PAUL HOFFMAN #71244
JOHN WASHINGTON #315991
Schonbrun, Seplow, Harris,
Hoffman & Zeldes LLP
200 Pier Avenue, Suite 226
Hermosa Beach, CA 90254
T: (424) 297-0114
F: (310) 399-7040
hoffpaul@aol.com

COREY STOUGHTON, *Pro Hac Vice*
ALVARO MON CUREÑO, *Pro Hac Vice*
Selendy Gay PLLC
1290 Avenue of the Americas
New York, NY 10104
T: (212) 390-9306
cstoughton@selendygay.com

*Counsel for Plaintiffs**

CARRIE DECELL, *Pro Hac Vice*
JAMEEL JAFFER, *Pro Hac Vice*
ALEX ABDO, *Pro Hac Vice*
STEPHANIE KRENT, *Pro Hac Vice*
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
T: (646) 745-8500
F: (646) 661-3361
carrie.decell@knightcolumbia.org

*Counsel for Plaintiffs**

**See Signature Page for Complete List of Plaintiffs*

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CARLOS DADA, SERGIO ARAUZ, GABRIELA CÁCERES GUTIÉRREZ, JULIA GAVARRETE, ROMAN GRESSIER, GABRIEL LABRADOR, ANA BEATRIZ LAZO ESCOBAR, EFREN LEMUS, DANIEL LIZÁRRAGA, CARLOS LÓPEZ SALAMANCA, CARLOS MARTÍNEZ, ÓSCAR MARTÍNEZ, MARÍA LUZ NÓCHEZ, VÍCTOR PEÑA, NELSON RAUDA ZABLAH, DANIEL REYES MARTÍNEZ, MAURICIO SANDOVAL SORIANO, and JOSÉ LUIS SANZ,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No. 3:22-cv-07513-JD

PLAINTIFFS' OPPOSITION TO DEFENDANTS' RENEWED NOTICE OF MOTION AND MOTION TO DISMISS FIRST AMENDED COMPLAINT

Hearing Date: November 20, 2025
Time: 10:00 a.m.
Ctrm: 11

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTRODUCTION 1

BACKGROUND 1

ARGUMENT 3

I. This Court is the proper forum for this case. 3

II. This Court has personal jurisdiction under California's long-arm statute. 6

A. Defendants carried out tortious conduct in California. 7

B. Defendants purposefully directed claim-related conduct at California. 10

C. This Court's exercise of personal jurisdiction is reasonable. 11

III. This Court has personal jurisdiction under the federal long-arm statute. 12

IV. Plaintiffs have adequately alleged their claims. 13

A. Plaintiffs have adequately alleged violations of the CFAA. 13

B. Plaintiffs have adequately alleged violations of California law. 15

CONCLUSION 15

TABLE OF AUTHORITIES

Cases

42 Ventures, LLC v. Mav, 2022 WL 2400030 (D. Haw. June 15, 2022) 9, 13

Alhathloul v. DarkMatter Grp., 2025 WL 2320474 (D. Or. Aug. 12, 2025) ..... passim

Apple Inc. v. NSO Grp. Techs. Ltd., 2024 WL 251448 (N.D. Cal. Jan. 23, 2024) 6, 13, 14

Atchley v. AstraZeneca UK Ltd., 22 F.4th 204 (D.C. Cir. 2022) 8, 13

Ayla, LLC v. Alya Skin Pty. Ltd., 11 F.4th 972 (9th Cir. 2021) 8, 10, 11, 12

Bos. Telecomms. Grp., Inc. v. Wood, 588 F.3d 1201 (9th Cir. 2009) 3, 11

Briskin v. Shopify, Inc., 135 F.4th 739 (9th Cir. 2025) (*en banc*) ..... passim

Burri L. PA v. Skurla, 35 F.4th 1207 (9th Cir. 2022) 8, 11

Calder v. Jones, 465 U.S. 783 (1984) 8

Carijano v. Occidental Petroleum Corp., 643 F.3d 1216 (9th Cir. 2011) 3, 5

Chloe SAS v. Sawabeh Info. Servs. Co, 2012 WL 7679386 (C.D. Cal. May 3, 2012) 5

City of Almaty v. Khrapunov, 685 F. App'x 634 (9th Cir. 2017) 3, 4

Cohodes v. MiMedx Grp., Inc., 2022 WL 15523079 (N.D. Cal. Oct. 27, 2022) 8

Cooper v. Tokyo Elec. Power Co., Inc., 860 F.3d 1193 (9th Cir. 2017) 5

COR Sec. Holdings Inc. v. Banc of Cal., N.A., 2018 WL 4860032 (C.D. Cal. Feb. 12, 2018) 15

Corallo v. NSO Grp. Techs. Ltd., 2024 WL 4367924 (N.D. Cal. Sept. 30, 2024) 4, 10

Dole Food Co. v. Watts, 303 F.3d 1104 (9th Cir. 2002) 3

Finan v. Lafarge S.A., 2025 WL 2504317 (E.D.N.Y. Aug. 29, 2025) 12

Finjan, Inc. v. Cisco Sys., Inc., 2019 WL 667766 (N.D. Cal. Feb. 19, 2019) 6

Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct., 141 S. Ct. 1017 (2021) 8

Fraser v. Mint Mobile, LLC, 2022 WL 1240864 (N.D. Cal. Apr. 27, 2022) 15

Freestream Aircraft (Bermuda) Ltd. v. Aero L. Grp., 905 F.3d 597 (9th Cir. 2018) 7

Fuld v. Palestinian Liberation Org., 606 U.S. 1 (2025) 1, 12, 13

Gates Learjet Corp. v. Jensen, 743 F.2d 1325 (9th Cir. 1984) 4

HB Prods., Inc. v. Faizan, 603 F. Supp. 3d 910 (D. Haw. 2022) 8

Hungerstation LLC v. Fast Choice LLC, 857 F. App'x 349 (9th Cir. 2021) 9

Hydentra HLP Int. Ltd. v. Sagan Ltd., 783 F. App'x 663 (9th Cir. 2019) 11

In re Apple & AT & TM Antitrust Litig., 596 F. Supp. 2d 1288 (N.D. Cal. 2008) 14

In re iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2012) 14

In re Meta Healthcare Pixel Litig., 713 F. Supp. 3d 650 (N.D. Cal. 2024) 15

In re W. States Wholesale Nat. Gas Antitrust Litig., 715 F.3d 716 (9th Cir. 2013) 7

Jenkins v. Pooke, 2009 WL 10692010 (N.D. Cal. July 13, 2009), *R&R adopted*, 2009 WL 10691375 (N.D. Cal. Aug. 19, 2009) 10

Keeton v. Hustler Mag., Inc., 465 U.S. 770 (1984) 8

Khashoggi v. NSO Grp. Techs. Ltd., 138 F.4th 152 (4th Cir. 2025) 9

Lamont v. Postmaster Gen. of U.S., 381 U.S. 301 (1965) 4

Lang Van, Inc. v. VNG Corp., 40 F.4th 1034 (9th Cir. 2022) 10, 13

Licci ex rel. Licci v. Lebanese Canadian Bank, SAL, 732 F.3d 161 (2d Cir. 2013) 8

Lineberry v. AddShopper, Inc., 2025 WL 551864 (N.D. Cal. Feb. 19, 2025) 15

Lueck v. Sundstrand Corp., 236 F.3d 1137 (9th Cir. 2001) 6

MacDermid, Inc. v. Deiter, 702 F.3d 725 (2d Cir. 2012) 9

Microsoft Corp. v. Does 1–2, 2021 WL 4755518 (E.D.N.Y. May 28, 2021) 13

Multiven, Inc. v. Cisco Systems, Inc., 725 F. Supp. 2d 887 (N.D. Cal. 2010) 15

NetApp, Inc. v. Nimble Storage, Inc., 41 F. Supp. 3d 816 (N.D. Cal. 2014) 9, 10

Neuralstem, Inc. v. ReNeuron, Ltd., 365 F. App'x 770 (9th Cir. 2010) 5

Nowak v. Xapo, Inc., 2020 WL 6822888 (N.D. Cal. Nov. 20, 2020) 15

Paccar Int'l, Inc. v. Com. Bank of Kuwait, S.A.K., 757 F.2d 1058 (9th Cir. 1985) 7

Ridgway v. Phillips, 383 F. Supp. 3d 938 (N.D. Cal. 2019) 5

Rodriguez v. Google LLC, 772 F. Supp. 3d 1093 (N.D. Cal. 2025) 15

Sinatra v. Nat'l Enquirer, Inc., 854 F.2d 1191 (9th Cir. 1988) 11

Soo Park v. Thompson, 851 F.3d 910 (9th Cir. 2017) 8

Tuazon v. R.J. Reynolds Tobacco Co., 433 F.3d 1163 (9th Cir. 2006) 4, 5

United States v. Millot, 433 F.3d 1057 (8th Cir. 2006) 14

United States v. Yücel, 97 F. Supp. 3d 413 (S.D.N.Y. 2015) 13

Walden v. Fiore, 571 U.S. 277 (2014) 7, 8

Walsh v. Microsoft Corp., 63 F. Supp. 3d 1312 (W.D. Wash. 2014) 14

WhatsApp Inc. v. NSO Group Techs. Ltd., No. 4:19-cv-07123 (N.D. Cal. Oct. 29, 2019) 4, 5

WhatsApp Inc. v. NSO Grp. Techs. Ltd., 2023 WL 7726411 (N.D. Cal. Nov. 15, 2023) 6

WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649 (N.D. Cal. 2020) 10, 11, 12, 15

Will Co., Ltd. v. Lee, 47 F.4th 917 (9th Cir. 2022) 9, 11, 13

Statutes

Cal. Comprehensive Comput. Data Access and Fraud Act, Cal. Penal Code § 502 1

Comput. Fraud and Abuse Act, 18 U.S.C. § 1030 1

Foreign Judgments Enforcement Law, 5718–1958, LSI 12 82 (1958), as amended (Isr.) 6

Other Authorities

147 Cong. Rec. S10990–02, S10997 (2001) 12

Brief for Microsoft Corp., et al., *Dada v. NSO Grp. Techs. Ltd.*, No. 24-2179 (9th Cir. July 8, 2025) 3

Compl., *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 3:21-cv-09078 (N.D. Cal. Nov. 23, 2021) 11

Israel, the West Bank and Gaza Travel Advisory, Dept. of State, https://perma.cc/UGA3-3BLJ (July 13, 2025) 5

Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L.R. 1561 (2010) 12

Pl.'s Mot. for Vol. Dismissal, *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 3:21-cv-09078 (N.D. Cal. Nov. 12, 2024) 3

U.S. Off. of the Dir. of Nat'l Intel., *Annual Threat Assessment of the U.S. Intelligence Community* 30–31 (2024) 4

Regulations

Exec. Order No. 14,093, 88 Fed. Reg. 18,957 (Mar. 27, 2023)..... 4

INTRODUCTION

Defendants developed and deployed their signature spyware system, "Pegasus," through the deliberate and sustained abuse of the software and services of California-based technology company Apple. Plaintiffs are members of the news organization El Faro whose iPhones were subjected to hundreds of Pegasus attacks, and who seek to hold Defendants accountable for their role in those attacks under U.S. and California law. Considering the deference due to Plaintiffs' choice of forum and the balance of *forum non conveniens* factors, this case belongs in this forum. Defendants are also subject to specific personal jurisdiction in this forum, because Plaintiffs' claims directly arise from Defendants' abuse of Apple's infrastructure, which was Defendants' "own choice and not random, isolated, or fortuitous." *Briskin v. Shopify, Inc.*, 135 F.4th 739, 758 (9th Cir. 2025) (*en banc*) (cleaned up). And this abuse easily satisfies the "more flexible jurisdictional inquiry" applicable under the U.S. long-arm statute. *Fuld v. Palestinian Liberation Org.*, 606 U.S. 1, 16 (2025). Finally, Plaintiffs have sufficiently pleaded their claims under U.S. and California law. Defendants designed Pegasus to provide unauthorized access to targets' devices in violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and California's equivalent ("CDAFA"), Cal. Penal Code § 502. Plaintiffs have adequately alleged damage and loss resulting from the Pegasus attacks, establishing statutory standing and demonstrating trespass to chattels. For these reasons and the further reasons provided below, the Court should deny Defendants' Renewed Motion to Dismiss ("RM"), ECF No. 94.

BACKGROUND

The Court is already familiar with Plaintiffs' allegations. For present purposes, the essential point is that the development and deployment of Pegasus against Plaintiffs entailed the targeted abuse of Apple's software and services, through repeated access to its servers in California and the United States, in violation of U.S. and California law. *See* Am. Compl. ("AC") ¶ 3, ECF No. 31.

At the core of Defendants' business is the development and deployment of "zero-click" exploits of vulnerabilities in Apple's software and services, through which Pegasus is delivered remotely and covertly to targets' iPhones. AC ¶¶ 3, 40. Defendants created Apple ID accounts "to discover vulnerabilities in Apple's software, to probe Apple's servers and services, and to test the

software that Defendants developed to infect iPhones with Pegasus." *Id.* ¶ 42. Defendants and their clients then use Apple ID accounts to deliver Pegasus through those exploits to targets' iPhones. *Id.* ¶ 43. Defendants designed Pegasus to disable Apple safeguards and to mimic Apple processes to avoid alerting Apple or Apple users to its presence. *Id.* ¶ 40.

Defendants sell Pegasus to government clients, including governments responsible for grave human rights abuses. AC ¶¶ 36, 46–49. They train those clients in the use of Pegasus and assist them in its deployment and operation. *Id.* ¶¶ 36, 44. Once a target's iPhone is infected, Pegasus operators (whether Defendants' employees or their clients) use command-and-control servers configured and maintained by Defendants to take control of the target's iPhone for however long the infection lasts. *Id.* ¶ 44. Operators can issue commands to the device to, e.g., exfiltrate data, enable location tracking, record audio, or take photographs. *Id.* ¶¶ 2, 37–39, 40. Operators can also access and extract data from cloud-based accounts, like iCloud or Google Drive. *Id.* ¶ 39.

Plaintiffs and their El Faro colleagues suffered 226 Pegasus attacks over the course of 18 months. *See* AC ¶¶ 5, 53–59, 63. The exploits used to deploy Pegasus against Plaintiffs, known as KISMET and FORCEDENTRY, relied on "Apple ID accounts to send malicious data through Apple's iMessage service" and temporarily stored the Pegasus file on Apple's iCloud servers before delivery to the target's iPhone. *Id.* ¶¶ 3, 43. The attacks against Plaintiffs damaged iPhones they used for both personal and professional purposes by "disabl[ing] certain Apple iOS features on the devices, infect[ing] the devices with Pegasus, [and] enabl[ing] Defendants and their clients to issue commands to the devices without Plaintiffs' knowledge or consent." *Id.* ¶ 63; *see, e.g.*, *id.* ¶¶ 65–66. Plaintiffs' "communications and activities [were] monitored, and their personal data accessed and stolen," including from cloud-based accounts. *Id.* ¶ 5; *see id.* ¶¶ 63, 105. The attacks compromised Plaintiffs' communications with confidential sources, including U.S. Embassy officials. *Id.* ¶¶ 5, 105, 121, 133. After learning of the attacks, Plaintiffs engaged in extensive efforts to investigate and remediate the resulting harms. *Id.* ¶¶ 60–61; *see, e.g.*, *id.* ¶¶ 67, 71, 79.

Plaintiffs filed their Amended Complaint in December 2022. ECF No. 31. In March 2024, this Court dismissed the case on the ground of *forum non conveniens*. ECF No. 78. In July 2025, the Ninth Circuit vacated the dismissal and remanded the case after concluding that this Court had

misapprehended or misapplied the relevant standard, explaining that it apparently "gave little to no deference to Plaintiffs' choice of forum, overlooked the allegations of the operative complaint, and shifted the burden of proof from Defendants to Plaintiffs." ECF No. 97.1, at 4.

ARGUMENT

I. This Court is the proper forum for this case.

Defendants fail to justify dismissal for *forum non conveniens* based on the balance of relevant public and private interest factors. *See Carijano v. Occidental Petroleum Corp.*, 643 F.3d 1216, 1224 (9th Cir. 2011); *id.* at 1229, 1232 (reciting factors). As clarified on appeal, the Court "should apply an intermediate level of deference" to Plaintiffs' choice of this forum, since they include a U.S. citizen and two U.S. residents. ECF No. 97.1, at 3; *see* AC ¶¶ 18, 28, 31. Defendants must therefore "'satisfy a heavy burden of proof,' such that 'unless the balance is strongly in favor of the defendant, the plaintiff's choice of forum should rarely be disturbed.'" ECF No. 97.1, at 4 (quoting *Bos. Telecomms. Grp., Inc. v. Wood*, 588 F.3d 1201, 1207 (9th Cir. 2009) (cleaned up)).

Public Interest. The first public-interest factor overwhelmingly favors this forum because both California and the United States have strong interests in this case.[1] California has a compelling interest in protecting California companies from being used as spyware vectors in violation of California law. *See Dole Food Co. v. Watts*, 303 F.3d 1104, 1119 (9th Cir. 2002). Defendants targeted Apple by accessing its servers, including those in California, to develop and deploy Pegasus against its users, including Plaintiffs, all in violation of California and U.S. law. AC ¶¶ 3, 13, 41–45. The fact that some harms resulting from those unlawful acts were felt outside California does not diminish its interest in this case.[2] *See Bos. Telecomms.*, 588 F.3d at 1212; *City of Almaty v. Khrapunov*, 685 F. App'x 634, 636 (9th Cir. 2017). California also has a strong interest in

[1] The Court "ask[s] only if there is an identifiable local interest in the controversy, not whether another forum also has an interest," *Bos. Telecomms.*, 588 F.3d at 1212 (cleaned up), so Israel's interests, *see* RM 6, are irrelevant. Defendants do not argue El Salvador as an alternative forum.

[2] Even in moving to dismiss, Apple "continue[d] to believe in the merits of its claims" against Defendants. Pl.'s Mot. for Vol. Dismissal 1, *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 3:21-cv-09078 (N.D. Cal. Nov. 12, 2024), ECF No. 98; *see also* Brief for Microsoft Corp., et al. 3, *Dada v. NSO Grp. Techs. Ltd.*, No. 24-2179 (9th Cir.), ECF No. 29 (emphasizing local interests in "protecting U.S. technology companies from hackers . . . exploiting their products and services").

protecting El Faro's significant California readership's access to El Faro's reporting, which was compromised by the Pegasus attacks. AC ¶¶ 4, 6, 62; *see Lamont v. Postmaster Gen. of U.S.*, 381 U.S. 301, 307 (1965) (recognizing First Amendment interest in reading foreign sources). Defendants entirely ignore the United States' clearly and repeatedly expressed interests in the exact issues presented by this case, which involves spyware attacks against journalists—including a U.S. citizen—that compromised their communications with U.S. Embassy officials. AC ¶¶ 5, 18, 105, 121, 133;[3] *see id.* ¶ 50 (describing addition of NSO Group to U.S. "Entity List" for "suppl[ying] spyware to foreign governments that used" it against "journalists" and "embassy workers"); *see also* Exec. Order No. 14,093, 88 Fed. Reg. 18,957, 18,957 (Mar. 27, 2023) (declaring a "fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware" given "core [U.S.] interests" in "defending . . . journalists against threats to their freedom and dignity"); U.S. Off. of the Dir. of Nat'l Intel., *Annual Threat Assessment of the U.S. Intelligence Community* 30–31 (2024) (identifying use of commercial spyware "to target dissidents and journalists" as creating "risks to U.S. national security").[4]

The remaining public interest factors likewise favor this forum. On the second factor, this district is most familiar with the governing U.S. and California law, given the litigation of lawsuits raising similar claims here. *See, e.g.*, *WhatsApp Inc. v. NSO Group Techs. Ltd.*, No. 4:19-cv-07123 (N.D. Cal. Oct. 29, 2019). Defendants make no mention of this factor. Nor do they present any evidence as to the relative congestion of U.S. and Israeli courts, as they must to count the fourth factor in their column. *See Gates Learjet Corp. v. Jensen*, 743 F.2d 1325, 1337 (9th Cir. 1984); *see also City of Almaty*, 685 F. App'x at 636. Finally, with respect to the third and fifth factors, given the strong local interests identified above and the fact that related litigation has proceeded through a damages trial in this forum, *see WhatsApp*, No. 4:19-cv-07123, ECF No. 736, no burden on local courts and juries or costs of resolving the dispute are unrelated to the forum's interests. *See Tuazon v. R.J. Reynolds Tobacco Co.*, 433 F.3d 1163, 1182 (9th Cir. 2006).

[3] These facts distinguish this case from *Corallo v. NSO Group*, where the plaintiff was a Dutch citizen residing in Sint Maarten. 2024 WL 4367924, at *1 (N.D. Cal. Sept. 30, 2024).

[4] Plaintiffs respectfully request that the Court take judicial notice of these statements. *See* Fed. R. Evid. 201(b)(2); *Kater v. Churchill Downs Inc.*, 886 F.3d 784, 788 n.3 (9th Cir. 2018).

Private Interest. The private-interest factors also favor this forum. On the first and second factors, given the Plaintiffs' residences in the United States and Central America, AC ¶¶ 14–31, California is clearly more convenient than Israel. *See Cooper v. Tokyo Elec. Power Co., Inc.*, 860 F.3d 1193, 1211 (9th Cir. 2017) (analyzing all parties' residences at time of filing, though injuries occurred in alternative forum); *Carijano*, 643 F.3d at 1227, 1230 (weighing Peruvian plaintiffs' "willingness to travel" to U.S. forum with co-plaintiffs' U.S. residency against dismissal). Almost all Plaintiffs would be required to travel much farther to litigate this case in Israel, at great expense and risk to their safety.[5] *See Chloe SAS v. Sawabeh Info. Servs. Co*, 2012 WL 7679386, at *23–24 (C.D. Cal. May 3, 2012). Moreover, most Plaintiffs are journalists working for an independent news outlet who took no affirmative steps to associate themselves with Israel and who already have U.S. *pro bono* counsel; in contrast, Defendants are sophisticated corporations that charge multi-million-dollar fees, have hired U.S. firms and marketed their technology to U.S. and California agencies, AC ¶ 34, and have already litigated related cases in this forum, also with U.S. counsel, *see, e.g.*, *WhatsApp*, No. 4:19-cv-07123. Therefore, it is far *less* convenient for Plaintiffs to litigate in Israel than it is for Defendants to litigate in California. *See Ridgway v. Phillips*, 383 F. Supp. 3d 938, 947 (N.D. Cal. 2019) (weighing against dismissal facts that defendant regularly traveled to California and that plaintiff took no "affirmative action to establish contacts" with alternative forum); *Tuazon*, 433 F.3d at 1180; *Chloe SAS*, 2012 WL 7679386, at *24.

On the third factor, Defendants fail to explain "the materiality and importance of the anticipated witnesses and documentary evidence" located outside the forum. *Neuralstem, Inc. v. ReNeuron, Ltd.*, 365 F. App'x 770, 772 (9th Cir. 2010) (cleaned up). They gesture at unspecified evidence and witnesses abroad, RM 4, but—as the Ninth Circuit noted—Plaintiffs' allegations focus on Defendants' deliberate targeting of Apple's infrastructure, AC ¶¶ 3, 39, 41–44, so much of the relevant evidence will be in Apple's control in California. ECF No. 97.1, at 4–5 (highlighting "allegations that Defendants facilitated the Pegasus attacks by creating Apple ID accounts and interacting extensively with Apple's U.S.-based servers, many of which are in California" (cleaned

[5] *See, e.g.*, *Israel, the West Bank and Gaza Travel Advisory*, Dept. of State, https://perma.cc/UGA3-3BLJ (July 13, 2025). Plaintiffs request judicial notice. *See supra* n.4.

up)); *see Lueck v. Sundstrand Corp.*, 236 F.3d 1137, 1146–47 (9th Cir. 2001) (holding that location of evidence is especially relevant when neither party controls it). Defendants nod to Israeli export law, RM 4, but provide "no basis for concluding that . . . Israeli restrictions would apply with any less force if the case were to be litigated in Israel." *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 2023 WL 7726411, at *2 (N.D. Cal. Nov. 15, 2023). Nor do discovery sanctions imposed in *WhatsApp* counsel against litigating this case here. *See* RM 4–5; *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 2024 WL 5190365, at *4–6 (N.D. Cal. Dec. 20, 2024). There, the court considered Defendants' arguments—including Israeli export law—and tailored discovery orders appropriately. Defendants' refusal to heed those orders should not earn them a "get out of forum free" card.

None of the remaining factors weighs in favor of dismissing this case, either. On the fourth and fifth factors, Defendants do not argue that there are unwilling witnesses who cannot be compelled to testify in California or that litigating here would impose significant costs on them. In any event, Defendants control the availability of their own witnesses, and they concede that Israeli witnesses may be compelled to testify in U.S. proceedings. Decl. of Roy Blecher ¶ 2, ECF No. 46-1; *see, e.g.*, *Finjan, Inc. v. Cisco Sys., Inc.*, 2019 WL 667766, at *1 (N.D. Cal. Feb. 19, 2019). Further, any litigation costs could be mitigated by using alternative mechanisms like "remote video depositions." *See Apple Inc. v. NSO Grp. Techs. Ltd.*, 2024 WL 251448, at *2 (N.D. Cal. Jan. 23, 2024). Finally, on the sixth factor, Defendants argue that enforcement of an Israeli judgment might be "easier" in Israel, RM 4 n.1, but they do not demonstrate that a judgment rendered in California would be unenforceable, and Plaintiffs would bear the burden of enforcement in any event. *See* § 3, Foreign Judgments Enforcement Law, 5718–1958, LSI 12 82 (1958), as amended (Isr.); *Apple*, 2024 WL 251448, at *2; *WhatsApp*, 2023 WL 7726411, at *3. The private-interest factors thus favor this forum, and the balance of factors overwhelmingly favors this forum, especially given the deference due to Plaintiffs.

II. This Court has personal jurisdiction under California's long-arm statute.

California's long-arm statute provides for personal jurisdiction to the full extent permitted by the Due Process Clause. *Briskin*, 135 F.4th at 750. For specific personal jurisdiction, the Ninth Circuit inquires whether: (1) the defendant "purposefully direct[ed] his activities or

consummate[d] some transaction with the forum or resident thereof; or perform[ed] some act by which he purposefully avail[ed] himself of the privilege of conducting activities in the forum"; (2) the claim "arise[s] out of or relate[s] to the defendant's forum-related activities"; and (3) the exercise of jurisdiction would be "reasonable." *Id.* at 750–51 (citation omitted). Contrary to Defendants' insistence, RM 6, there is no "rigid dividing line between purposeful direction and purposeful availment," and the first prong of the test "may be satisfied by purposeful availment, by purposeful direction, or by some combination thereof." *Briskin*, 135 F.4th at 751 n.10 (cleaned up). The Ninth Circuit considers the first two prongs together, such that "a single forum state contact can support jurisdiction if the cause of action arises out of that particular purposeful contact of the defendant with the forum state." *In re W. States Wholesale Nat. Gas Antitrust Litig.*, 715 F.3d 716, 742 (9th Cir. 2013) (cleaned up). Plaintiffs satisfy the first two prongs of the test, and Defendants fail to carry their burden on the third. *See Briskin*, 135 F.4th at 751.

A. Defendants carried out tortious conduct in California.

Defendants are subject to personal jurisdiction in California in this case because it arises from tortious conduct that Defendants carried out in California. *See Freestream Aircraft (Bermuda) Ltd. v. Aero L. Grp.*, 905 F.3d 597, 603 (9th Cir. 2018) ("Generally, the commission of an intentional tort in a state is a purposeful act that will satisfy the first two requirements of the minimum contacts test." (cleaned up)); *id.* at 606; *Paccar Int'l, Inc. v. Com. Bank of Kuwait, S.A.K.*, 757 F.2d 1058, 1064 (9th Cir. 1985). Defendants developed Pegasus to subvert the privacy and security features of iPhones manufactured by California company Apple. AC ¶¶ 3, 40. Defendants repeatedly accessed Apple's servers, including those in California, "to identify and exploit vulnerabilities in Apple software and services, to enable the delivery of Pegasus to targets' iPhones, and to allow Pegasus operators to extract data from their targets' iPhones and their targets' cloud-based accounts." *Id.* ¶ 3; *see id.* ¶¶ 41–43, 55. Because Defendants' intentional "suit-related conduct . . . create[d] a substantial connection with the forum State," they are subject to personal jurisdiction here. *Walden v. Fiore*, 571 U.S. 277, 284 (2014); *see Briskin*, 135 F. 4th at 756 (holding that defendant's intentional entry into the forum by electronic means was a relevant contact); *Freestream*, 905 F.3d at 606; *HB Prods., Inc. v. Faizan*, 603 F. Supp. 3d 910, 926 (D.

Haw. 2022) ("[W]hen a defendant uses the Internet to commit a tort . . ., the defendant's tortious actions occur at the location of the computer (e.g., web server) that the defendant manipulates to commit the tort."). Defendants' counterarguments are unavailing:

First, Defendants argue that Plaintiffs' harms were not suffered in the forum, RM 6–7, but "[t]he plaintiff's lack of 'contacts' will not defeat otherwise proper jurisdiction." *Calder v. Jones*, 465 U.S. 783, 788 (1984); *see Keeton v. Hustler Mag., Inc.*, 465 U.S. 770, 779 (1984). "The proper question is not where the plaintiff experienced a particular injury or effect but whether the defendant's conduct connects him to the forum in a meaningful way." *Walden*, 571 U.S. at 290; *accord Ayla, LLC v. Alya Skin Pty. Ltd.*, 11 F.4th 972, 980 (9th Cir. 2021). Plaintiffs' claims must arise from or relate to Defendants' forum contacts under the test's second prong. *See Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.*, 141 S. Ct. 1017, 1026 (2021). That prong is plainly met here because the exploits Defendants developed by abusing Apple's California-based infrastructure were the vectors of the Pegasus attacks against Plaintiffs—in other words, Defendants' forum contacts were a but-for cause of Plaintiffs' harms. AC ¶¶ 3, 41–43, 55, 63. Defendants' forum contacts thus suffice for specific personal jurisdiction. *See, e.g.*, *Atchley v. AstraZeneca UK Ltd.*, 22 F.4th 204, 233–35 (D.C. Cir. 2022); *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL*, 732 F.3d 161, 171–72 (2d Cir. 2013) (holding that foreign defendant's use of a U.S. bank account "as an instrument to achieve the very wrong alleged" was a sufficient contact).

Second, Defendants argue that any contacts with California servers were "pure happenstance." RM 8.[6] Hardly. Defendants specifically targeted Apple, a California company, to develop exploits capable of infecting iPhones with Pegasus. *See* AC ¶¶ 3, 40–45. And they designed Pegasus specifically to subvert privacy and security features unique to iPhones. *Id.* ¶ 40. It was hardly happenstance that this effort entailed extensive interaction with Apple's

[6] Plaintiffs have adequately alleged Defendants' contact with Apple's servers, including those in California. AC ¶¶ 3, 41; *contra* RM 7. Plaintiffs may plead facts based on information and belief "where the facts are peculiarly within the possession and control of the defendant," as clearly is the case here. *Soo Park v. Thompson*, 851 F.3d 910, 928 (9th Cir. 2017) (cleaned up); *see Alhathloul v. DarkMatter Grp.*, 2025 WL 2320474, at *21 (D. Or. Aug. 12, 2025). Defendants do not dispute those allegations, so they "must be taken as true." *Cohodes v. MiMedx Grp., Inc.*, 2022 WL 15523079, at *1 (N.D. Cal. Oct. 27, 2022). Otherwise, Plaintiffs request broader jurisdictional discovery. *See Burri L. PA v. Skurla*, 35 F.4th 1207, 1217–18 (9th Cir. 2022).

infrastructure—subverting Apple's infrastructure was a core component of Defendants' business. *See supra* pp. 1–2; *Briskin*, 135 F.4th at 756. And it is hardly happenstance that Apple has servers in the United States and in California in particular, where it is based. *See* AC ¶ 3. Defendants' contacts with this forum were thus their "own choice and not random, isolated, or fortuitous." *Briskin*, 135 F.4th at 758 (cleaned up). Defendants rely on *Hungerstation LLC v. Fast Choice LLC*, 857 F. App'x 349 (9th Cir. 2021), *see* RM 8–9, but that decision "simply states that the location of the server *alone* is insufficient to establish personal jurisdiction, not that it is irrelevant to the analysis." *Will Co., Ltd. v. Lee*, 47 F.4th 917, 926 (9th Cir. 2022). In other cases Defendants cite, RM 8 n.6, the plaintiffs sought to establish personal jurisdiction based on defendants' incidental use of third-party servers for website hosting, data storage, or data theft. In this case, the subversion of Apple's infrastructure in California was core to Defendants' tortious conduct. *See 42 Ventures, LLC v. Mav*, 2022 WL 2400030, at *4 (D. Haw. June 15, 2022) (distinguishing *Hungerstation* from case where defendants "specifically chose servers" in the forum); *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 826–27 (N.D. Cal. 2014) (finding personal jurisdiction where defendant deliberately accessed servers it knew were located in the forum); *MacDermid, Inc. v. Deiter*, 702 F.3d 725, 730 (2d Cir. 2012) (same).

Third, Defendants rely on three decisions that do not dictate dismissal here. RM 7–8. In *Khashoggi v. NSO Group*, the Fourth Circuit dismissed for lack of personal jurisdiction in part *because* there were insufficient allegations that NSO Group targeted activities in the forum, explicitly distinguishing that case from *WhatsApp*, where—as here—Defendants targeted a California-based company and its California servers. 138 F.4th 152, 163 (4th Cir. 2025) (citing *WhatsApp v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 669–74 (N.D. Cal. 2020)). In *Alhathloul v. DarkMatter Group*, although the district court initially dismissed the plaintiff's complaint, it allowed for jurisdictional discovery and subsequently determined that defendants *were* subject to personal jurisdiction—not only because the plaintiff was located in the United States during some of the spyware attacks, but also because defendants had purchased exploits from U.S. companies and used U.S.-based proxy servers. 2025 WL 2320474, at *7–13 ("These choices to purchase U.S. exploits from U.S. companies and to use U.S. anonymization services and proxy servers

demonstrate Defendants expressly aimed their conduct at the U.S." *Id.* at *12.). Here, Defendants' deliberate and sustained abuse of Apple's software and services to develop their own exploits, including those used in this case, AC ¶ 42, establish much more significant, case-specific contact with the forum than the mere purchase of exploits from U.S. companies. Finally, the district court dismissed *Corallo* because the plaintiff had no connection to the United States and had sparsely alleged defendants' forum-related activities. 2024 WL 4367924, *3–4. Both points readily distinguish that case, *cf. supra* pp. 1–2, 4 & n.3, 7–9, which was decided before the Ninth Circuit clarified the relevant law in *Briskin*, 135 F.4th at 756.

B. Defendants purposefully directed claim-related conduct at California.

Plaintiffs need not satisfy the effects test in this case. But they do, in any event, because Defendants committed intentional acts that were expressly aimed at California and caused foreseeable harm in California. *See Ayla*, 11 F.4th at 980. Because those acts were the but-for cause of Plaintiffs' harms, *supra* p. 8, Plaintiffs satisfy the second prong of the specific jurisdiction test as well. *See Ayla*, 11 F.4th at 983.

***First*,** Defendants committed intentional acts in developing and using exploits to deliver Pegasus to target Plaintiffs' devices. AC ¶¶ 3, 41–43; *see WhatsApp*, 472 F. Supp. 3d at 672–73, (concluding that Defendants had committed an intentional act by "design[ing] and manufactur[ing] a program to exploit WhatsApp's app, servers, and infrastructure").

***Second*,** Defendants expressly aimed their conduct at California by "purposefully target[ing]" Apple and its California-based servers in developing and using exploits to deliver Pegasus to Plaintiffs' iPhones. *Lang Van, Inc. v. VNG Corp.*, 40 F.4th 1034, 1041 (9th Cir. 2022); *see supra* pp. 1–2, 7–9; *cf. WhatsApp*, 472 F. Supp. 3d at 673 ("[D]efendants sought out WhatsApp's California-based servers for the purpose of routing malicious code through those servers to ultimately reach individual users' phones."); *NetApp*, 41 F. Supp. 3d at 826; *Jenkins v. Pooke*, 2009 WL 10692010, at *4 (N.D. Cal. July 13, 2009), *R&R adopted*, 2009 WL 10691375 (N.D. Cal. Aug. 19, 2009) (concluding that foreign defendant's "tortious conduct was directed at California" because he accessed an e-mail account "maintained by a California corporation headquartered in California," though plaintiff resided outside the forum).

Third, Defendants' conduct caused harm to Apple that they knew was likely to be suffered in California, where Apple is headquartered. AC ¶ 3. A significant component of "the 'bad acts' that form the basis of [Plaintiffs'] complaint"—Defendants' development and use of Apple exploits to deliver Pegasus to Plaintiffs' iPhones—occurred in California, *Will Co.*, 47 F.4th at 926 (citation omitted), foreseeably harming Apple in the forum. AC ¶ 3; *see supra* pp. 1–3 & n.2, 7–9; Compl., *Apple Inc. v. NSO Grp. Techs. Ltd.*, No. 3:21-cv-09078 (N.D. Cal. Nov. 23, 2021), ECF No. 1, at ¶¶ 5, 24, 26; *Hydentra HLP Int. Ltd. v. Sagan Ltd.*, 783 F. App'x 663, 665 (9th Cir. 2019) (explaining that a corporation incurs loss, for jurisdictional purposes, in forum of its principal place of business); *cf. Burri*, 35 F.4th at 1213 (holding that acts taken to interfere with in-forum contract "target the forum state itself"). That harm suffices for personal jurisdiction. *See Will Co.*, 47 F.4th at 926 ("[J]urisdiction is proper in any forum where a sufficient amount of harm occurs, even if that amounts to only a small percentage of the overall harm caused." (cleaned up)).

C. This Court's exercise of personal jurisdiction is reasonable.

Defendants fail to make a "compelling case" that the exercise of jurisdiction would be unreasonable, which is their burden. *Briskin*, 135 F.4th at 751 (cleaned up). Indeed, the reasonableness factors weigh heavily in favor of exercising personal jurisdiction here. *See id.* at 761 (reciting factors). First, Defendants interjected themselves into California's affairs by abusing Apple's infrastructure to develop and use exploits to deliver Pegasus to Plaintiffs' iPhones. *See supra* pp. 1–2, 7–9; *Ayla*, 11 F.4th at 984; *WhatsApp*, 472 F. Supp. 3d at 676. Second, for all the reasons stated above, the burden on Defendants of defending in this forum is slight, and "the corresponding burden on" Plaintiffs of litigating in Israel would be substantial. *Sinatra v. Nat'l Enquirer, Inc.*, 854 F.2d 1191, 1199 (9th Cir. 1988) (citation omitted); *see supra* p. 5. Third, any conflict with Israel's sovereignty "is not dispositive" because otherwise "it would always prevent suit against a foreign national in a [U.S.] court." *Sinatra*, 854 F.2d at 1199 (citation omitted). Fourth, as explained above, California has a significant interest in this dispute. *See supra* pp. 3–4; *Bos. Telecomms.*, 588 F.3d at 1212. Fifth and sixth, because Plaintiffs' claims arise from in-forum conduct and "rest on the law of California and the United States," this forum will "provide the most efficient judicial resolution of the controversy" and "better provide [Plaintiffs] convenient

and effective relief." *Ayla*, 11 F.4th at 984 (cleaned up). Finally, "whether another reasonable forum exists" is not an issue because Defendants have not shown that this forum is unreasonable. *Ayla*, 11 F.4th at 984–85 (cleaned up); *see WhatsApp*, 472 F. Supp. 3d at 677.

III. This Court has personal jurisdiction under the federal long-arm statute.

Alternatively, Defendants are subject to personal jurisdiction under Federal Rule of Civil Procedure 4(k)(2). Plaintiffs' CFAA claims arise under federal law, and if Defendants were not subject to personal jurisdiction in California, they would not be subject to personal jurisdiction in any state. The only remaining question is whether the exercise of personal jurisdiction over Defendants would comport with the Fifth Amendment, which, the Supreme Court recently clarified, "necessarily permits a more flexible jurisdictional inquiry" than the minimum-contacts inquiry of the Fourteenth Amendment. *Fuld*, 606 U.S. at 16. It would.

Defendants' deliberate and sustained abuse of Apple's software and services is "conduct closely related to the United States that implicates important foreign policy" and national security concerns. *Fuld*, 606 U.S. at 18. Congress addressed those concerns in adopting and amending the CFAA. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L.R. 1561, 1563–64 (2010) (explaining national security concerns animating CFAA's initial passage); 147 Cong. Rec. S10990–02, S10997 (2001) (statement of Sen. Leahy) (explaining 2001 CFAA amendment to "include qualified computers even when they are physically located outside of the United States" so as to "preserve the ability of the United States to assist in international hacking cases"). The executive branch put an even finer point on those concerns in the context of commercial spyware—specifically, spyware used against journalists and U.S. citizens, as in this case. *See supra* p. 4; *cf. Fuld*, 606 U.S. at 15 (recognizing U.S. "interest in holding accountable" those who harm "U.S. nationals—who, even when physically outside our borders, remain 'under the particular protection' of American law"). Plaintiffs' claims thus "implicate important foreign policy and national security concerns," such that "this court's exercise of personal jurisdiction over Defendants is consistent with the [U.S.] Constitution and laws." *Finan v. Lafarge S.A.*, 2025 WL 2504317, at *17 (E.D.N.Y. Aug. 29, 2025) (citing *Fuld*, 606 U.S. at 18; Fed. R. Civ. P. 4(k)(2)).

Even under the Fourteenth Amendment inquiry, Defendants have sufficient "minimum contacts" with the United States as a whole. *See Will Co.*, 47 F.4th at 922. Defendants have case-related contacts not only with Apple's California-based servers, but also with other U.S.-based servers, including those used for cloud storage. AC ¶¶ 38–44. In addition to Defendants' other U.S. activities, AC ¶ 34, these contacts exceed the minimum required for personal jurisdiction. *Will Co.*, 47 F.4th at 927; *42 Ventures*, 2022 WL 2400030, at *4–5. For the same reasons stated above, the exercise of personal jurisdiction would also be reasonable. *See supra* pp. 11–12; *Fuld*, 606 U.S. at 24; *Lang Van*, 40 F.4th at 1041–43; *Atchley*, 22 F.4th at 234–36.

IV. Plaintiffs have adequately alleged their claims.

A. Plaintiffs have adequately alleged violations of the CFAA.

As this Court and others have ruled, those responsible for creating and installing malware or spyware are liable under the CFAA. *See Apple*, 2024 WL 251448, at *4 ("The anti-hacking purpose of the CFAA fits Apple's allegations to a T[.]"); *Alhathloul*, 2025 WL 2320474, at *21; *Microsoft Corp. v. Does 1–2*, 2021 WL 4755518, at *7 (E.D.N.Y. May 28, 2021). Defendants' counterarguments are unavailing:

***First*,** Plaintiffs have adequately alleged damage to their devices because the Pegasus attacks disabled iPhone features, infected Plaintiffs' devices with spyware, and enabled Defendants and their clients to surreptitiously control the devices. *See* AC ¶ 140. Defendants argue that there was no damage because Plaintiffs could technically continue to use their devices following the attacks, RM 11, but this is incorrect. Infected with spyware, a device "no longer operates only in response to the commands of the owner," but instead "may be operated by unauthorized users who have the capability of extracting confidential information from [it]." *United States v. Yücel*, 97 F. Supp. 3d 413, 420 (S.D.N.Y. 2015). This fundamentally impairs the integrity of the device and the data stored on it—in a way that merely copying information does not. Defendants are also wrong to suggest that disabling crash reporting is insufficient damage. Removing features from a device "impair[s]" it, *see id.*, and while Plaintiffs were not required to describe how that damage affected their experience as end users, they did, by alleging that it enabled the installation of Pegasus and therefore caused the harms described above. AC ¶ 40.

Second, Plaintiffs have adequately alleged loss. The Pegasus attacks diminished the value of Plaintiffs' iPhones, *see* AC ¶ 140. This is not "subjective loss," RM 11, because a device transformed into a surveillance tool clearly can no longer be used for its primary purpose of private communication.[7] Plaintiffs also lost the value of considerable time spent investigating and remediating the attacks, including developing new security policies and upgrading IT systems. *See generally* AC ¶¶ 61, 67–136. Defendants argue that the Court "cannot assign a monetary value to that time" at this stage, RM 11, but these allegations plainly suffice on a motion to dismiss. *See Alhathloul*, 2025 WL 2320474, at *23 ("Courts in the Ninth Circuit do not require plaintiffs to allege the type of detailed cost itemizations Defendants suggest."); *Apple, Inc.*, 2024 WL 251448, at *4. Many Plaintiffs also incurred further financial losses, like purchasing security software, which Defendants ignore. *See* AC ¶¶ 71, 75, 79, 87, 95, 107, 111, 123, 127, 131.

Third, Plaintiffs have adequately alleged more than $5,000 of loss in a one-year period. Because this case involves "coordinated and sustained" attacks against Plaintiffs' iPhones "in a similar manner" and which "caus[ed] similar damage," AC ¶ 63, losses may be aggregated. *E.g.*, *In re Apple & AT & TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008). Defendants argue that losses incurred by El Faro do not count, RM 12, but the CFAA includes losses to "any victim." *See Alhathloul*, 2025 WL 2320474, at *23 (counting time spent by plaintiff and cyber-security experts she communicated with); *United States v. Millot*, 433 F.3d 1057, 1060–61 (8th Cir. 2006) (holding losses include those felt by "1 *or more persons*"). Because El Faro, which owned many of the devices, *see, e.g.*, AC ¶ 65, was also a victim, whether certain losses were borne by Plaintiffs or El Faro is irrelevant: the losses meet the $5,000 threshold either way.[8]

Fourth, Plaintiffs have adequately pleaded aiding-and-abetting liability. Defendants argue that this liability does not exist under the CFAA, RM 12–13, but many cases—including some

[7] In the cases on which Defendants rely, the plaintiffs failed to allege a causal connection between the damage to the device and diminishment in its value. *See, e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1067 (N.D. Cal. 2012).

[8] In *Walsh v. Microsoft Corporation*, RM 12, the plaintiffs "state[d] cursorily" that the threshold had been met and appeared to rely on "absent members of their putative class" rather than specific allegations of losses. 63 F. Supp. 3d 1312, 1320 (W.D. Wash. 2014). Plaintiffs' allegations are far more detailed than in *Walsh* and the other cases Defendants cite, RM 12 n.12.

from this district—have countenanced civil CFAA aiding-and-abetting claims. *See COR Sec. Holdings Inc. v. Banc of Cal., N.A.*, 2018 WL 4860032, at *7 (C.D. Cal. Feb. 12, 2018) ("Defendants have not persuaded the Court that legal precedent forecloses a civil aiding and abetting claim under CFAA."); *see also Fraser v. Mint Mobile, LLC*, 2022 WL 1240864, at *5 (N.D. Cal. Apr. 27, 2022) (dismissing claim without foreclosing possibility of aiding-and-abetting liability); *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *4 (N.D. Cal. Nov. 20, 2020) (same).

B. Plaintiffs have adequately alleged violations of California law.

Defendants' objections to Plaintiffs' California claims rehash arguments they press elsewhere, and those arguments fail for the same reasons here. First, because this case involves the abuse Apple's infrastructure in California to develop and deploy Pegasus against Plaintiffs, *see supra* pp. 1–2, 7–9, no extraterritorial application of California law is required. This is a far cry from cases where plaintiffs did not allege wrongful conduct in the state. *See Lineberry v. AddShopper, Inc.*, 2025 WL 551864, at *3 (N.D. Cal. Feb. 19, 2025); RM 13 (citing similar cases). Second, for the reasons stated above, *supra* pp. 13–14, the harms caused by the Pegasus attacks suffice for both CDAFA and trespass to chattels.[9] The attacks disabled iPhone features, used up storage space, and enabled the exfiltration of Plaintiffs' data—and by selling Pegasus to clients, Defendants wrongly profited from this scheme. *See In re Meta Healthcare Pixel Litig.*, 713 F. Supp. 3d 650, 655–59 (N.D. Cal. 2024) (refusing to dismiss CDAFA and trespass claims "based on surreptitious placement" of code that usurped devices' normal functioning and caused "measurable decrease in the[ir] storage"); *Rodriguez v. Google LLC*, 772 F. Supp. 3d 1093, 1109–11 (N.D. Cal. 2025).[10]

CONCLUSION

The Court should deny Defendants' Renewed Motion to Dismiss.

[9] The relevant provisions of CDAFA are generally interpreted in the same way as the CFAA. *See Multiven, Inc. v. Cisco Systems, Inc.*, 725 F. Supp. 2d 887, 895–96 (N.D. Cal. 2010).

[10] *WhatsApp* is not to the contrary. WhatsApp argued that NSO Group's conduct affected its provision of services to others, 472 F. Supp. 3d at 685, but here, Plaintiffs have alleged that Defendants' conduct impaired their ability to use their own devices, *see, e.g.*, AC ¶¶ 67, 71, 75.

Dated: October 16, 2025

Respectfully submitted,

/s/ Carrie DeCell

Carrie DeCell, *Pro Hac Vice*
Jameel Jaffer, *Pro Hac Vice*
Alex Abdo, *Pro Hac Vice*
Stephanie Krent, *Pro Hac Vice*
*Nicola Morrow
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
carrie.decell@knightcolumbia.org

**Pro Hac Vice* application forthcoming

/s/ Corey Stoughton

Corey Stoughton, *Pro Hac Vice*
Alvaro Mon Cureño, *Pro Hac Vice*
Selendy Gay PLLC
1290 Avenue of the Americas
New York, NY 10104
(212) 390-9000
cstoughton@selendygay.com

Counsel for the Plaintiffs Carlos Dada, Sergio Arauz, Gabriela Cáceres Gutiérrez, Julia Gavarrete, Roman Gressier, Gabriel Labrador, Ana Beatriz Lazo Escobar, Efren Lemus, Daniel Lizárraga, Carlos López Salamanca, Carlos Martínez, Óscar Martínez, María Luz Nóchez, Víctor Peña, Nelson Rauda Zablah, Daniel Reyes Martínez, Mauricio Sandoval Soriano, and José Luis Sanz

Paul Hoffman #71244
John Washington #315991
Schonbrun, Seplow, Harris,
Hoffman & Zeldes LLP
200 Pier Avenue, Suite 226
Hermosa Beach, CA 90254
T: (424) 297-0114
F: (310) 399-7040
hoffpaul@aol.com