); *Sadlock v. Walt Disney Co.*, 2023 WL 4869245, at *13 (N.D. Cal. July 31, 2023).

On January 28, 2020, WhatsApp amended the forum selection clause to state: "[Y]ou agree that you and WhatsApp will resolve any Claim 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 . . . and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such Disputes." Ex. 14 (WA-NSO-00195067) at -071. NSO admits that this revised language "covers 'any Claim,' period," and "expand[s] coverage . . . to the two way 'you and WhatsApp will resolve any claim' between the parties" in California. Dkt. No. 62 at 3. In a declaration filed on April 2, 2020, NSO's counsel admitted he became aware of this amendment in February 2020, after it was posted on WhatsApp's website. Dkt. No. 45-1; *see Roche v. Hyde*, 51 Cal. App. 5th 757, 797 (Cal. Ct. App. 2020) (attorney's knowledge is imputed to its client). NSO admits it continued using WhatsApp *after* his declaration was filed, through at least May 2020, Ex. 5 (Gazneli Dep.) at 267:2-271:8, and its documents show it had installed versions of the Official Client released after the amendments.[4] Dkt. No. 401-1 (Block Decl.) ¶ 18 & Ex. 23; Dkt. No. 401-3 (Andre Decl.) ¶ 9 & Ex. A. NSO thus accepted the amended forum selection clause and consented to this Court's jurisdiction. *See Li v. Amazon.com Servs. LLC*, 2023 WL 8720669, at *7 (N.D. Cal. Dec. 18, 2023) (amendment applies to preexisting disputes).

B. NSO Purposefully Directed Its Conduct at Plaintiffs' Servers

The "purposeful direction" test requires that the defendant "(1) committed an intentional act,

[4] NSO has prevented Plaintiffs from using the phone numbers from these devices to determine whether NSO also expressly accepted the 2020 version of the Terms. *See* Dkt. No. 408 at 1-2.

(2) expressly aimed at the forum state, [and] (3) caus[ed] harm that the defendant knows is likely to be suffered in the forum state." *See Axiom Foods*, 874 F.3d at 1069 (citation omitted). The Court found these elements satisfied by Plaintiffs' allegations that: (1) NSO "target[ed] WhatsApp's systems and servers . . . to disseminate malicious code and malware" and "designed and manufactured a program to exploit WhatsApp's app, servers, and infrastructure," Dkt. No. 111 at 18-19; (2) NSO's "program sought out specific servers—including servers in California—in order to transmit malicious code through those servers," *id.* at 21-22; and (3) NSO "would have known they were harming plaintiffs" at "their principal place of business in California," *id.* at 25. Plaintiffs' Motion demonstrates that discovery proved all these allegations. In its motion, NSO only disputes the proof that it sought out California servers. NSO's own admissions demonstrate that it did.

It is undeniable that NSO deliberately sought out WhatsApp servers because its messages "*had to be* transmitted through WhatsApp servers" to reach the target devices. Ex. 5 (Gazneli Dep.) at 184:6-10; *see also id.* at 277:17-278:2; 282:1-10; 325:23-326:19. That is why NSO researched WhatsApp's servers to understand "[t]he required server functionality that enables you to send messages from one side to another," *id.* at 68:10-69:21, and the "limitations in terms of sending messages from peer to peer," *id.* at 145:23-146:12. NSO then designed the WIS to use WhatsApp's internal, proprietary "FunXMPP" protocol for the sole purpose of "communicat[ing] with WhatsApp servers," *id.* at 279:16-282:10 ("There is no other way to communicate."), and hardcoded the domain name for WhatsApp's signaling servers into its source code to "direct the communication to that server specifically," *id.* at 276:19-278:2. NSO also admits it deliberately designed its Eden Malware Vector to use WhatsApp's relay servers to circumvent WhatsApp's 2018 security updates. *See id.* at 254:2-260:2; Ex. 6 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 10-12.

There is no dispute about the servers' locations. Br. at 5-6, 9. WhatsApp's signaling servers were exclusively in the United States. Ex. 4 (Palau Dep.) at 89:7-93:14. And NSO used U.S.-based relay servers at least 176 times out of 379 attacks (46%) recorded by Plaintiffs' server logs over just ten days in May 2019, including using relay servers located in California 43 times (11%). *See* Ex. 15 (WA-NSO-00166473); Ex. 3 (Gheorghe Dep.) at 206:8-17; Br. at 6.

There is no requirement that NSO "target[] any server ***based on its location***," as NSO insists.

Br. at 2.[5] This Court already concluded it is irrelevant whether NSO "selected the location of the server," and rejected NSO's arguments that "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." Dkt. No. 111 at 23. The Court's rationale relied on well-established Ninth Circuit authority, all of which remains good law and NSO ignores. The Ninth Circuit has held that whether conduct is "expressly aimed" at the forum "depends, to a significant degree, on the specific type of tort or other wrongful conduct at issue." *Picot v. Weston*, 780 F.3d 1206, 1214 (9th Cir. 2015) (quoting *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 807 (9th Cir. 2004)). And the Ninth Circuit has held that "the conduct prohibited [by the CFAA] is analogous to that of 'breaking and entering,'" *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1196 (9th Cir. 2022) (citation omitted). This Court thus reasonably concluded that "[b]y 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." Dkt. No. 111 at 23. In the four years since that decision, courts have followed this Court's rationale,[6] and none have disagreed with it.

NSO's connection with California is thus not dependent on Plaintiffs' "unilateral activity," and NSO's reliance on *Walden v. Fiore*, 571 U.S. 277 (2014), continues to be misplaced. Br. at 11. In *Walden*, DEA agents seized Nevada residents' property in Georgia, who then unilaterally returned to Nevada and sued there. 571 U.S. at 280-81. The Supreme Court found no jurisdiction because the defendants "never traveled to, conducted activities within, contacted anyone in, or *sent anything or anyone to Nevada*." *Id.* at 288-89. This case is completely different. NSO did not merely target Plaintiffs, who happened to be California residents, but intentionally reached into California to access WhatsApp's servers located here. And as discussed in more detail below, NSO also leased a California server, whose IP address NSO hardcoded into over 700 messages sent over WhatsApp servers, and which NSO used to install Pegasus on target devices. *See infra* § I.C.1. As this Court

[5] *GreatFence.com, Inc. v. Bailey* is not to the contrary. 726 F. App'x 260, 261 (5th Cir. 2018); *see* Br. at 11. Defendants there did not direct any conduct at the forum servers, and had not "played any role in selecting [their website hosting company's] server's location." 726 F. App'x at 261

[6] *See, e.g.*, *Facebook, Inc. v. Sahinturk*, 2022 WL 1304471, at *4 (N.D. Cal. May 2, 2022); *E3 Innovation Inc. v. DCL Techs. Inc.*, 2021 WL 5741442, at *9 (D. Ariz. Dec. 2, 2021).

recognized, Dkt. No. 111 at 24 n.7, *Walden* did not address these "very different questions whether and how a defendant's virtual 'presence' and conduct" "committed via the Internet or other electronic means" "translate into 'contacts' with a particular State." *Walden*, 571 U.S. at 290 n.9. NSO identifies no authority undermining this Court's correct conclusion that "[b]y sending the malicious code, defendants electronically entered the forum state seeking out plaintiffs' servers," and thus "created a connection with the forum beyond an individualized targeting theory." Dkt. No. 111 at 24-25; *see also Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.*, 592 U.S. 351, 371 (2021) (rejecting arguments that *Walden* precluded jurisdiction where plaintiffs unilaterally brought their vehicles to Montana and Minnesota because of defendants' own contacts with the forum). NSO therefore cannot complain that Plaintiffs unilaterally decided where to locate their own servers, because NSO was intent on accessing them no matter where they were, and did in fact access them.

NSO also contends that Plaintiffs unilaterally directed NSO's messages to these U.S.- and California-based servers, but that is false. As a threshold matter, NSO violated this Court's orders by not producing its Pegasus code, nor any discovery showing how it selected the WhatsApp servers. NSO therefore, tellingly, does not rely on any of its own documents, *cf.* Dkt. No. 397-2 (McGraw Decl.) ¶ 49, and instead relies on evidence concerning how WhatsApp's *Official Client* ordinarily selects servers. *See, e.g.*, Ex. 3 (Gheorghe Dep.) at 103:14-104:7; Br. at 4-5. To be sure, ordinarily, the *Official Client* chooses which relay server to use. Ex. 3 (Gheorghe Dep.) at 120:21-121:17. But as shown in Plaintiffs' Motion, NSO *did not use the Official Client*, and instead constructed and used the WIS to access WhatsApp's servers. *See* Ex. 5 (Gazneli Dep.) at 157:7-22, 161:20-162:3, 186:10-17. Although NSO refused to disclose how the WIS selected those servers, however it worked, NSO alone decided which servers *the WIS* used, not Plaintiffs. Youssef Decl. ¶¶ 8-15.

The undisputed evidence shows that NSO designed the WIS to select WhatsApp relay servers used during the attack. First, NSO admits that for the Heaven Malware Vector, the WIS manipulated the relay server options generated by the signaling servers and tricked the Official Client on the target device into using NSO's server as the relay server. Ex. 5 (Gazneli Dep.) at 189:25-196:22. An NSO document indicates that, to accomplish this feat, NSO carefully researched how WhatsApp's relay servers were selected by WhatsApp. Ex. 16 (PX2033). Then, to circumvent WhatsApp's 2018

security updates disabling Heaven, NSO developed Eden, which relied exclusively on WhatsApp's relay servers. *See* Ex. 5 (Gazneli Dep.) at 254:14-23, 259:21-260:2; Ex. 6 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 10-12. Because NSO designed the WIS for Eden, it could have used any relay server, and even if it selected them using an algorithm similar to the Official Client's, as NSO contends (Br. at 10), the resulting relay server used in the attack would still be an intentional choice *by NSO*—not WhatsApp. *See* Ex. 5 (Gazneli Dep.) at 157:7-20, 186:10-17; Dkt. No. 401 at 15-18.

NSO also knew or should have known the locations of WhatsApp's relay and signaling servers. It is well known, and would have been known to NSO, that Plaintiffs are located in California, and at least some of its servers were likely there.[7] *See Facebook, Inc. v. Rankwave Co.*, 2019 WL 8895237, at *6 (N.D. Cal. Nov. 14, 2019) (considering it a "well-known fact that Facebook is headquartered in California"). The Terms also indicated that WhatsApp's notice address was in California. *See* Ex. 13 (WA-NSO-00014825) at -834. Log files from the Amazon Web Services server, which NSO admits it controlled at the relevant time, Dkt. No. 339-1, and NSO's expert relies on, Dkt. No. 397-2 ¶¶ 48-52, demonstrate that NSO recorded the IP addresses for the relay server options that it received from the signaling servers and that it used with Pegasus, which was enough information for NSO to determine their location. *See* Youssef Decl. ¶¶ 8-15, Ex. B at 37, Ex. C at 21. If NSO, in fact, took no steps to determine those servers' location, as they claim, Ex. 5 (Gazneli Dep.) at 323:23-325:8, that could only result from willful blindness, which is no defense. *See United States v. Nosal* ("*Nosal II*"), 844 F.3d 1024, 1039-40 (9th Cir. 2016); *Facebook, Inc. v. ConnectU LLC*, 2007 WL 2326090, at *6 (N.D. Cal. Aug. 13, 2007) ("remaining ignorant of Facebook's precise location" did not "warrant[ ] a different result").

In addition, it is undisputed that NSO hardcoded the domain name for WhatsApp's signaling servers into the WIS in order to "direct the communication to that server specifically." Ex. 5 (Gazneli Dep.) at 276:19-278:2. NSO does not dispute that it targeted the signaling servers, or that all were in the United States, and only argues that none were in California. Br. at 9. That is irrelevant, because

[7] *See, e.g.*, *Oregon Int'l Airfreight Co. v. Bassano*, 2022 WL 2068755, at *4 (D. Or. May 16, 2022); *DBSI, Inc. v. Oates*, 2020 WL 5517305, at *3 (D. Ariz. Sept. 14, 2020); *Seattle Sperm Bank, LLC v. Cryobank Am., LLC*, 2018 WL 3769803, at *1 (W.D. Wash. Aug. 9, 2018).

Plaintiffs' CFAA claim arises under federal law and Rule 4(k)(2) permits jurisdiction based on NSO's contacts with the United States as a whole. *See* Fed. R. Civ. P. 4(k)(2); *Hydentra HLP Int'l v. Sagan Ltd.*, 783 F. App'x 663, 665 (9th Cir. 2019). Because the "[t]he due process analysis under Rule 4(k)(2) is nearly identical," except it "consider[s] contacts with the nation as a whole," *Axiom Foods*, 874 F.3d at 1072 (citation omitted), targeting U.S. servers—including the signaling servers—suffices for the same reasons this Court found jurisdiction in California.[8]

NSO has not met its burden under Rule 4(k)(2) to identify another state where it is subject to jurisdiction. *See Holland Am. Line Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 462 (9th Cir. 2007). NSO provides no evidence that any FBI license supports jurisdiction in Washington, D.C., when NSO demonstrated Pegasus for the FBI in California, *see* Ex. 17 (DIVITTORIO_WHATSAPP_00000003), and deployed it in New Jersey, *see* Ex. 9 (Shohat Dep.) at 172:8-16. NSO argues that it *would* be subject to jurisdiction in Delaware if Westbridge were its alter ego, but that does not address where NSO itself is subject to jurisdiction, and NSO disputes that Westbridge is its alter ego. NSO is wrong, *see infra* § I.C.2, but the Court need not even reach that issue to find jurisdiction.[9]

C. NSO Purposefully Availed Itself of Doing Business in California

When a defendant does business in the forum, it "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 v. Denckla*, 357 U.S. 235, 253 (1958)). NSO admits that it created WhatsApp accounts for itself and its customers, and thus repeatedly consented to the Terms, including its California choice-of-law provision, and a forum selection clause governing at least NSO's disputes with WhatsApp. *See supra* § I.A; Ex. 13 (WA-NSO-00014825)

[8] NSO's cases do not show that Rule 4(k)(2) requires more extensive contacts for specific jurisdiction. *See Good Job Games Bilism Yazilim Ve Pazarlama A.S. v. SayGames LLC*, 458 F. Supp. 3d 1202, 1212 (N.D. Cal. 2020) (finding jurisdiction unreasonable when defendant only selected app store's option to sell mobile app in United States, among other countries), *rev'd and remanded*, 2021 WL 5861279 (9th Cir. Dec. 10, 2021) (remanding for discovery because "[t]he question of jurisdiction in the Internet age is not well-settled"); *Glencore Grain Rotterdam B.V. v. Shivnath Rai Harnarain Co.*, 284 F.3d 1114, 1127 (9th Cir. 2002) (concluding seven shipments years before suit were too "few in number and old in vintage" to exercise *general* jurisdiction).

[9] In the event the Court concludes that NSO is not subject to jurisdiction in California, but is subject to jurisdiction in another state, Plaintiffs respectfully request a transfer to that state's courts.

at -830-31; *Rankwave*, 2019 WL 8895237, at *5-6. The Court acknowledged this "would be relevant if it were combined with other facts to demonstrate that defendants purposefully availed themselves of California law." Dkt. No. 111 at 27. Discovery has now confirmed that NSO did purposefully avail itself by doing business in California related to Plaintiffs' claims. *See Ford Motor Co.*, 592 U.S. at 359, 362. First, NSO leased a California-based server for clients that NSO then hardcoded into 720 payloads used in the May 2019 attacks. Second, NSO partnered with a California firm to secure the funding to develop its products and to help market its products in California.

1. NSO Leased and Used a California Server for Its Customers

The undisputed evidence shows that NSO purposefully leased and used a California server in the attack. Records created during the May 2019 attack revealed that the data initially sent to the WhatsApp servers by the Malware Vectors contained IP addresses that represented servers, *see* Ex. 18 (Robinson Dep.) at 231:4-235:2, 337:22-340:4, from which the target device would "download and install additional data packets, including the Pegasus agent." Ex. 6 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 12. NSO had hardcoded each IP address into the data sent by the Malware Vectors. Dkt. No. 55-2 ¶ 4. One IP address used at least 700 times was 104.223.76.220, which is a QuadraNet server in California. *See* Dkt. No. 55-2 ¶ 4; Dkt. No. 55-6 ¶ 2 (showing server's coordinates in LA, and evidence of QuadraNet's LA-based data center). NSO provides no evidence that the server was located elsewhere.[10] Br. at 12.

The Court previously construed the pleadings as failing to allege that NSO "controlled where the third parties placed their servers," Dkt. No. 111 at 21, but discovery revealed that NSO clearly knew the server was in California and decided to use it in the attack as evidenced by NSO hardcoding that IP address into the malicious messages. NSO's customers could not have, because they only pushed a button to install Pegasus; the actual installation process was "a matter for NSO and the system to take care of, not a matter for customers to operate." Ex. 9 (Shohat Dep.) at 68:1-16. NSO could determine the server's location from the IP address alone. *See* Dkt. 55-6 (Mornin Decl.) ¶ 2.

NSO's denial that it had a contract or communications with QuadraNet is misleading. The

[10] The same information correctly placed the AWS server in Germany. Dkt. No. 55-2 ¶ 5 & Ex. 6.

QuadraNet server was subleased to 365 Online Technology JSC (d/b/a Greencloud VPS), a provider of virtual private servers ("VPS"). Ex. 19 (WA-NSO-00014771). NSO does not deny leasing VPS from Greencloud. Br. at 13-14. Ramon Eshkar, the head of NSO's White Services Team responsible for setting up infrastructure and accounts for clients, admitted he had "heard of" Greencloud VPS "in connection with [his] work for defendants," and that NSO set up VPS anonymously for its customers' use with Pegasus. Ex. 7 (Eshkar Dep.) at 151:3-155:1; *see* Ex. 5 (Gazneli Dep.) at 293:8-15. Moreover, NSO concealed its relationship with Greencloud by using a fake persona to lease the server. Greencloud's records indicate that the 104.223.76.220 IP address was leased in 2019 to a "Lisa Hoover," who paid in Bitcoin and registered with a Gmail account. *See* Ex. 20 (WA-NSO-00000019); Ex. 21 (WA-NSO-00000023) at -33-35. NSO admits to using Bitcoin "for setting up anonymized VPS," Ex. 7 (Eshkar Dep.) at 151:3-155:1, and produced documents indicating it used Gmail for anonymized accounts. *See, e.g.*, Ex. 22 (NSO_WHATSAPP_00007959). Because only NSO could have hardcoded the IP address into the Malware Vectors' messages, NSO must have leased the QuadraNet server, too. NSO therefore knowingly leased and repeatedly used a California-based server in the May 2019 attack.[11]

2. NSO Attempted to Create a Market for Its Spyware in California

The undisputed evidence shows that NSO purposefully availed itself of the privilege of doing business in California to obtain funding to develop the Malware Vectors and to market them.

In 2014, NSO sold a stake in its business to California-based firm Francisco Partners L.P. ("FP") for $115 million. Ex. 23 (WA-NSO-00067661) at 682; Ex. 24 (WA-NSO-00069802). FP owned NSO until February 2019, Ex. 9 (Shohat Dep.) at 124:12-19, and was "very involved" in running NSO's business as a managing director of NSO's parent OSY Technologies, *id.* at 42:13-43:13, 141:7-22; Ex. 25 (WA-NSO-00067809) at 11 (FP had "an integral role in Q's development"); *see Berkeley Lights, Inc. v. AbCellera Biologics Inc.*, 2021 WL 4497874, at *3 (N.D. Cal. Jan. 29,

[11] NSO's cases are completely distinguishable. *See, e.g.*, *Carefirst of Maryland, Inc. v. Carefirst Pregnancy Centers, Inc.*, 334 F.3d 390, 402 (4th Cir. 2003) (defendant hired a website hosting company that independently used forum servers); *Hungerstation LLC v. Fast Choice LLC*, 2020 WL 137160, at *1-2 (N.D. Cal. Jan. 13, 2020), *aff'd*, 2021 WL 1697886 (9th Cir. Apr. 29, 2021) (defendant incidentally used non-parties' forum servers while infringing plaintiff's trademarks).

2021) (concluding that "business dealings" with, and "acquisition of financing" from, "California companies" was conduct "purposefully directed at California"). With FP's capital, NSO developed the Heaven Malware Vector in 2018, and Eden by January 2019, and briefed Francisco Partners on their development. Ex. 5 (Gazneli Dep.) at 299:21-300:15, 256:16-258:9; Ex. 9 (Shohat Dep.) at 68:22-69:18; *see, e.g.*, Ex. 26 (FPM-00015812) at -890 ("massive introduction of Heaven vectors – huge effort (and success!).").

On FP's initiative, an NSO affiliate called Westbridge Technologies, Ltd. ("Westbridge") was established for "the purpose . . . [of] penetrat[ing] North America and generat[ing] sales" for NSO's products. Ex. 9 (Shohat Dep.) at 95:6-13; *id.* at 137:3-11 ("Westbridge was created . . . to expand business in North America"). In an Intercompany Distribution Agreement, NSO "appoint[ed] [Westbridge] as [its] distributor with respect to the Products," and granted Westbridge "[t]he non-exclusive right to market, distribute, and allow Resellers to sell and license the Products . . . solely in the Territory to Resellers and Customers, in accordance with the terms and conditions of this Agreement." Dkt. No. 396-3 (Shohat Decl.), Ex. D § 2.1. "Westbridge was authorized to sell in the United States," including in California. *See* Ex. 27 (Shaner Dep.) at 45:22-46:18, 204:19-205:15.

Westbridge advertised itself as the "North American Branch of NSO" and the "NSO Office in the US," and highlighted Pegasus's ability to extract information from WhatsApp. Ex. 28 (NSO_WHATSAPP_00046430); Ex. 29 (PX2023) (brochure for "Phantom"); Ex. 9 (Shohat Dep.) at 157:10-12 ("Phantom" is "a marketing name, for Pegasus in North America"). Westbridge marketed NSO's "expensive products" "wherever" agencies had "the biggest budgets," including in California, and demonstrated Pegasus for prospective California customers. *See* Ex. 27 (Shaner Dep.) at 289:12-290:24, 200:3-14, 211:4-21 (admitting marketing in San Francisco, San Bernadino, Los Angeles, and San Diego); Ex. 17 (DIVITTORIO_WHATSAPP_00000003) ("[W]e're in California, really good [Pegasus] demo yesterday for the FBI here in Los Angeles.").

The Court need not find that Westbridge is NSO's alter ego to find that NSO did business in California, as NSO contends. Br. at 14. The "alter ego test [is] for 'imput[ing]' *general* jurisdiction" from one entity to another. *Williams v. Yamaha Motor Co.*, 851 F.3d 1015, 1021 (9th Cir. 2017) (citation omitted). *Specific* jurisdiction may be based on Westbridge's marketing activity for NSO if

"the 'agent act[s] on the principal's behalf and subject to the principal's control.'" *Bluestar Genomics v. Song*, 2023 WL 4843994, at *23 (N.D. Cal. May 25, 2023) (quoting *Williams*, 851 F.3d at 1025). Indeed, the Supreme Court has acknowledged "marketing the product through a distributor who has agreed to serve as the sales agent in the forum State" can "indicate an intent or purpose to serve the market in the forum State." *Asahi Metal Indus. Co. v. Superior Ct. of California, Solano Cnty.*, 480 U.S. 102, 112 (1987) (plurality opinion); *see also Sinatra v. National Enquirer, Inc.*, 854 F.2d 1191, 1197 (9th Cir. 1988) (Swiss clinic subject to jurisdiction because it "instructed [an agent] to advertise [in California] and approved the ads placed"); *Williams*, 851 F.3d at 1023 n.3 (affirming *Sinatra* after *Daimler* because defendant in *Sinatra* "actively directed [agent's] advertising and sales efforts").

The preponderance of the evidence shows that Westbridge acted on NSO's behalf and that NSO directed and controlled Westbridge's marketing activities. NSO authorized Westbridge to market and demonstrate its products "as [NSO's] distributor," and "in accordance with the terms and conditions of [its] Agreement" with NSO. Dkt. No. 396-3 (Shohat Decl.), Ex. D § 2.1; Ex. 27 (Shaner Dep.) at 45:22-46:18, 204:19-205:15. NSO funded Westbridge's sales operations. Ex. 30 (DiVittorio Dep.) 132:17-134:1, 192:5-10, 200:9-17. NSO trained Westbridge's sales staff. *See* Ex. 27 (Shaner Dep.) at 33:22-36:21; Ex. 31 (NSO_WHATSAPP_00046461). Westbridge kept NSO informed of its marketing activities. *See, e.g.*, Ex. 27 (Shaner Dep.) at 152:3-8 ("[W]ould you generally make the [NSO] presales team aware when you were going to be doing a demonstration? A. Yes. Q. Consistently? A. Yes."); Ex. 17 (DIVITTORIO_WHATSAPP_00000003); Ex. 32 (DIVITTORIO_WHATSAPP_00000123). NSO and Westbridge employees coordinated on product demonstrations, with NSO deciding which sales servers to use and providing technical support "behind the scenes." *See* Ex. 27 (Shaner Dep.) at 148:19-152:13, 116:11-118:3; Ex. 9 (Shohat Dep.) at 170:1-171:10; *see, e.g*, Ex. 33 (SHANER_WHATSAPP_00001484); Dkt. No. 401-1, Ex. 36. NSO employees met with prospective customers in the U.S. *See* Ex. 30 (DiVittorio Dep.) at 163:7-16, 212:4-214:8; Ex. 34 (DIVITTORIO_WHATSAPP_00000120) (asking NSO engineer Aviv Melman "if we discussed you coming to California with us"). NSO's Chief Business Officer had input on Westbridge's pricing decisions, Ex. 30 (DiVittorio Dep.) at 248:22-249:15, and NSO reviewed and approved all of Westbridge's potential customers. Ex. 35 (Gil Dep.) at 64:11-68:19. Westbridge's sales efforts

resulted in a license agreement between the FBI and NSO, and with NSO employees installing the system in the United States. *See* Dkt. No. 396-5 (Akro. Decl.), Ex. N; Ex. 9 (Shohat Dep.) at 143:15-144:23. Westbridge sales agents admitted they also assisted NSO, at NSO's direction, with marketing and product demonstrations outside the United States. Ex. 27 (Shaner Dep.) at 180:25-184:9. The preponderance of the evidence demonstrates that NSO directed and controlled Westbridge's sales efforts, which suffices for specific jurisdiction in California. *See Williams*, 851 F.3d at 1023 n.3 (citing *Sinatra*, 854 F.2d at 1197). Westbridge's efforts to create a market for NSO's products in the United States generally also suffice under Rule 4(k)(2).

Even if it were necessary (it is not) to determine whether Westbridge is NSO's alter ego, the preponderance of the evidence shows that it was. An alter ego relationship exists when "there is such a unity of interest and ownership that the individuality, or separateness, of the said person and corporation has ceased" and "adherence to the fiction of the separate existence of the corporation would . . . sanction a fraud or promote injustice." *In re Schwarzkopf*, 626 F.3d 1032, 1038 (9th Cir. 2010). Courts consider several factors indicative of "a unity of interest and ownership." *City & Cnty. of San Francisco v. Purdue Pharma L.P.*, 491 F. Supp. 3d 610, 635 (N.D. Cal. 2020) (citing *Daewoo Elecs. Am. Inc. v. Opta Corp.*, 875 F.3d 1241, 1250 (9th Cir. 2017)). Several are present here: (1) NSO and Westbridge are owned by the same parent company, Ex. 9 (Shohat Dep.) at 76:1-77:1; Ex. 36 (PX2009); (2) NSO and Westbridge had overlapping directors and officers, as Omri Lavie, an NSO founder, was both a director of NSO and head of Westbridge, Ex. 9 (Shohat Dep.) at 73:20-25, 137:12-14, 142:2-143:14; (3) Westbridge had inadequate capitalization and was not "self-sustaining," Ex. 30 (DiVittorio Dep.) at 87:11-19; (4) there was commingling of funds because Westbridge's bank accounts and expenses were all funded by Defendants or OSY, *id.* at 98:13-99:8, 132:17-134:1, 192:5-10, 200:9-17; and (5) their employees overlapped, with Westbridge relying on Q Cyber's staff to file tax returns, *id.* at 94:2-13, 275:15-18, helping with NSO's own product demonstrations, Ex. 27 (Shaner Dep.) at 180:25-184:9, and using NSO and Q Cyber email addresses, Ex. 37 (PX2050). It would be "an inequitable result" if Westbridge's sales efforts were "treated as those of the corporation alone," *Wehlage v. EmpRes Healthcare, Inc.*, 791 F. Supp. 2d 774, 782 (N.D. Cal. 2011), when the entire purpose of setting up Westbridge as at least a nominally separate entity

was solely to facilitate the sale of NSO's products to U.S. customers. *See* Ex. 9 (Shohat Dep.) at 140:6-23. This record establishes that Westbridge was NSO's alter ego. At a minimum, it shows that NSO cannot prevail on summary judgment on an argument that Westbridge was *not* its alter ego.

3. Plaintiffs' Claims Arise from NSO's Business Activities in California

Plaintiffs' claims arise from or at least relate to NSO's California business activities. A "strict causal relationship" is not required, and it is sufficient if the claims "relate to" the forum contacts. *Ford Motor*, 592 U.S. at 359, 362. For example, in *Ford Motor*, the defendant was subject to suit for motor vehicle accidents in Montana and Minnesota because it "had systematically served a market [there] for the very vehicles that the plaintiffs allege malfunctioned and injured them in those States," even though the plaintiffs had unilaterally brought the vehicles to those states. *Id.* at 365. Here, Plaintiffs' claims directly arise from NSO's leasing and use of a California server more than 700 times in the attack. They also relate to the California funding NSO obtained to develop the Malware Vectors that are the subject of Plaintiffs' claims, and NSO's efforts to market them in California and the United States, including demonstrating those products and thus accessing Plaintiffs' servers from within the country. These contacts suffice for jurisdiction. *See Ayla, LLC v. Alya Skin Pty. Ltd.*, 11 F.4th 972, 981 (9th Cir. 2021) (marketing mostly "to an international or Australian audience does not alter the jurisdictional effect of marketing targeted specifically at the United States").

II. NSO IS LIABLE FOR PEGASUS AND ITS USE

A. NSO Is Liable for Its Own Conduct

Plaintiffs' Motion shows that NSO is liable under the CFAA and CDAFA for accessing WhatsApp's servers and the target devices without authorization. NSO argues that it was authorized to use the Malware Vectors against target devices that NSO owned, and that it is not liable for its customers' use of Pegasus against other WhatsApp users. Both arguments are meritless.

First, NSO admits that it used the Malware Vectors itself on WhatsApp's servers during development, testing, and product demonstrations, and they operated no differently than when customers utilized them operationally. Ex. 9 (Shohat Dep.) at 68:22-69:18; Ex. 5 (Gazneli Dep.) at 272:11-274:1, 289:22-290:24. NSO's claim that it only used the Malware Vectors to install Pegasus on, and extract information from, devices NSO owned and controlled is legally irrelevant, because it

still obtained the information through unauthorized access to WhatsApp's servers. *See infra* § III.A-B; Dkt. No. 401 at 13-20. The CFAA prohibits the *manner* in which information is obtained, even if the defendant has authorization to obtain it in other ways. *See Van Buren v. United States*, 593 U.S. 374, 385 (2021) (CFAA "forecloses" any "defense" that defendant "was 'entitled to obtain' the information if he had the right to access personnel files through another method").

Second, NSO is solely responsible for Pegasus's unauthorized access to WhatsApp's servers. *See, e.g.*, *Ryanair DAC v. Booking Holdings Inc.*, 636 F. Supp. 3d 490, 502 (D. Del. 2022) ("[L]iability can be based on 'the principal's active role in the CFAA violator's conduct' by directing, encouraging, or inducing a CFAA violation" (citation omitted)); 2 W. LaFave Subst. Crim. L. § 13.1(a) (3d ed.) (principal is liable for "acts or omissions" by one from whom he "withheld facts"). NSO owns the Pegasus technology, and only licenses it to customers to extract information from devices. Ex. 9 (Shohat Dep.) at 70:5-71:21 (customers "pay us for the capability to obtain intelligence"). NSO's customers' role is minimal. The customer only needed to enter the target device's number and "press Install, and Pegasus will install the agent on the device remotely without any engagement." Ex. 27 (Shaner Dep.) 82:24-89:25, 111:20-116:25; Ex. 38 (PX2051); Dkt. No. 1-1 at 37-38 ("The rest is done automatically by the system …."). In other words, the customer simply places an order for a target device's data, and NSO controls every aspect of the data retrieval and delivery process through its design of Pegasus. NSO admits the actual process for installing Pegasus through WhatsApp was "a matter for NSO and the system to take care of, not a matter for customers to operate." Ex. 9 (Shohat Dep.) at 68:1-16. NSO alone decided to access WhatsApp's servers when it designed (and continuously upgraded) Pegasus to do so at its customers' click of a button, "[b]ecause customers don't care which vector they use." *Id.*; *see* Ex. 5 (Gazneli Dep.) at 265:1-267:25 ("It was our decision whether to trigger it using WhatsApp messages or not."). NSO even secured the WhatsApp accounts used by Pegasus for customer installations, Ex. 7 (Eshkar Dep.) at 39:15-17, 151:3-153:8, and set up and controlled all the server infrastructure used to implant Pegasus and deliver the exfiltrated data to a customer. *See* Dkt. No. 1-1 at 37-38, 46-47.

Third, NSO is liable for conspiring with its customers to access target devices without authorization. *See* 18 U.S.C. § 1030(b); Dkt. No. 401 at 23-24. A conspiracy "requires 'specific

allegations of an agreement and common activities.'" *In re Lenovo Adware Litig.*, 2016 WL 6277245, at *6 (N.D. Cal. Oct. 27, 2016) (quoting *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 835 (N.D. Cal. 2014)). In *Ryanair DAC v. Booking Holdings Inc.*, the Court denied defendants' motion for summary judgment on a conspiracy claim where there were agreements that necessarily "require[d] circumventing" access limitations, and "defendants knew or should have known that its vendors were accessing protected portions of the Ryanair website without authorization." 2024 WL 3732498, at *23 (D. Del. June 17, 2024). Here, too, NSO entered agreements with its clients to use NSO's technology, *see* Ex. 6 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 15-16, which NSO had designed and intended to access WhatsApp's servers and target devices without authorization. NSO supported its clients' use of the technology by setting up infrastructure, providing technical support, and continuously circumventing security updates to "deliver[ ] the customers the software they needed." Ex. 5 (Gazneli Dep.) at 258:1-5; Ex. 6 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 15-16; Ex. 7 (Eshkar Dep.) at 39:15-17, 151:3-153:8.[12]

Finally, NSO is liable for trafficking in "password or similar information" that provides unauthorized access to WhatsApp's servers and users' target devices. 18 U.S.C. § 1030(a)(6); Cal. Penal Code § 502(c)(6); Dkt. No. 401 at 24-25. NSO admits that its technology permits a user to access the "same information [in a target device] that you could access if you had a password to the device." Ex. 5 (Gazneli Dep.) at 247:4-17. And NSO admits it marketed and licensed its technology to at least 45 customers across the globe in exchange for millions of dollars. *See* Ex. 7 (Eshkar Dep.) at 81:5-87:3 (discussing sales teams in various regions); Ex. 9 (Shohat Dep.) at 70:5-71:21; Ex. 6 (Defs. Supp. Resps. to Pls.' First Interrogs.) at 15-16; Ex. 39 (PX2045).

B. The Identity of NSO's Customers Provides No Defense

NSO's unsubstantiated allegations that its customers are all sovereigns is no defense. Even

[12] NSO is liable even if its co-conspirators are immune. *See Rabkin v. Dean*, 856 F. Supp. 543, 551 (N.D. Cal. 1994); *Risk v. Kingdom of Norway*, 707 F. Supp. 1159, 1167–69 (N.D. Cal. 1989). NSO's belief that they would use the spyware only for law enforcement purposes is not a defense, *see United States v. Christensen*, 828 F.3d 763, 794 (9th Cir. 2015), including because there is no foreign law enforcement exemption under the CFAA. *Cf.* 18 U.S.C. § 1030(f); *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 448–49 (N.D. Cal. 2018).

if they were sovereigns, the act of state doctrine would not apply, because it only "bars suit where '(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) (quoting *Credit Suisse v. U.S. Dist. Court*, 130 F.3d 1342, 1346 (9th Cir. 1997)) (alterations in original). None of these criteria are applicable here.

First, NSO provided no discovery regarding the identity of its customers other than the FBI, or that any, let alone all, were foreign sovereigns. NSO relies solely on Plaintiffs' belief that certain activity on Plaintiffs' platforms was associated with foreign governments. *See* Br. at 19 & n.15; Dkt. No. 396-5 (Akro. Decl.), Ex. S-V. That is not proof that any NSO customer was a sovereign.

Second, there is no evidence that Plaintiffs' claims concern any "official act," which are "actions that, by their nature, could only be undertaken by a sovereign power." *McKesson Corp. v. Islamic Republic of Iran*, 672 F.3d 1066, 1073-74 (D.C. Cir. 2012). NSO is a private company, and its unilateral development, testing, marketing, and use of its own commercial spyware cannot constitute "official acts." Nor do those activities become "official acts" simply because a sovereign uses that spyware, or based on NSO's say-so.[13] *See Saudi Arabia v. Nelson*, 507 U.S. 349, 360–61 (1993) ("[T]he issue is whether the particular actions that the foreign state performs (whatever the motive behind them) are the type of actions by which a private party engages in 'trade and traffic or commerce.'"); *see also, e.g.*, *McKesson*, 672 F.3d at 1073-74 (Iran's hostile takeover of a board of directors was not an "official act"); *Timberlane Lumber Co. v. Bank of Am., N.T. and S.A.*, 549 F.2d 597, 606 (9th Cir. 1976) ("[T]he [act of state] doctrine does not bestow a blank-check immunity upon all conduct blessed with some imprimatur of a foreign government.").

Third, NSO has provided no evidence that any conduct was undertaken by a sovereign "within its own territory," and in fact, the evidence shows the opposite is true. *Sea Breeze*, 899 F.3d at 1069. NSO developed the technology in Israel, WhatsApp's servers were accessed in the United States, *see*

[13] NSO also concedes some customers "misused the system" and "used [it] for a purpose other than fighting or preventing crime or terror." Ex. 9 (Shohat Dep.) at 24:1-7, 29:24-32:14.

Ex. 15 (WA-NSO-00166473), victims were located in dozens of countries, *see* Ex. 40 (WA-NSO-00192007) at -015-16, and at least 45 different customers licensed the Malware Vectors, Ex. 39 (PX2045). NSO's reliance on *In re Philippine National Bank*, 397 F.3d 768 (9th Cir. 2005) is misplaced. The Ninth Circuit applied the act of state doctrine to extraterritorial conduct in *Philippine National* only "in the extraordinary circumstances of th[at] case," where the Philippines seized its former President's property held by a state-owned bank's foreign branch. *Id.* at 773-74. NSO has provided no evidence of any similar "extraordinary" or even legitimate "underlying governmental interest" justifying applying the act of state doctrine to the extraterritorial conduct here. *Id.*

Finally, the doctrine "does not establish an exception for cases and controversies that may embarrass foreign governments, but merely requires that, in the process of deciding, the acts of foreign sovereigns taken within their own jurisdictions shall be deemed valid." *W.S. Kirkpatrick & Co. v. Env't Tectonics Corp., Int'l*, 493 U.S. 400, 409-10 (1990). In other words, it applies only "where resolution of a plaintiff's claims would *require* a court to evaluate a foreign sovereign's compliance *with its own laws*." *Royal Wulff Ventures LLC v. Primero Mining Corp.*, 938 F.3d 1085, 1093 (9th Cir. 2019). Unlike in *Du Daobin v. Cisco Systems, Inc.*, where the claims required a finding "that the Chinese government, with substantial assistance from Cisco, has engaged in multiple violations of international law," 2 F. Supp. 3d 717, 726 (D. Md. 2014), NSO would be liable under U.S. law even if its customers' actions were valid under foreign law.

III. NSO IS LIABLE ON PLAINTIFFS' CFAA CLAIMS

As demonstrated in Plaintiffs' Motion, NSO violated the CFAA when it accessed WhatsApp's servers and target devices without authorization or in excess of any purported authorization. NSO does not and cannot dispute that (1) NSO created and used a modified client application (the WIS) to access WhatsApp's servers to bypass the technological, code-based limitations built into the Official Client and WhatsApp's servers, Dkt. No. 401 at 15-17; (2) NSO circumvented Plaintiffs' 2018 security updates and continued accessing WhatsApp's servers after Plaintiffs had revoked their purported authorization, *id.* at 17-18; and (3) NSO developed and continued using a new WhatsApp-based Malware Vector even after Plaintiffs remediated the May 2019 attacks, disabled NSO's WhatsApp accounts, and filed this litigation, *id.* at 18-19. The FBI's

purported Pegasus license does not whitewash any of NSO's unlawful conduct.

A. Discovery Confirms NSO Accessed WhatsApp's Servers Without Authorization

The Court's Order on NSO's motion to dismiss concluded that the complaint did not state a "without authorization" claim as to WhatsApp's servers, based on the understanding that NSO implemented its attacks by "send[ing] messages using the WhatsApp app." Dkt. No. 111 at 37. The undisputed evidence developed through discovery confirms that it did not use "the WhatsApp app." NSO admits it accessed WhatsApp's servers using its own fake client—the WIS—to send messages that are not permitted by the Official Client, which confirms the Complaint's allegations that NSO "reverse-engineered the WhatsApp app and developed a program to enable them to emulate legitimate WhatsApp network traffic." Dkt. No. 1 ¶¶ 35, 53-54; Ex. 5 (Gazneli Dep.) at 161:20-162:3, 298:12-300:23, 301:18-302:19, 304:23-305:19; *see also* Dkt. No. 401 § II.A.2.a. NSO knew using a fake client was unauthorized and banned, *see* Ex. 16 (PX2033) at -959, and so leveraged real authentication keys from an Official Client to gain unauthorized access to WhatsApp's servers, and make the WIS appear to be an Official Client. Ex. 5 (Gazneli Dep.) at 161:20-162:3, 278:16-23. "[D]eceit vitiates consent," *Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2004), and NSO's use of misappropriated authentication keys is not a defense. *See Nosal II*, 844 F.3d at 1035.

It therefore makes no difference that "the messages Pegasus sent passed through the exact same areas of WhatsApp's servers as any other WhatsApp message," Br. at 22-23, because NSO had no authorization to use the WIS to access WhatsApp's servers at all. NSO provides no evidence of any general authorization "to access WhatsApp's servers." Br. at 21. As this Court recognized, "[b]y 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*." Dkt. No. 111 at 37. The Terms only provide authorization "to use our Services"—defined as "*our apps*, services, features, software, or website"—not to use WhatsApp's servers by any means. Ex. 13 (WA-NSO-00014825) at -825, -828. That is confirmed on a technological level, because the authentication keys needed to access WhatsApp servers are created when the Official Client is downloaded, installed, and registered. Ex. 3 (Gheorghe Dep.) at 135:20-140:1.

In addition, discovery has revealed new and previously unknown facts that Plaintiffs' security

upgrades in 2018 and 2019 prevented NSO's access to WhatsApp's servers and users' devices, but NSO continued accessing them anyway. *See* Dkt. No. 401 § II.A.2.b-c. NSO admits that WhatsApp's 2018 security upgrades blocked NSO's unauthorized access using the Heaven Malware Vector. *See* Ex. 5 (Gazneli Dep.) at 254:2-259:9. Yet NSO developed a new Malware Vector—Eden—to circumvent those changes. *Id.* at 254:2-258:16. Plaintiffs then disabled Eden. Ex. 5 (Gazneli Dep.) at 262:2-263:9. Plaintiffs also "purge[d]" the attackers' and NSO's WhatsApp accounts, *see* Exs. 41 & 42 (WA-NSO-00192176); Ex. 12 (SHANER_WHATSAPP_00001480) at -481, and filed this lawsuit, Dkt. No. 1. Yet, NSO admits it created a new Malware Vector and continued using it on WhatsApp even while this litigation was pending. *See* Ex. 5 (Gazneli Dep.) at 270:16-271:13. "[U]nauthorized access" includes "getting into the computer after categorically being barred from entry," *Nosal II*, 844 F.3d at 1034-36, and "technological gamesmanship . . . will not excuse liability." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016).

B. This Court Can Still Consider Plaintiffs' "Without Authorization" Theory

NSO argues that the Court's Order concluding that Plaintiffs' complaint had not adequately alleged a "without authorization" theory, Dkt. No. 111, "forecloses" NSO's liability on any "without authorization" theory regardless of the evidence.[14] Br. at 21. Not so. Courts deem new evidence to be "part of the complaint" where the other party was on notice of the theory and there was no prejudice, undue delay, bad faith, or dilatory motive. *In re JDS Uniphase Corp. Sec. Litig.*, 2007 WL 2429593, at *5-6 (N.D. Cal. Aug. 24, 2007). NSO had clear notice that Plaintiffs were exploring their "without authorization" theory in discovery.[15] And of course, NSO has long known that the Court's assumption in its Order that NSO had used the Official Client was incorrect.

NSO's cases only concern attempts to revive meritless claims, without new evidence. *See Chronic Tacos Enters., Inc. v. Chronic Tacos Huntington Beach, Inc.*, 2011 WL 6010265, at *2 (C.D. Cal. Nov. 28, 2011); *City of L.A. v. Bank of Am. Corp.*, 2015 WL 4880511, at *5 (C.D. Cal. May 11,

[14] The Court sustained Plaintiffs' "without authorization" theory as to the target devices (Dkt. No. 111 at 39-40), and NSO does not dispute that they were accessed without authorization. Br. at 20.

[15] *See, e.g.*, Dkt. No. 235-2 at 2, 10-11 (seeking information regarding "without authorization" claim); Dkt. No. 319-2 at 1-2, app'x A (same); Dkt. No. 235-4, Ex. M at 2 (seeking "the TECHNOLOGY used in the RELEVANT SPYWARE to communicate with WhatsApp").

2015). Plaintiffs' meritorious "without authorization" claim is backed by legal authority and undisputed evidence. To the extent necessary, Plaintiffs respectfully request that the Court either deem the pleadings amended to conform to the evidence or grant reconsideration to revisit this issue on this full record. *Desertrain v. City of Los Angeles*, 754 F.3d 1147, 1154 (9th Cir. 2014) (holding that new claims raised at summary judgment "should be allowed . . . by amendment"); *JDS Uniphase*, 2007 WL 2429593, at *5-6 ("deem[ing]" new alleged misstatements "part of the complaint").

C. NSO Exceeded Any Purported Authorization

Even if NSO had any authorization, NSO exceeded it by circumventing limitations built into the Official Client and WhatsApp's servers. This admitted conduct was not merely a "violation of the terms of use . . . without more," as NSO contends (Br. at 22), but a circumvention of "technological (or 'code-based') limitations on access," *Van Buren*, 593 U.S. at 390 n.8.

NSO first circumvented the technological limitations built into the Official Client. WhatsApp "designed it[s code] and . . . wrote it, assuming that the messages being sent are a part of the WhatsApp network and that they're official clients built by the WhatsApp team." Ex. 3 (Gheorghe Dep.) at 279:25-280:10. NSO circumvented those code-based limitations by building its own application—the WIS—to create and send messages that the Official Client technologically could not. Ex. 5 (Gazneli Dep.) at 298:12-300:23, 301:18-302:19, 304:23-305:19.

NSO also circumvented the servers' technological limitations. NSO knew in December 2018 that "WhatsApp had [sic] made changes in their servers that currently fail all installations." Ex. 8 (PX2007) at -098. Finding new ways to engage in the same activity is not "complying with WhatsApp's technological restrictions," as NSO claims. Br. at 23; *see also United States v. Phillips*, 477 F.3d 215, 220 (5th Cir. 2007) ("finding 'holes in . . . programs,' . . . amounts to obtaining unauthorized access" (quoting *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991))). Unlike the IT worker in *Abu v. Dickson*, who "lack[ed] notice that his access [was] unauthorized," 107 F.4th 508, 516 (6th Cir. 2024), NSO knew Plaintiffs revoked their access, and would block NSO again if it was discovered. Ex. 16 (PX2033) at -958-60; Ex. 5 (Gazneli Dep.) at 206:12-208:15.

By circumventing these technological limitations on access, NSO was able "to obtain or alter information in the computer that [NSO] was not entitled so to obtain or alter." 18 U.S.C.

§ 1030(e)(6). *Van Buren* does not require proof that NSO accessed parts of WhatsApp's servers that it could not with the Official Client, as NSO argues (Br. at 22-23), but merely that it "obtains *information* located in particular areas of the computer—*such as files, folders, or databases*—that are off limits to [NSO]." 593 U.S. at 396. That information need not come from the servers alone, because the CFAA prohibits using unauthorized access to "a *computer*" to obtain information from "any *protected computer*," not necessarily the same computer, 18 U.S.C. § 1030(a)(2)(C), (4); *see also Morris,* 928 F.2d at 511; Dkt. No. 401 at 21-22. In any event, the CFAA defines "computer" to "include[ ] any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(1); *see Nosal II*, 844 F.3d at 1032 n.2; Dkt. No. 401 at 22. NSO admits that, using the WIS, it obtained certain information directly from WhatsApp's servers, and obtained information "[v]ia the WhatsApp servers" from the target device, such as the structure of its operating system, and the location of crucial memory files, which "a regular WhatsApp user using the WhatsApp client app cannot obtain." Ex. 5 (Gazneli Dep.) at 294:10-15; 300:24-304:22; 306:12-307:15. NSO also admits that, using the WIS, it altered information by "forcing" WhatsApp's servers, which ordinarily only propose five relay servers, to add a sixth controlled by NSO, *see id.* at 189:25-194:5, and by "forging" a "server response" that only the server can send, *see id.* at 158:14-160:17. And of course, using the WIS, NSO was able to install Pegasus on target devices and extract a substantial amount of information. *See* Ex. 27 (Shaner Dep.) at 123:3-23, 193:4-195:14, 296:6-298:16; Dkt. No. 1-1, Ex. 10; Ex. 43 (Defs.' Resps. to Pls.' First RFAs) at 13-16. NSO is therefore liable even under an "exceeds authorized access" theory.

D. NSO Cannot Evade Liability Based on a "Law Enforcement Defense"

NSO claims that the FBI purchased a Pegasus license, and therefore it cannot be liable for maintaining Pegasus afterwards. NSO fails to prove that the FBI in fact licensed Pegasus. NSO has not produced any license agreement, but instead relies on a letter certifying that a Delaware company is authorized to purchase Pegasus on the FBI's behalf, Ex. 30 (DiVittorio Dep.) at 264:7-18, and a certificate submitted to the Israeli government indicating how the FBI intended to use Pegasus. *See* Akro. Decl., Ex. N, O. NSO therefore cannot show any alleged FBI license excuses NSO's conduct. A government contract provides a defense only if "(1) the United States set forth 'reasonably precise

specifications'; (2) 'the equipment conformed to those specifications'; and (3) the supplier provided the United States with adequate warnings of the dangers." *Rodriguez v. Lockheed Martin Corp.*, 627 F.3d 1259, 1266 (9th Cir. 2010). NSO provides no evidence the FBI "required NSO to maintain Pegasus in an operational state." Br. at 23. The certificate's bare reference to "Maintenance," Akro. Decl., Ex. N, does not show the FBI actually contracted for maintenance, what that required NSO to do, or whether it applied to the WhatsApp-specific Malware Vectors at issue here. Ex. 7 (Eshkar Dep.) at 122:24-125:24; Ex. 35 (Gil Dep.) at 88:25-89:14. There also is no evidence the FBI was informed about how they worked so that the FBI could have authorized NSO's use of WhatsApp. Ex. 9 (Shohat Dep.) at 68:1-16. Furthermore, NSO "maintained" Pegasus for 45 different customers. Ex. 39 (PX2045). NSO's independent conduct is not transformed into the *FBI's* "investigative, protective, or intelligence activity," 18 U.S.C. § 1030(f), simply because it purchased one license.[16]

IV. NSO IS LIABLE ON PLAINTIFFS' CDAFA CLAIM

NSO is liable under CDAFA for the same reasons. *See supra* §§ II, III; Dkt. No. 401 at 25; *Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1260 (N.D. Cal. 2022). NSO concedes that the CDAFA applies if NSO "knowingly access[ed] a computer *in California*." Br. at 25. There is no dispute that it did. NSO intentionally used California-based WhatsApp relay servers at least 43 times. *See supra* § I.B; Ex. 15 (WA-NSO-00166473); Ex. 3 (Gheorghe Dep.) at 206:8-19; Ex. 5 (Gazneli Dep.) at 258:6-22. NSO had "advance knowledge or control of which relay servers any Pegasus message passed through," Br. at 25, because it logged their IP addresses, and decided which to use. *See supra* § I.B. In addition, NSO also knowingly used the California-based QuadraNet server over 700 times. *See supra* § I.C.2; Dkt. No. 55-2. There is therefore a "'sufficient nexus between California and [NSO's] alleged wrongful conduct' to permit application of California law." Br. at 25 (quoting *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *6 (N.D. Cal. Nov. 20, 2020)).

CONCLUSION

For the foregoing reasons, the Court should deny NSO's motion for summary judgment.

[16] Even if NSO attempted to rely on the FBI's out-of-court statements, they indicate that the FBI never used Pegasus "operationally" or "in any investigation" at all. Ex. 44 (C. Wray Tr.) at 37.

Dated: October 11, 2024

Respectfully Submitted,

DAVIS POLK & WARDWELL LLP

By: */s/ Micah G. Block*

Greg D. Andres
Antonio J. Perez-Marques
Craig T. Cagney
Gina Cora
Luca Marzorati
(admitted *pro hac vice*)
DAVIS POLK & WARDWELL LLP
450 Lexington Avenue
New York, New York 10017
Telephone: (212) 450-4000
Facsimile: (212) 701-5800
Email: greg.andres@davispolk.com
antonio.perez@davispolk.com
craig.cagney@davispolk.com
gina.cora@davispolk.com
luca.marzorati@davispolk.com

Micah G. Block (SBN 270712)
DAVIS POLK & WARDWELL LLP
1600 El Camino Real
Menlo Park, California 94025
Telephone: (650) 752-2000
Facsimile: (650) 752-2111
Email: micah.block@davispolk.com

Attorneys for Plaintiffs
WhatsApp LLC and Meta Platforms, Inc.