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

*Counsel for all Plaintiffs**

**See Signature Page for Complete List of Plaintiffs*

CARRIE DECELL, *Pro Hac Vice*
JAMEEL JAFFER, *Pro Hac Vice*
ALEX ABDO, *Pro Hac Vice*
STEPHANIE KRENT, *Pro Hac Vice*
EVAN WELBER FALCÓN, *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 all 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' CORRECTED NOTICE OF MOTION AND MOTION TO DISMISS FIRST AMENDED COMPLAINT

Hearing Date: May 25, 2023
Time: 10:00 a.m.
Ctrm: 11

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTRODUCTION 1

BACKGROUND 1

ARGUMENT 2

I. This Court has personal jurisdiction under California's long-arm statute. 2

A. The first two prongs of the specific jurisdiction test are satisfied because Defendants carried out tortious conduct in California. 3

B. The first two prongs of the specific jurisdiction test are satisfied because Defendants purposefully directed claim-related conduct at California. 6

C. This Court's exercise of personal jurisdiction is reasonable. 7

II. This Court has personal jurisdiction under the federal long-arm statute. 9

III. This Court is the proper forum for this case. 9

IV. Plaintiffs have adequately alleged their claims. 11

A. Plaintiffs have adequately alleged violations of the CFAA. 12

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

CONCLUSION 15

TABLE OF AUTHORITIES

Cases

42 Ventures, LLC v. Mav, No. 20-00228, 2022 WL 2400030 (D. Haw. June 15, 2022) 4, 6, 9

42 Ventures, LLC v. Mav, No. 20-17305, 2021 WL 5985018 (9th Cir. Dec. 16, 2021) 4

Alhathloul v. DarkMatter Group, No. 3:21-cv-01787, 2023 WL 2537761 (D. Or. Mar. 16, 2023) 4

Alternate Health USA Inc. v. Edalat, No. 8:17-cv-01887, 2022 WL 767573 (C.D. Cal. Mar. 14, 2022) 11

Apple Inc. v. NSO Group Techs. Ltd., No. 3:21-cv-09078 (N.D. Cal. Nov. 23, 2021) 8

Atchley v. AstraZeneca UK Ltd., 22 F.4th 204 (D.C. Cir. 2022) 5, 9

Ayla, LLC v. Alya Skin Pty. Ltd., 11 F.4th 972 (9th Cir. 2021) 5, 6, 8, 9

Bos. Telecomms. Grp., Inc. v. Wood, 588 F.3d 1201 (9th Cir. 2009) 8

Burri L. PA v. Skurla, 35 F.4th 1207 (9th Cir. 2022) 3, 7

Carijano v. Occidental Petrol. Corp., 643 F.3d 1216 (9th Cir. 2011) 9, 10

Climax Portable Mach. Tools, Inc. v. Trawema GmbH, No. 3:18-cv-1825, 2020 WL 1304487 (D. Or. Mar. 19, 2020) 4

Cohodes v. MiMedx Grp., Inc., No. 3:22-cv-00368, 2022 WL 15523079 (N.D. Cal. Oct. 27, 2022) 3

COR Sec. Holdings Inc. v. Banc of Cal., N.A., No. SA CV 17-1403, 2018 WL 4860032 (C.D. Cal. Feb. 12, 2018) 14

Corallo v. NSO Group Techs. Ltd., No. 3:22-cv-05229 (N.D. Cal. Sept. 13, 2022) 8

DEX Sys., Inc. v. Deutsche Post AG, 727 F. App'x 276 (9th Cir. 2018) 4

Dole Food Co., Inc. v. Watts, 303 F.3d 1104 (9th Cir. 2002) 9, 10

Facebook, Inc. v. ConnectU LLC, No. C 07-01389, 2007 WL 2326090 (N.D. Cal. Aug. 13, 2007) 7

Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016) 13, 15

Facebook, Inc. v. Studivz Ltd., No. C 08-3468, 2009 WL 1190802 (N.D. Cal. May 4, 2009) 11

Finjan, Inc. v. Cisco Sys., Inc., No. 5:17-cv-00072, 2019 WL 667766 (N.D. Cal. Feb. 19, 2019) 11

Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct., 141 S. Ct. 1017 (2021) 5

Fraser v. Mint Mobile, LLC, No. C 22-00138, 2022 WL 1240864 (N.D. Cal. Apr. 27, 2022) 14

Freestream Aircraft (Bermuda) Ltd. v. Aero L. Grp., 905 F.3d 597 (9th Cir. 2018) 3, 4

Gates Learjet Corp. v. Jensen, 743 F.2d 1325 (9th Cir. 1984) 8

Glazer Cap. Mgmt., L.P. v. Forescout Techs., Inc., 63 F.4th 747 (9th Cir. 2023) 12

Glob. Commodities Trading Grp., Inc. v. Beneficio de Arroz Choloma, S.A., 972 F.3d 1101 (9th Cir. 2020) 2, 3, 9

Goodman v. Goodman, No. 21-CV-10902, 2022 WL 17826390 (S.D.N.Y. Dec. 21, 2022) 12, 14

HB Prods., Inc. v. Faizan, 603 F. Supp. 3d 910 (D. Haw. 2022) 4

Hungerstation LLC v. Fast Choice LLC, 857 F. App'x 349 (9th Cir. 2021) 6

Hydentra HLP Int. Ltd. v. Sagan Ltd., 783 F. App'x 663 (9th Cir. 2019) 7

In re Apple & AT & TM Antitrust Litig., 596 F. Supp. 2d 1288 (N.D. Cal. 2008) 13

In re Apple Device Performance Litig., 347 F. Supp. 3d 434 (N.D. Cal. 2018) 15

In re iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2012) 13

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

Jenkins v. Pooke, No. C-07-3112, 2009 WL 10692010 (N.D. Cal. July 13, 2009) 7

Lang Van, Inc. v. VNG Corp., 40 F.4th 1034 (9th Cir. 2022) 7, 9

Licci ex rel. Licci v. Lebanese Canadian Bank, SAL, 732 F.3d 161 (2d Cir. 2013) 5

Lueck v. Sundstrand Corp., 236 F.3d 1137 (9th Cir. 2001) 11

MacDermid, Inc. v. Deiter, 702 F.3d 725 (2d Cir. 2012) 6

Microsoft Corp. v. Does 1–2, No. 20-CV-1217, 2021 WL 4755518 (E.D.N.Y. May 28, 2021) 12

Microsoft Corp. v. John Does 1–8, No. 1:14-cv-811, 2015 WL 4937441 (E.D. Va. Aug. 17, 2015) 12

Mintz v. Mark Bartelstein & Assocs. Inc., 906 F. Supp. 2d 1017 (C.D. Cal. 2012) 14

MSC Safety Sols., LLC v. Trivent Safety Consulting, LLC, No. 19-cv-00938, 2020 WL 7425874 (D. Colo. Dec. 18, 2020) 14

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) 6, 7

NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 938 (N.D. Cal. 2014) 14

Nowak v. Xapo, Inc., No. 5:20-cv-03643, 2020 WL 6822888 (N.D. Cal. Nov. 20, 2020) 14, 15

Paccar Int'l, Inc. v. Com. Bank of Kuwait, S.A.K., 757 F.2d 1058 (9th Cir. 1985) 3, 4

Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998) 6

Silk v. Bond, 65 F.4th 445 (9th Cir. 2023) 8

Sinatra v. Nat'l Enquirer, Inc., 854 F.2d 1191 (9th Cir. 1988) 8, 9

United States v. Janosko, 642 F.3d 40 (1st Cir. 2011) 14

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) 12

Universal Ent. Corp. v. Aruze Gaming Am., Inc., No. 2:18-cv-00585, 2020 WL 2840153 (D. Nev. May 30, 2020) 10

Verizon Online Servs., Inc. v. Ralsky, 203 F. Supp. 2d 601 (E.D. Va. 2002) 5

Walden v. Fiore, 571 U.S. 277 (2014) 1, 5

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

Ward v. United Airlines, Inc., 466 P.3d 309 (Cal. 2020) 15

Wesch v. Yodlee, Inc., No. 20-cv-05991, 2021 WL 1399291 (N.D. Cal. Feb. 16, 2021) 14

WhatsApp Inc. v. NSO Group Techs. Ltd., 472 F. Supp. 3d 649 (N.D. Cal. 2020) ..... passim

WhatsApp Inc. v. NSO Group Techs. Ltd., No. 4:19-cv-07123 (N.D. Cal. Oct. 29, 2019) 8

Will Co., Ltd. v. Lee, 47 F.4th 917 (9th Cir. 2022) 6, 7, 9

Wilson v. Playtika, Ltd., 349 F. Supp. 3d 1028 (W.D. Wash. 2018) 11

Statutes

18 U.S.C. § 1030 ..... 1, 12, 13, 14

Cal. Penal Code § 502 1

Foreign Judgments Enforcement Law, 5718–1958, 12 LSI 82 (5718-1957/58), as amended (Isr.) 11

Other Authorities

Compl., *Apple Inc. v. NSO Group Techs. Ltd.*, No. 3:21-cv-09078 (N.D. Cal. Nov. 23, 2021) 3, 5, 7, 9

Exec. Order. No. 14,093, 88 Fed. Reg. 18,957, 18,957 (Mar. 27, 2023) 10

Rules

Fed. R. Civ. P. 4(k)(2) 9

N.D. Cal. Civ. L.R. 3-12(a) 8

INTRODUCTION

Defendants NSO Group and Q Cyber have developed a malicious surveillance system called "Pegasus" and sold it to rights-abusing governments around the world. Through the deliberate and sustained abuse of the software and services of major U.S. technology companies headquartered in California, Defendants have enabled and assisted in the deployment of Pegasus against countless journalists, human rights defenders, and others. This lawsuit seeks to hold Defendants accountable for their role in the Pegasus attacks against Plaintiffs—journalists and other members of the renowned digital newspaper El Faro.

Defendants are subject to specific personal jurisdiction in this forum. The specific jurisdiction inquiry "focuses on the relationship among the defendant, the forum, and the litigation." *Walden v. Fiore*, 571 U.S. 277, 284 (2014) (cleaned up). Plaintiffs' claims arise from the same course of conduct at issue in Apple's related litigation: specifically, Defendants' abuse of Apple's infrastructure, through which Defendants developed and then used exploits to deliver Pegasus to Apple users, including Plaintiffs. Contrary to Defendants' arguments, their abuse of Apple's infrastructure was indispensable—not incidental—to the Pegasus attacks against Plaintiffs. The relationship among Defendants, this forum, and the litigation is airtight.

Plaintiffs have sufficiently pleaded their claims. Defendants designed Pegasus to provide unauthorized access to targets' smartphone 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 against them, satisfying statutory standing requirements and demonstrating trespass to chattels. Finally, California law applies because the attacks were carried out through Apple's infrastructure.

The Court should deny Defendants' Corrected Motion to Dismiss ("CM"), ECF No. 46.

BACKGROUND

Defendants' signature spyware system, often called "Pegasus," allows its operators to access and control smartphones covertly. Am. Compl. ("AC") ¶¶ 2, 37–39, ECF No. 31. Defendants configure and maintain the infrastructure that supports the operation of Pegasus. *Id.* ¶ 44. They sell Pegasus to government clients, including those responsible for grave abuses of

human rights. *Id.* ¶¶ 36, 46–49. They train those clients in the use of Pegasus and assist those clients throughout its deployment and operation. *Id*. ¶¶ 36, 44.

Crucial to Defendants' business—and to this case—is their development of "zero-click" exploits of vulnerabilities in Apple's software and services, through which Pegasus is delivered remotely and surreptitiously to targets' iPhones. *Id*. ¶¶ 3, 40. Defendants used 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 used Apple ID accounts to deliver Pegasus through those exploits to targets' iPhones. *Id*. ¶ 43. The exploits used 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 one of Apple's iCloud servers before delivery to a target's iPhone." *Id.* Defendants designed Pegasus to disable Apple safeguards, including crash reporting, and to mimic Apple processes to avoid alerting Apple or Apple users to its presence. *Id*. ¶ 40.

Plaintiffs and their El Faro colleagues suffered 226 Pegasus attacks over the course of 18 months. *See id*. ¶¶ 5, 53–59, 63. The attacks damaged iPhones Plaintiffs 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 their 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.

ARGUMENT

I. 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. *Glob. Commodities Trading Grp., Inc. v. Beneficio de Arroz Choloma, S.A.*, 972 F.3d 1101, 1106 (9th Cir. 2020). For specific jurisdiction, the Ninth Circuit employs a

three-prong test, inquiring 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 1107 (citation omitted). 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 Glob. Commodities*, 972 F.3d at 1106.

A. The first two prongs of the specific jurisdiction test are satisfied because Defendants carried out tortious conduct in California.

Although Defendants argue otherwise, CM 1, this case centers on 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)); *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 Apple, a California company. AC ¶¶ 3, 40. To do so, Defendants repeatedly accessed Apple's servers, including servers 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; Compl. ¶ 42, *Apple Inc. v. NSO Group Techs. Ltd.*, No. 3:21-cv-09078 (N.D. Cal. Nov. 23, 2021) ("Apple Compl."), ECF No. 1.[1] Because

[1] Defendants argue that Plaintiffs have not adequately alleged the location of Apple's servers, CM 4, but Plaintiffs have, AC ¶¶ 3, 41, and Defendants submit no declaration disputing those allegations. Therefore, the "[u]ncontroverted allegations in the complaint must be taken as true." *Cohodes v. MiMedx Grp., Inc.*, 2022 WL 15523079, at *1 (N.D. Cal. Oct. 27, 2022). If Defendants did dispute them, Plaintiffs would request jurisdictional discovery. *See Burri L. PA v. Skurla*, 35 F.4th 1207, 1217–18 (9th Cir. 2022).

Defendants' forum activities formed a crucial component of their tortious conduct, they are subject to personal jurisdiction here. *See 42 Ventures, LLC v. Mav*, 2022 WL 2400030, at *3–4 (D. Haw. June 15, 2022), *R&R adopted*, 2022 WL 2392484 (D. Haw. July 1, 2022); *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 confined to the digital realm, the defendant's tortious actions occur at the location of the computer (e.g., web server) that the defendant manipulates to commit the tort."); *Climax Portable Mach. Tools, Inc. v. Trawema GmbH*, 2020 WL 1304487, at *4 (D. Or. Mar. 19, 2020) (finding that alleged tort "was at least in part committed in Oregon" where foreign defendants remotely accessed and used a server located in Oregon); *see also DEX Sys., Inc. v. Deutsche Post AG*, 727 F. App'x 276, 278 (9th Cir. 2018) (finding jurisdiction where defendant's "limited contacts with California" included "the allegedly tortious conduct in California that gave rise to [plaintiff's] claims"); *cf. Paccar*, 757 F.2d at 1064.[2]

Defendants' counterarguments are unavailing.

***First*,** Defendants argue that Plaintiffs cannot carry their burden without showing that Defendants "purposefully directed [their] activities towards California." CM 2. Plaintiffs *do* show purposeful direction, *see infra* pp. 6–7, but do not need to. Although the Ninth Circuit has typically applied the purposeful direction—or "effects"—test in tort cases, it has observed that the effects test "makes more sense when dealing with out-of-forum tortfeasors" and "appears unnecessary where, as here, part of the alleged tort occurred in the forum." *Freestream*, 905 F.3d at 606 (cleaned up); *see id.* at 604–07 (explaining development of circuit doctrine). In intentional tort cases, plaintiffs must show "*either* (1) that the tortious conduct occurred in the [forum]; *or* (2) that out-of-forum tortious conduct was purposefully directed to the [forum]." *42 Ventures, LLC v. Mav*, 2021 WL 5985018, at *1 (9th Cir. Dec. 16, 2021) (emphasis added). Plaintiffs have demonstrated the former, so need not demonstrate the latter.

[2] In *Alhathloul v. DarkMatter Group*, the court concluded that DarkMatter did not commit a tort in the United States when it transmitted spyware through Apple servers. 2023 WL 2537761, at *5 (D. Or. Mar. 16, 2023). That conclusion was incorrect because DarkMatter *did* "manipulate" Apple's servers to commit the tort. *Id.* But in any event, Defendants' abuse of Apple infrastructure to develop their own exploits, AC ¶ 42, distinguishes this case from *Alhathloul*, in which DarkMatter allegedly purchased exploits developed by others. 2023 WL 2537761, at *2.

Second, Defendants argue that the Court cannot exercise personal jurisdiction over them because Plaintiffs' harms were not suffered in the forum. CM 1–3. As the Supreme Court has emphasized, however, "[t]he 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 of course relate to Defendants' contacts with the forum—this is the focus of the test's second prong. *See Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.*, 141 S. Ct. 1017, 1026 (2021). But that prong is plainly satisfied here because the exploits Defendants developed by abusing Apple's 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. *See, e.g.*, *Atchley v. AstraZeneca UK Ltd*., 22 F.4th 204, 233–35 (D.C. Cir. 2022) (holding that defendants' contacts in the United States sufficiently related to plaintiffs' harms abroad to establish personal jurisdiction); *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL*, 732 F.3d 161, 171–72 (2d Cir. 2013) (same).

Third, Defendants argue that their contacts with California servers were "pure happenstance." CM 4–5. Hardly. Defendants specifically targeted Apple, a California company, in order to develop exploits capable of infecting Apple's 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 infrastructure—subverting Apple's infrastructure was the whole point. And it is hardly happenstance that Apple has servers in the United States and in California in particular, where it is based. *See id.* ¶ 3; Apple Compl. ¶¶ 5, 24, 26; *Verizon Online Servs., Inc. v. Ralsky*, 203 F. Supp. 2d 601, 620 (E.D. Va. 2002) ("Defendants' conduct and connections to Virginia were of their own choosing, not someone else's.").

Defendants' intentional and extensive interaction with Apple's servers distinguishes this case from those in which defendants' sole contact with the forum was their *incidental* contact with third-party servers. Here, Defendants directly and repeatedly targeted Apple's servers to transform Apple's software and services into vectors of Pegasus attacks against Apple users. AC ¶¶ 3, 41–

45. Defendants rely on *Hungerstation LLC v. Fast Choice LLC*, 857 F. App'x 349 (9th Cir. 2021), 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 the other cases Defendants cite, CM 4 n.4, the plaintiffs sought to establish personal jurisdiction based on the defendants' incidental use of third-party servers for website-hosting or data-storage purposes or to steal or copy data stored there. In none of those cases did the defendants deliberately abuse the third party's servers to "discover vulnerabilities" in the third party's software, "to probe" the third party's services, and "to test the software" that the defendants had developed to deliver malware to the third party's users. AC ¶ 42. In this case, the subversion of Apple's infrastructure in California was the core of Defendants' tortious conduct. *See 42 Ventures*, 2022 WL 2400030, at *4 (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); *cf. Will Co.*, 47 F.4th at 922–26; *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1322 (9th Cir. 1998); *MacDermid, Inc. v. Deiter*, 702 F.3d 725, 730 (2d Cir. 2012).

B. The first two prongs of the specific jurisdiction test are satisfied because Defendants purposefully directed claim-related conduct at California.

As explained above, Plaintiffs need not satisfy the effects test in this case. But they do, in any event, because Defendants (1) committed intentional acts that (2) were expressly aimed at California and (3) foreseeably caused harm in California. *See Ayla*, 11 F.4th at 980. Because those acts were the but-for cause of Plaintiffs' harms, as explained above, *supra* p. 5, 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 targets' devices. AC ¶¶ 3, 41–43; *see WhatsApp Inc. v. NSO Group Techs. Ltd.*, 472 F. Supp. 3d 649, 672–73 (N.D. Cal. 2020), *aff'd on other grounds*, 17 F.4th 930 (9th Cir. 2021) (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, a California-based company, in developing and using exploits to deliver

Pegasus to Plaintiffs' iPhones, *see supra* pp. 3–4. *Lang Van, Inc. v. VNG Corp.*, 40 F.4th 1034, 1041 (9th Cir. 2022), *petition for cert. filed*, No. 22-937 (U.S. Mar. 23, 2023); *see 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.");[3] *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," and explaining that the express aiming requirement can be satisfied even where plaintiff resides outside the forum); *Facebook, Inc. v. ConnectU LLC*, 2007 WL 2326090, at *5–6 (N.D. Cal. Aug. 13, 2007).

***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). Those bad acts foreseeably harmed Apple in the forum. AC ¶ 3; *see* Apple Compl. ¶¶ 2, 5, 10, 13, 24, 54, 56–59; *Hydentra HLP Int. Ltd. v. Sagan Ltd.*, 783 F. App'x 663, 665 (9th Cir. 2019) ("[A] corporation incurs economic loss, for jurisdictional purposes, in the forum of its principal place of business." (citation omitted)); *cf. Burri*, 35 F.4th at 1213 (holding that acts taken to interfere with an in-forum contract "target the forum state itself"). And that harm suffices to support personal jurisdiction. *See Will Co.*, 47 F.4th at 926 (explaining that "jurisdiction 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." (citation omitted)).

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

Defendants fail to make a "compelling case" that the exercise of jurisdiction would be

[3] The *WhatsApp* court distinguished between servers Defendants leased to "send malware and other commands to users' devices" and WhatsApp's servers, which "defendants' program sought out . . . to transmit malicious code through those servers." The former servers were incidental to Defendants' tortious activity; the latter were not. 472 F. Supp. 3d at 671–72. Like WhatsApp's servers, Apple's servers were indispensable to Defendants' tortious activity here.

unreasonable. *Ayla*, 11 F.4th at 979 (cleaned up). The seven reasonableness factors weigh heavily in favor of exercising personal jurisdiction here. *See id.* at 984 (reciting factors).

The second, fifth, and sixth factors favor this forum, especially given that Defendants are litigating *three* other similar cases here, including one in discovery. *WhatsApp Inc. v. NSO Group Techs. Ltd.*, No. 4:19-cv-07123 (N.D. Cal. Oct. 29, 2019); *Apple Inc. v. NSO Group Techs. Ltd.*, No. 3:21-cv-09078 (N.D. Cal. Nov. 23, 2021); *Corallo v. NSO Group Techs. Ltd.*, No. 3:22-cv-05229 (N.D. Cal. Sept. 13, 2022). The burden on Defendants "would not be substantial here, primarily because the defendants must litigate in [the forum] anyway." *Gates Learjet Corp. v. Jensen*, 743 F.2d 1325, 1333 (9th Cir. 1984). "[T]he 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), since two reside in the United States and the rest, including a U.S. citizen, reside in Central America, AC ¶¶ 14–31. Further, the "most efficient judicial resolution" favors this forum because, as this Court has concluded, there would likely "be an unduly burdensome duplication of labor and expense or conflicting results if" this case and the *Apple* case "are conducted before different Judges." N.D. Cal. Civ. L.R. 3-12(a); *see* Order, ECF No. 36. Defendants suggest that evidence and witnesses are located in Israel, *see* CM 6, but these considerations are "no longer weighed heavily given the modern advances in communication and transportation." *Silk v. Bond*, 65 F.4th 445, 459 (9th Cir. 2023) (citation omitted). And because Plaintiffs' "claims rest on the law of California and the United States," this forum will not only "provide 'the most efficient judicial resolution of the controversy,'" but also "better provide [Plaintiffs] 'convenient and effective relief.'" *Ayla*, 11 F.4th at 984 (citation omitted).

The first and fourth factors likewise favor this forum. Defendants interjected themselves into California's affairs by abusing Apple's infrastructure to develop and then use exploits to deliver Pegasus to Plaintiffs' and others' iPhones. *See supra* pp. 6–7; *Ayla*, 11 F.4th at 984; *WhatsApp*, 472 F. Supp. 3d at 676. Because Plaintiffs' claims arise from that in-forum conduct under U.S. and California law, *see supra* pp. 3–5, the fourth factor also favors this forum. *See Bos. Telecomms. Grp., Inc. v. Wood*, 588 F.3d 1201, 1212 (9th Cir. 2009) ("California's interest in this controversy [need not] somehow be unique or not shared with any other forum.").

The third and seventh factors are neutral at best. A "conflict with the sovereignty of the defendant's state 'is not dispositive because, if given controlling weight, it would always prevent suit against a foreign national in a United States court.'" *Sinatra*, 854 F.2d at 1199 (citation omitted). And "whether another reasonable forum exists becomes an issue only when the forum state is shown to be unreasonable." *Ayla*, 11 F.4th at 984–85 (cleaned up). Defendants have not shown that litigating in this Court would be unreasonable. *See WhatsApp*, 472 F. Supp. 3d at 677.

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

Alternatively, Defendants have sufficient "minimum contacts" with the United States as a whole for the exercise of personal jurisdiction under the federal long-arm statute. Fed. R. Civ. P. 4(k)(2). Plaintiffs' CFAA claims arise under federal law, and if Defendants were not subject to the personal jurisdiction of California, they would not be subject to the personal jurisdiction of any state. The only remaining question is whether the exercise of personal jurisdiction over Defendants would comport with due process. *See Will Co.*, 47 F.4th at 922. It would. Even if Defendants' contacts with Apple's servers in California fall short (which they do not), Defendants' case-related contacts with Apple's U.S.-based servers exceed the minimum required for personal jurisdiction. AC ¶¶ 38–41; *see* Apple Compl. ¶¶ 24, 26, 51; *Will Co.*, 47 F.4th at 927; *42 Ventures*, 2022 WL 2400030, at *4–5. The exercise of personal jurisdiction would also be reasonable. *See supra* pp. 7–9; *Lang Van*, 40 F.4th at 1041–43; *Atchley*, 22 F.4th at 234–36.

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

For similar reasons, Defendants fail to carry their burden in seeking dismissal for *forum non conveniens*, which is "an exceptional tool to be employed sparingly." *Glob. Commodities*, 972 F.3d at 1111 (citation omitted). Defendants fail to make "a clear showing of facts which establish such oppression and vexation of a defendant as to be out of proportion to plaintiff's convenience." *Id.* (cleaned up). The public and private interest factors favor Plaintiffs' choice of forum. *See Carijano v. Occidental Petrol. Corp.*, 643 F.3d 1216, 1224 (9th Cir. 2011) (reciting factors); *Dole Food Co., Inc. v. Watts*, 303 F.3d 1104, 1118 (9th Cir. 2002).

Public Interest. The public-interest factors overwhelmingly favor this forum. First, California and the United States have strong interests in this case. California has a compelling

interest in protecting California companies from being used as spyware vectors in violation of state law. *See Dole*, 303 F.3d at 1119 ("California has an interest in protecting corporations based in California."). California also has a strong interest in protecting the ability of El Faro's California readers to access El Faro's reporting, which was compromised by the Pegasus attacks against Plaintiffs. AC ¶ 4; *see id.* ¶¶ 6, 62. The United States has a strong interest in the issues presented here, as President Biden made plain in a recent executive order:

> The United States has a fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware that has been . . . misused . . . , in light of the core interests of the United States in protecting [U.S.] Government personnel and [U.S.] citizens around the world; . . . and defending . . . journalists against threats to their freedom and dignity.

Exec. Order. No. 14,093, 88 Fed. Reg. 18,957, 18,957 (Mar. 27, 2023); *see also* AC ¶¶ 1, 50–51. Indeed, the United States' interest in this case is especially compelling because one of the Plaintiffs is a U.S. citizen, AC ¶ 18, and the Pegasus attacks compromised Plaintiffs' communications with U.S. embassy officials, AC ¶¶ 5, 105, 121, 133. Second, this district and this Court are very familiar with the governing U.S. and California law, given the ongoing suits raising similar claims here. *See supra* p. 8. Finally, for the same reason, any special burdens involved in litigating this case would only be greater in another forum.

Defendants argue that Israel also has an interest in this case because Israel regulates the sale of Pegasus, CM 8–9, but Israel has not expressed any opposition to the litigation of this case or related cases in U.S. court. Even if it had, the clearly expressed domestic interests prevail.

Private Interest. The private-interest factors also favor this forum. This forum is the most convenient for the parties because Defendants are already litigating related cases here. *See supra* p. 8. Additionally, two of the Plaintiffs currently reside in the United States, AC ¶¶ 28, 31, and the remaining Plaintiffs "indicated a willingness to travel to the United States for trial" by "filing suit in California," *Carijano*, 643 F.3d at 1230. Although Defendants' evidence and witnesses might otherwise have been located abroad, they will already be present in this forum for the related cases. *Cf. Universal Ent. Corp. v. Aruze Gaming Am., Inc.*, 2020 WL 2840153, at *18 (D. Nev. May 30, 2020) ("[T]he witnesses and evidence necessary to these claims will already be in this forum due

to the underlying suit."); *Facebook, Inc. v. Studivz Ltd.*, 2009 WL 1190802, at *2 (N.D. Cal. May 4, 2009) ("Facebook currently is litigating an action in Germany that is extremely similar to the instant action."). Regardless, "while witnesses and documents related to the development, marketing, or operation" of Pegasus "may be in Israel, most if not all of that evidence will likely be capable of electronic transmission to the U.S. forum." *Wilson v. Playtika, Ltd.*, 349 F. Supp. 3d 1028, 1039 (W.D. Wash. 2018).

Defendants' arguments regarding the availability of witnesses and the enforceability of a judgment, CM 8, are unavailing. First, Defendants control the availability of their own witnesses, and Plaintiffs do not anticipate calling third-party witnesses from Israel. *Cf. Alternate Health USA Inc. v. Edalat*, 2022 WL 767573, at *8–9 (C.D. Cal. Mar. 14, 2022), *appeal docketed*, No. 22-55353 (9th Cir. Apr. 7, 2022) (concerning unwilling third-party witnesses in Canada). In any event, as Defendants concede, 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) (submitting requests for testimony of Israeli witnesses). Second, Defendants cite no authority for the assertion that "Israeli witnesses could . . . testify if this case were litigated in Israel, but they could not give the same testimony for use in this Court." CM 8. To the extent they rely on Israel's Defense Export Control Law, any prohibition on testimony relevant to this case would apply in Israeli courts, too. Decl. of Yaron Shohat Ex. A, at 22 (§ 15(a)(2)), ECF No. 46-3. And this case does not require evidence under the Israeli government's control. *Cf. Lueck v. Sundstrand Corp.*, 236 F.3d 1137, 1146–47 (9th Cir. 2001). Finally, Israel's Foreign Judgments Enforcement Law provides a framework for the enforcement of final judgments of foreign courts in civil matters. *See* § 3, Foreign Judgments Enforcement Law, 5718–1958, 12 LSI 82 (5718-1957/58), as amended (Isr.). The private-interest factors thus favor this forum, and the balance of all factors overwhelmingly favors this forum.

IV. Plaintiffs have adequately alleged their claims.

A complaint must allege facts that—construed "in the light most favorable to Plaintiffs"—"state a claim to relief that is plausible on its face." *Glazer Cap. Mgmt., L.P. v. Forescout Techs.,*

Inc., 63 F.4th 747, 763 (9th Cir. 2023) (cleaned up). The Amended Complaint stated plausible claims for relief under the CFAA, CDAFA, trespass to chattels, and intrusion upon seclusion.

A. Plaintiffs have adequately alleged violations of the CFAA.

The CFAA prohibits exactly the type of unauthorized access alleged in this case. As multiple courts have held, those responsible for creating and installing malware or spyware are liable under the CFAA. *See Microsoft Corp. v. John Does 1–8*, 2015 WL 4937441, at *9 (E.D. Va. Aug. 17, 2015) (explaining that the core of the CFAA protects against "fraudulent conduct facilitated by malware and botnet activity"); *Microsoft Corp. v. Does 1–2*, 2021 WL 4755518, at *7 (E.D.N.Y. May 28, 2021), *R&R adopted*, 2021 WL 4260665 (E.D.N.Y. Sept. 20, 2021) (entering default judgment on CFAA claim where defendants created infrastructure that allowed them "to control infected computers without the users' knowledge").

Defendants' counterarguments are unavailing.

First, Plaintiffs have adequately alleged damage to their devices. The Pegasus attacks disabled certain Apple iOS features on Plaintiffs' iPhones, infected the devices with spyware, and enabled Defendants and their clients to control the devices without Plaintiffs' knowledge or consent. *See* AC ¶ 140. This is precisely the type of "damage" the CFAA guards against. *See* 18 U.S.C. § 1030(e)(8) (defining "damage" as "any impairment to the integrity or availability of data, a program, a system, or information"). Defendants' argument that the installation of spyware on a device does not damage it, CM 10, is both absurd and incorrect as a matter of law. Infecting a device with spyware is not akin to merely copying data from a device, CM 9; it damages the device, which "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); *accord John Does 1–8*, 2015 WL 4937441, at *9.[4] Defendants' related argument that, despite disabling some device

[4] *Goodman v. Goodman*, 2022 WL 17826390 (S.D.N.Y. Dec. 21, 2022), *R&R adopted*, 2023 WL 1967577 (S.D.N.Y. Feb. 12, 2023), is not to the contrary. In that case, the plaintiff failed to explain how the defendant's installation of "third-party utilities" on his computer had "actually impaired" it. *Id.* at *7. Here, Plaintiffs have explained how Defendants' conduct damaged the integrity of their devices and the data stored on them.

features, they did not cause "damage" because Plaintiffs could technically continue to "use their devices or access their data," CM 10, is similarly unsupported. Disabling features necessarily "impair[s]" the device. 18 U.S.C. § 1030(e)(8). In any event, Plaintiffs explicitly alleged that the impairment to their devices' crash reporting system did affect their ability to use the devices by enabling Defendants to evade the devices' security measures and install Pegasus. AC ¶ 40.

Second, Plaintiffs have adequately alleged loss as well. As an initial matter, the Pegasus attacks diminished the value of Plaintiffs' iPhones, *see* AC ¶ 140, which can no longer serve their primary purposes of private communication and computing. This is not a "subjective loss," CM 10, because a device transformed into a surveillance tool clearly can no longer be used for private communication.[5] Plaintiffs have also properly pleaded loss through the time they were required to spend investigating and remediating the attacks. *See* AC ¶¶ 61, 67, 71, 75, 79, 83, 87, 91, 95, 99, 103, 107, 111, 115, 119, 123, 127, 131, 135–36. Despite Defendants' protests, CM 11, this time constitutes "loss." *See Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) ("It is undisputed that Facebook employees spent many hours, totaling more than $5,000 in costs, analyzing, investigating, and responding to Power's actions. Accordingly, Facebook suffered a loss under the CFAA."). Finally, although overlooked by Defendants, many Plaintiffs incurred further financial losses from the Pegasus attacks because they had to purchase new external hard drives, security software, or devices. *See* AC ¶¶ 71, 75, 79, 87, 95, 107, 111, 123, 127, 131.

Third, Plaintiffs have adequately alleged that Defendants' conduct led to more than $5,000 of loss in a one-year period. Where, as here, Defendants and their clients used Pegasus in a "coordinated and sustained effort" against El Faro, attacking the devices "in a similar manner," and "caus[ing] similar damage," AC ¶ 63, losses stemming from the attacks may be aggregated. *E.g.*, *In re Apple & AT & TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008). In aggregate, Plaintiffs spent hundreds of hours investigating the attacks and remediating the harms caused by them. *See* AC ¶¶ 60–61, 67, 71, 75, 79, 83, 87, 91, 95, 99, 103, 107, 111, 115, 119, 123,

[5] In the cases on which Defendants rely, in contrast, the plaintiffs were unable to allege a causal connection between the damage to the device or data and the diminishment in its value. *See, e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1067 (N.D. Cal. 2012) (noting no allegation of impairment from consumption of some memory); CM 10 & n.6 (citing other cases).

127, 131, 135–36. Defendants argue that only losses incurred by Plaintiffs themselves count towards the statutory requirement, CM 12, but the plain text of 18 U.S.C. § 1030(c)(4)(A)(i)(I) and § 1030(e)(11) includes at the very least losses to "any victim." *See United States v. Millot*, 433 F.3d 1057, 1060–61 (8th Cir. 2006) (holding losses include those felt by "1 *or more persons*"); *United States v. Janosko*, 642 F.3d 40, 41–42 (1st Cir. 2011); *Mintz v. Mark Bartelstein & Assocs. Inc.*, 906 F. Supp. 2d 1017, 1029 n.3 (C.D. Cal. 2012) (explaining that losses include "***reasonable cost[s] to any victim***"). Because El Faro, which owned many hacked devices, *see, e.g.*, AC ¶ 65, was undoubtedly also a victim of the Pegasus attacks, whether certain losses were technically borne by Plaintiffs or El Faro is of no moment: the losses suffice to meet the $5,000 threshold either way. *Walsh v. Microsoft Corporation*, *see* CM 12, is not to the contrary; there, the plaintiffs "state[d] cursorily" that the threshold had been met, 63 F. Supp. 3d 1312, 1320 (W.D. Wash. 2014), but did not specifically describe the aggregate losses as Plaintiffs have done here, AC ¶ 61.[6]

***Fourth*,** Plaintiffs have adequately pleaded a claim for aiding-and-abetting liability. Defendants argue that this liability does not exist under the CFAA, CM 12–13, but many cases—including some 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); *see also Fraser v. Mint Mobile, LLC*, 2022 WL 1240864, at *5 (N.D. Cal. Apr. 27, 2022) (dismissing claim but refusing to foreclose possibility of aiding-and-abetting liability); *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at *4 (N.D. Cal. Nov. 20, 2020) (same). These cases are correct: the CFAA embraces secondary liability, *see* 18 U.S.C. § 1030(b), and the fact that multiple participants are involved in a CFAA violation does not mean that each of them escapes liability,

[6] These allegations, which approximate the time each plaintiff spent on specific investigation- and remediation-related activities, are far more detailed than those made in the cases on which Defendants rely, CM 11, 12 n.8. *See Wesch v. Yodlee, Inc.*, 2021 WL 1399291, at *7 (N.D. Cal. Feb. 16, 2021) (rejecting allegations made "in a conclusory fashion"); *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 949 (N.D. Cal. 2014) (same); *Goodman*, 2022 WL 17826390, at *10 (rejecting allegations that did not distinguish countable investigative costs and uncountable losses relating to divorce proceedings); *MSC Safety Sols., LLC v. Trivent Safety Consulting, LLC*, 2020 WL 7425874, at *9 (D. Colo. Dec. 18, 2020) (faulting plaintiff at summary judgment stage for failure to account for time investigating the defendant's conduct).

cf. Power Ventures, 844 F.3d at 1067 ("[T]echnological gamesmanship or the enlisting of a third party to aid in access will not excuse liability.").

B. Plaintiffs have adequately alleged violations of California law.

Defendants' arguments regarding the nexus between Plaintiffs' claims and California, CM 13–14, and the damage to the Plaintiffs' iPhones, CM 14–15, fare no better on reprise.

***First*,** this case requires no extraterritorial application of California law because Defendants abused Apple's infrastructure in California to develop and deliver Pegasus to Plaintiffs' iPhones. *See supra* pp. 3–4. Because the question is "what kinds of California connections will suffice to trigger the relevant provisions of California law," *see Ward v. United Airlines, Inc.*, 466 P.3d 309, 319 (Cal. 2020), it is not surprising that the court questioned California connections in cases like *Nowak*, CM 13. In that case, the only wrongful conduct alleged was the defendants' receipt of stolen funds after the plaintiff was hacked and the plaintiff had not specified where that—or any other relevant conduct—had occurred. *See* 2020 WL 6822888, at *4–6; CM 13–14 (similar cases).

***Second*,** for the reasons stated above, *supra* pp. 12–13, the harms caused by the Pegasus attacks, including the disabling of certain Apple iOS features, constitute cognizable damage for purposes of both CDAFA and trespass to chattels. *See Multiven, Inc. v. Cisco Systems, Inc.*, 725 F. Supp. 2d 887, 895–96 (N.D. Cal. 2010) ("[T]he necessary elements of Section 502 do not differ materially from the necessary elements of the CFAA."); *In re Apple Device Performance Litig.*, 347 F. Supp. 3d 434, 455 (N.D. Cal. 2018) (holding that damage under trespass law is shown "when . . . the trespass 'impaired the condition, quality, or value of the personal property'" (citation omitted)).[7]

CONCLUSION

The Court should deny Defendants' Corrected Motion to Dismiss.

Dated: May 19, 2023

Respectfully submitted,

/s/ Carrie DeCell

[7] *WhatsApp* is not to the contrary. WhatsApp argued NSO Group's conduct impaired its ability to provide services to others, not to use its own servers. 472 F. Supp. 3d at 685. Here, Plaintiffs have alleged that Defendants' conduct impaired Plaintiffs' ability to use their own devices.

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

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

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