

Received by NSD/FARA Registration Unit 04/03/2020 10:13:44 AM

DISSEMINATED BY MERCURY PUBLIC AFFAIRS, LLC, A REGISTERED FOREIGN AGENT, ON BEHALF OF Q CYBER TECHNOLOGIES LTD. MORE INFORMATION IS ON FILE WITH THE DEPT. OF JUSTICE, WASHINGTON, DC.

Received by NSD/FARA Registration Unit 04/03/2020 10:13:44 AM

1 JOSEPH N. AKROTIRIANAKIS (Bar No. 197971)

jakro@kslaw.com

2 AARON S. CRAIG (Bar No. 204741)

acraig@kslaw.com

3 KING & SPALDING LLP

633 West Fifth Street, Suite 1700

4 Los Angeles, CA 90071

Telephone: (213) 443-4355

5 Facsimile: (213) 443-4310

6 Attorneys for Defendants NSO GROUP TECHNOLOGIES
7 LIMITED and Q CYBER TECHNOLOGIES LIMITED

8 UNITED STATES DISTRICT COURT

9 NORTHERN DISTRICT OF CALIFORNIA

10 OAKLAND DIVISION

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

13 Plaintiffs,

14 v.

15 NSO GROUP TECHNOLOGIES LIMITED
16 and Q CYBER TECHNOLOGIES LIMITED,

17 Defendants.

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

**DEFENDANTS NSO GROUP
TECHNOLOGIES LIMITED AND
Q CYBER TECHNOLOGIES LIMITED'S
NOTICE OF MOTION AND MOTION TO
DISMISS UNDER FEDERAL RULES OF
CIVIL PROCEDURE 12(B)(1), 12(B)(2),
12(B)(6), AND 12(B)(7); MEMORANDUM
OF POINTS AND AUTHORITIES IN
SUPPORT THEREOF**

Date: May 13, 2020

Time: 9:00 a.m.

Ctrm: 3

Action Filed: 10/29/2019

TABLE OF CONTENTS

	Page(s)
1	
2	
3	NOTICE OF MOTION 1
4	MEMORANDUM OF POINTS AND AUTHORITIES 1
5	I. BACKGROUND 2
6	A. Defendants’ Technology and Its Use in Preventing Terrorism and
7	Other Crimes..... 2
8	B. Use of Plaintiffs’ Services in Committing Terrorism and Other
9	Crimes..... 4
10	C. Alleged Use of Plaintiffs’ Services..... 6
11	II. THE COURT SHOULD DISMISS THE COMPLAINT FOR LACK OF SUBJECT-
12	MATTER JURISDICTION BECAUSE DEFENDANTS HAVE DERIVATIVE
13	FOREIGN SOVEREIGN IMMUNITY 8
14	A. This Court Lacks Subject-Matter Jurisdiction Under the FSIA 8
15	B. This Court Also Lacks Subject-Matter Jurisdiction Under the
16	Doctrine of Derivative Foreign Sovereign Immunity..... 9
17	III. THE COURT SHOULD DISMISS THE COMPLAINT BECAUSE IT LACKS
18	PERSONAL JURISDICTION OVER DEFENDANTS 11
19	A. Defendants Did Not Consent to Personal Jurisdiction in
20	California 11
21	B. The Court Lacks General Jurisdiction Over Defendants..... 12
22	C. The Court Lacks Specific Jurisdiction Over Defendants..... 13
23	1. Plaintiffs Do Not Allege That Defendants Purposefully
24	Directed Their Alleged Activities Toward California 13
25	2. Plaintiffs Do Not Allege That Defendants Purposefully
26	Availed Themselves of the Privilege of Conducting
27	Activities in California..... 16
28	3. Exercising Jurisdiction Over Defendants in California
	Would Be Unreasonable 16
	IV. THE COURT SHOULD DISMISS THE CASE UNDER RULE 12(B)(7) FOR
	FAILURE TO JOIN A NECESSARY PARTY 18

1 V. THE COURT SHOULD DISMISS PLAINTIFFS’ CFAA AND TRESPASS TO
2 CHATTELS CLAIMS FOR FAILURE TO STATE A CLAIM UNDER RULE
3 12(B)(6) 20
4 A. Plaintiffs Cannot State a CFAA Claim 20
5 1. Plaintiffs Cannot State a Claim Based on Defendants’
6 Alleged Access to Plaintiffs’ Servers Because They
7 Cannot Plead That Defendants Accessed the Servers
8 Without Authorization 20
9 2. Plaintiffs Cannot State a Claim Based on Defendants’
10 Alleged Access to WhatsApp Users’ Phones Because It
11 Did Not Harm Plaintiffs 22
12 3. Plaintiffs Cannot State a Claim for Conspiracy Because
13 They Do Not Plead Any Conduct That Would Violate
14 Section 1030(a) 23
15 B. Plaintiffs Cannot State a Claim for Trespass to Chattels Because
16 the Alleged Actions Did Not Damage WhatsApp’s Servers 23
17 VI. CONCLUSION 25
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Page(s)

Cases

Ackerson v. Bean Dredging LLC,
589 F.3d 196 (5th Cir. 2009) 10

Alicog v. Kingdom of Saudi Arabia,
860 F. Supp. 379 (S.D. Tex. 1994) 10

Amberson Holdings LLC v. Westside Story Newspaper,
110 F. Supp. 2d 332 (D.N.J. 2000) 15

Amoco Egypt Oil Co. v. Leonis Navigation Co.,
1 F.3d 848 (9th Cir. 1993) 18

Andrews v. Sirius XM Radio Inc.,
932 F.3d 1253 (9th Cir. 2019) 22

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 24

Axiom Foods, Inc. v. Acerchem Int’l, Inc.,
874 F.3d 1064 (9th Cir. 2017) 13, 14

Boschetto v. Hansing,
539 F.3d 1011 (9th Cir. 2008) 16

Broidy Capital Mgmt., LLC v. Qatar,
2018 WL 6074570 (C.D. Cal. Aug. 8, 2018) 9

Estate of Burkhart v. United States,
2008 WL 4067429 (N.D. Cal. Aug. 26, 2008) 19

Butters v. Vance Int’l, Inc.,
225 F.3d 462 (4th Cir. 2000) 10

Cabalce v. Thomas E. Blanchard & Assocs., Inc.,
797 F.3d 720 (9th Cir. 2015) 10

Campbell-Ewald Co. v. Gomez,
136 S. Ct. 663 (2016) 9, 10

Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs., Inc.,
334 F.3d 390 (4th Cir. 2003) 15

Core-Vent Corp. v. Nobel Indust. AB,
11 F.3d 1482 (9th Cir. 1993) 18

1	<i>Daimler AG v. Bauman</i> , 571 U.S. 117 (2014).....	12
2	<i>Dawavendewa v. Salt River Project Agric. Improvement & Power Dist.</i> ,	
3	276 F.3d 1150 (9th Cir. 2002)	19
4	<i>Depot, Inc. v. Caring for Montanans, Inc.</i> ,	
5	915 F.3d 643 (9th Cir. 2019)	7
6	<i>DEX Sys., Inc. v. Deutsche Post AG</i> ,	
7	727 F. App'x 276 (9th Cir. 2018)	15
8	<i>DNC v. Russian Fed'n</i> ,	
9	392 F. Supp. 3d 410 (S.D.N.Y. 2019).....	9
10	<i>Doğan v. Barak</i> ,	
11	2016 WL 6024416 (C.D. Cal. Oct. 13, 2016).....	9
12	<i>Doğan v. Barak</i> ,	
13	932 F.3d 888 (9th Cir. 2019)	9
14	<i>Facebook, Inc. v. Power Ventures, Inc.</i> ,	
15	844 F.3d 1058 (9th Cir. 2016)	22
16	<i>Friends of Amador Cty. v. Salazar</i> ,	
17	2011 WL 4709883 (E.D. Cal. Oct. 4, 2011).....	19
18	<i>Glencore Grain Rotterdam B.V. v. Shivnath Rai Harnarain Co.</i> ,	
19	284 F.3d 1114 (9th Cir. 2002)	17
20	<i>GreatFence.com, Inc. v. Bailey</i> ,	
21	726 F. App'x 260 (5th Cir. 2018)	15
22	<i>Hungerstation LLC v. Fast Choice LLC</i> ,	
23	2020 WL 137160 (N.D. Cal. Jan. 13, 2020).....	14
24	<i>IAM v. OPEC</i> ,	
25	649 F.2d 1354 (9th Cir. 1981)	11
26	<i>Intel Corp. v. Hamidi</i> ,	
27	30 Cal. 4th 1342 (2003)	23, 24
28	<i>Interface Partners Int'l Ltd. v. Hananel</i> ,	
	575 F.3d 97 (1st Cir. 2009).....	18
	<i>In re iPhone App. Litig.</i> ,	
	844 F. Supp. 2d 1040 (N.D. Cal. 2012)	24
	<i>Israel Discount Bank Ltd. v. Schapp</i> ,	
	505 F. Supp. 2d 651 (C.D. Cal. 2007)	18

1	<i>Ivey v. Lynch,</i>	
	2018 WL 3764264 (M.D.N.C. Aug. 8, 2018).....	10
2	<i>Joseph Saveri Law Firm, Inc. v. Criden,</i>	
3	696 F. App'x 189 (9th Cir. 2017)	15
4	<i>LVRC Holdings LLC v. Brekka,</i>	
5	581 F.3d 1127 (9th Cir. 2009)	21
6	<i>Martinez v. Aero Caribbean,</i>	
7	764 F.3d 1062 (9th Cir. 2014)	12
8	<i>Moriah v. Bank of China Ltd.,</i>	
9	107 F. Supp. 3d 272 (S.D.N.Y. 2015).....	10, 19
10	<i>Mount v. PulsePoint, Inc.,</i>	
11	2016 WL 5080131 (S.D.N.Y. Aug. 17, 2016).....	24
12	<i>Myers v. United States,</i>	
13	323 F.2d 580 (9th Cir. 1963)	10
14	<i>Otani Props., L.P. v. Centerline Tool, Inc.,</i>	
15	2016 WL 10999268 (C.D. Cal. Mar. 28, 2016).....	19
16	<i>Pam Int'l, Inc. v. James,</i>	
17	2006 WL 8455280 (S.D. Cal. Aug. 3, 2006)	12
18	<i>Perkins v. Benguet Consolidated Mining Co.,</i>	
19	342 U.S. 437 (1952).....	12
20	<i>Picot v. Weston,</i>	
21	780 F.3d 1206 (9th Cir. 2015)	16
22	<i>Rep. of the Philippines v. Pimentel,</i>	
23	553 U.S. 851 (2008).....	19
24	<i>Rosen v. Terapeak, Inc.,</i>	
25	2015 WL 12724071 (C.D. Cal. Apr. 28, 2015)	14
26	<i>Royal Wulff Ventures LLC v. Primero Mining Corp.,</i>	
27	938 F.3d 1085 (9th Cir. 2019)	11
28	<i>Safe Air for Everyone v. Meyer,</i>	
	373 F.3d 1035 (9th Cir. 2004)	8
	<i>Schwarzenegger v. Fred Martin Motor Co.,</i>	
	374 F.3d 797 (9th Cir. 2004)	11, 12, 13, 16
	<i>Sea Breeze Salt, Inc. v. Mitsubishi Corp.,</i>	
	2016 WL 8648638 (C.D. Cal. Aug. 18, 2016).....	11

1	<i>Siderman de Blake v. Rep. of Argentina</i> ,	
	965 F.2d 699 (9th Cir. 1992)	9
2	<i>Stewart v. Screen Gems–EMI Music, Inc.</i> ,	
3	81 F. Supp. 3d 938 (N.D. Cal. 2015)	14
4	<i>Synopsys, Inc. v. Ubiquiti Networks, Inc.</i> ,	
5	313 F. Supp. 3d 1056 (N.D. Cal. 2018)	24
6	<i>Theofel v. Farey-Jones</i> ,	
	359 F.3d 1066 (9th Cir. 2004)	22
7	<i>United States v. Nosal</i> ,	
8	676 F.3d 854 (9th Cir. 2012)	22
9	<i>Walden v. Fiore</i> ,	
10	571 U.S. 277 (2014).....	13, 14, 15
11	<i>Walenco, Inc. v. Corbell</i> ,	
	126 F. Supp. 3d 1154 (E.D. Cal. 2015).....	23
12	<i>Yearsley v. W.A. Ross Constr. Co.</i> ,	
13	309 U.S. 18 (1940).....	9
14	Statutes and Rules	
15	18 U.S.C.	
	§ 1030(a)(2)(C)	20, 21, 23
16	§ 1030(a)(4)	20, 21
17	§ 1030(b)	20, 23
	§ 1030(e)(11)	22, 23
18	§ 1030(g).....	22, 23
19	28 U.S.C.	
	§ 1604.....	9
20	§ 1605(a)(2)	9
21	§ 1605(a)(5)	9
22	Fed. R. Civ. P.	
	12(b)(7)	18
23	19.....	18
	19(1)(A)	19
24	19(b)(1)	19
25	Other Authorities	
26	Dan Sabbagh, <i>Call for Backdoor Access to WhatsApp as Five Eyes Nations Meet</i> ,	
27	The Guardian (July 30, 2019, 3:32 p.m.).....	5
28	Dipesh Gadhur, <i>London Bridge Terror Attack Planned on WhatsApp, Sunday</i>	
	Times (May 12, 2019).....	5

1 Dov Lieber et al., *Police Tracked a Terror Suspect—Until His Phone Went Dark*
2 *After a Facebook Warning*, Wall St. J. (Jan. 2, 2020, 3:29 pm)6
3
4 Facebook, *Join Us in Facebook Israel as We Bring the World Closer Together*,
5 <https://bit.ly/3dkyhoC>18
6
7 Gordon Rayner, *WhatsApp Accused of Giving Terrorists ‘A Secret Place to Hide’*
8 *as It Refuses to Hand over London Attacker’s Messages*, The Telegraph (Mar.
9 27, 2017, 1:54 p.m.)5
10
11 Katie Benner & Mike Isaac, *Child-Welfare Activists Attack Facebook over*
12 *Encryption Plans*, N.Y. Times (Feb. 5, 2020)5
13
14 NSPCC, *Facebook Must Be Stopped from Creating Hiding Places for Child*
15 *Abuse* (Dec. 5, 2019), <https://bit.ly/2TxrtfH>5
16
17 Ryan Sabey, *Tool of Terror: Social Media Giants Will Be Made to Hand Over*
18 *Encrypted WhatsApp Messages in Fight Against Terrorism*, The Sun (Sept.
19 29, 2019, 7:45 a.m.)5
20
21
22
23
24
25
26
27
28

1 TO THE COURT AND PLAINTIFFS AND THEIR COUNSEL:

2 PLEASE TAKE NOTICE that on May 13, 2020, at 9:00 a.m., or as soon thereafter as the
3 matter may be heard, Defendants NSO Group Technologies Limited (“NSO”) and Q Cyber
4 Technologies Limited (“Q Cyber”) will bring on for hearing before the Honorable Phyllis J.
5 Hamilton, Chief United States District Judge, in Courtroom 3 of the United States Courthouse
6 located in the Ronald V. Dellums Federal Building & United States Courthouse, 1301 Clay Street,
7 Oakland, California, a Motion to Dismiss the Complaint of Plaintiffs WhatsApp Inc., and
8 Facebook, Inc., under Rules 12(b)(1), 12(b)(2), 12(b)(6), and 12(b)(7) of the Federal Rules of Civil
9 Procedure. This motion is based on this Notice of Motion and Motion, the following Memorandum
10 of Points and Authorities, the concurrently-filed Declarations of NSO Chief Executive Officer
11 Shalev Hulio, NSO Chief Financial Officer Nachum Falek, and Joseph N. Akrotirianakis, the
12 pleadings, papers and records on file in this case, and such oral argument as may be presented.

13 By this Motion, Defendants ask the Court to dismiss the Complaint with prejudice.

14 **POINTS AND AUTHORITIES**

15 Seeking to extend the Computer Fraud and Abuse Act and other causes of action well
16 beyond existing precedent, Plaintiffs bring this action to prevent Defendants from licensing NSO’s
17 Pegasus technology that enables sovereign governments to investigate and combat terrorism, child
18 exploitation, and other heinous crimes.

19 Encrypting communications, like locking doors, serves important goals. As a collateral
20 consequence, however, terrorists and criminals take advantage of Plaintiffs’ services to plan and
21 execute illegal schemes, while Plaintiffs disclaim all responsibility for the consequences. NSO
22 supplies governments with a technology they can use to enforce their laws and protect their
23 citizens, much as a manufacturer of a Slim Jim tool outfits police to unlock doors. In this case,
24 however, NSO takes precautions so that only government agencies, not criminals, can use NSO
25 Pegasus technology.

26 This Court should dismiss the Complaint with prejudice under Federal Rule of Civil
27 Procedure 12(b)(1) and (2). Plaintiffs cannot establish the Court’s subject matter jurisdiction—
28 because the conduct alleged in the Complaint was performed by governments protected by the

1 Foreign Sovereign Immunities Act—or personal jurisdiction over Defendants,

2 Moreover, this case should be dismissed under Rule 12(b)(7) because Defendants’
3 sovereign customers are necessary parties who cannot be joined under Rule 19. Finally, the
4 allegations, even if accepted as true as required in a challenge under Rule 12(b)(6), do not
5 adequately plead several of the claims alleged.

6 **I. BACKGROUND**

7 **A. Defendants’ Technology and Its Use in Preventing Terrorism and Other
8 Crimes**

9 Defendant NSO is an Israeli technology company that designs and markets a highly-
10 regulated technology to government agencies for uses such as counterterrorism and investigating
11 child exploitation and other serious crimes.¹ (Compl. ¶ 5; Declaration of Shalev Hulio (“Hulio
12 Decl.”) ¶¶ 5-9.) Defendant Q Cyber, also an Israeli corporation, is NSO’s sole director and majority
13 shareholder. (Compl. ¶ 6; Hulio Decl. ¶ 1.) Defendants’ customers are exclusively government
14 agencies. (Hulio Decl. ¶ 9; Declaration of Nachum Falek (“Falek Decl.”) Exh. 1.) Plaintiffs
15 erroneously allege in their Complaint that Defendants’ customers include private entities, citing
16 three newspaper articles. (Compl. ¶ 43 & n.2.) None of the cited articles makes that assertion,
17 however, and it is false. NSO licenses its Pegasus technology only to sovereign government
18 agencies and not to any private entity.² (Hulio Decl. ¶ 9, Falek Decl., Exh. 1.)

19 ¹ The exhibits to the Complaint demonstrate this. They include a purported email to the Drug
20 Enforcement Agency discussing intelligence applications of NSO’s technology (Exh. 2); a
21 document entitled “Our Technology: Helping Governments Maintain Public Safety,” which
22 describes NSO’s Pegasus technology as “best-in-class technology to help government agencies
23 detect and prevent a wide-range of local and global threats” and to “help government intelligence
24 and law-enforcement agencies use technology to meet the challenges of encryption to prevent and
25 investigate terror and crime.” (Exh. 8); a “Product Description” document that describes NSO’s
26 Pegasus technology as “a world-leading cyber intelligence solution that enables law enforcement
27 and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any
28 mobile device.” (Exh. 10 at 31); and a purported NSO customer agreement from 2015 with a
foreign government’s communications authority. (Exh. 11).

² Facebook once tried to obtain a license from NSO to use certain capabilities of the Pegasus
program, the software at issue in this case, in order to circumvent privacy restrictions imposed on
it by third party(ies). (Hulio Decl. ¶ 10.) Facebook is, of course, not a government agency that
conducts counterterrorism and criminal investigations, and NSO declined the sale. (*Id.*)

1 The export of NSO's Pegasus technology is regulated under Israel's Defense Export
2 Control Law ("ECL"). (Hulio Decl. ¶ 5 and Exh. A.) To export its Pegasus technology, NSO is
3 required to register with the Israeli Ministry of Defense ("MoD") and obtain appropriate export
4 licenses. (Hulio Decl. ¶ 6.) Under the ECL, the MoD may investigate NSO and its business and to
5 refuse or cancel NSO's registration. (*Id.*) The MoD is also authorized to grant or deny NSO's
6 licenses, taking into account several factors, including the intended use of NSO's technology and
7 the identity of its customers, as well as to revoke NSO's licenses entirely. (ECL, Hulio Decl. Exh.
8 A, Ch. C (3-4)). The MoD may also request declarations from NSO and information about its
9 customers, and their intended uses of its Pegasus technology. (ECL, *Id.* Ch. D 6 (b)(1-4)). As
10 Plaintiffs' own submissions to the Court demonstrate, the requirements that NSO customers
11 demonstrate their identities and provide any other necessary documentation for approval by the
12 MoD are built directly into NSO customer contracts. (Compl. Exh. 11 § 5.1; Hulio Decl. ¶¶ 6-7).
13 MoD also requires NSO to have Pegasus' end users sign end-use certificates declaring that NSO's
14 Pegasus technology "will be used only for prevention and investigation of terrorism and criminal
15 activity." (Hulio Decl. ¶ 8.)

16 In addition, NSO has voluntarily undertaken additional steps to ensure that its Pegasus
17 technology is used responsibly by authorized public safety authorities. NSO takes into account
18 U.S. and European Union export control restrictions in addition to the ECL. (Hulio Decl. ¶ 11.) It
19 conducts due diligence on all potential customers, examining publicly available information, rule-
20 of-law considerations, questionnaires, and other items. (*Id.*) As is shown in the exhibits to the
21 Complaint, government customers contractually must provide these due diligence materials before
22 receiving NSO technology. (Compl. Exh. 11 § 2.2.)³

23 NSO requires its customers—the government agencies that license NSO's Pegasus
24

25
26 ³ NSO follows an internal process for investigating any misuse. If NSO suspects any improper use
27 of its Pegasus technology by a customer other than in conformity with the customer's contract with
28 NSO, service to that customer would be suspended pending NSO's investigation, and if that
investigation revealed ongoing misuse, that customer's license would be terminated. (Hulio Decl.
¶ 17.)

1 technology—to agree that they (1) will use NSO technology “only for the prevention or
2 investigation of crimes and terrorism and ensure that the [technology] will not be used for human
3 rights violations” and (2) will immediately notify NSO of any potential misuse. (Hulio Decl. ¶ 12;
4 Compl. Exh. 11, Sec. 2.1 (obligating customer to use NSO technology solely for its intended
5 purpose).) Defendants contractually can suspend—and have suspended, and would terminate—
6 service to customers engaged in any improper use of NSO’s Pegasus technology outside these
7 parameters. (Hulio Decl. ¶ 12; Compl. Exh. 11, Sec. 7). Israel may itself deny or revoke export
8 licenses if the Israeli government learns of an abuse of the Pegasus technology or non-compliance
9 with the intended use, such as a use of the technology to violate human rights. (Hulio Decl. ¶ 12.)

10 Moreover, Defendants’ technology is designed with technical safeguards, such as general
11 and customer-specific geographic limitations. (Compl. Exh. 11 at Exhibit A [Dkt. No., 1-1 at p.
12 74].) One of the limitations is that NSO’s technology *cannot* be used against U.S. mobile phone
13 numbers or devices within the United States.. (Compl. Exh. 11 at Exhibit D [Dkt. No. 1-1 at p.
14 111]; Hulio Decl. ¶ 13.)

15 In summary, as NSO’s Chief Executive Officer and auditor state, and as Plaintiffs’ pleading
16 corroborates, Defendants (1) license Pegasus exclusively to government agencies, (2) are regulated
17 by Israeli export control law, (3) voluntarily impose informational and other due diligence
18 requirements on all Pegasus customers, (4) license their Pegasus technology only for national
19 security and law enforcement purposes such as the prevention and investigation of terrorism and
20 other serious criminal activity, and (5) can cancel or suspend service for misuse of NSO’s Pegasus
21 technology and have done so.

22 **B. Use of Plaintiffs’ Services in Committing Terrorism and Other Crimes**

23 Plaintiff WhatsApp, which is owned by Plaintiff Facebook, alleges it offers an “encrypted
24 communication service” for mobile phones and computers. (Compl. ¶¶ 16-17.) Plaintiffs provide
25 communications services globally through WhatsApp, Facebook Messenger, and Instagram, and
26 allege that “1.5 billion people in 180 countries” use their services. (*Id.*)

27 Violent criminals and some of the world’s most brutal and dangerous terrorists use
28 Plaintiffs’ services to plan and execute their crimes, while Plaintiffs disclaim responsibility and

1 leave it to others—sovereign governments and innocent victims—to deal with the horrendous
2 crimes facilitated by WhatsApp. For example, the Islamic State terrorist who attacked London’s
3 Westminster Bridge in 2017 used WhatsApp “two minutes before killing five” in the attack. Ryan
4 Sabey, *Tool of Terror: Social Media Giants Will Be Made to Hand Over Encrypted WhatsApp*
5 *Messages in Fight Against Terrorism*, The Sun (Sept. 29, 2019, 7:45 a.m.),
6 <https://bit.ly/2TuLNhK>. Facebook refused to reveal the terrorist’s message to authorities, a
7 decision the United Kingdom’s Home Secretary called “completely unacceptable.” Gordon
8 Rayner, *WhatsApp Accused of Giving Terrorists ‘A Secret Place to Hide’ as It Refuses to Hand*
9 *over London Attacker’s Messages*, The Telegraph (Mar. 27, 2017, 1:54 p.m.),
10 <https://bit.ly/38uHkjl>.

11 Three months later, terrorists used WhatsApp to plan a “knife rampage” on London Bridge.
12 Dipesh Gadher, *London Bridge Terror Attack Planned on WhatsApp*, Sunday Times (May 12,
13 2019, 12:01 a.m.), <https://bit.ly/38xG2Uy>. Their use of WhatsApp “may have prevented the
14 authorities from identifying the plot.” *Id.* But Plaintiffs again refused to give authorities access to
15 the terrorists’ messages. Dan Sabbagh, *Call for Backdoor Access to WhatsApp as Five Eyes*
16 *Nations Meet*, The Guardian (July 30, 2019, 3:32 p.m.), <https://bit.ly/2InSNpZ>.

17 It is no surprise that Plaintiffs dislike Defendants’ technology, because it enables sovereign
18 governments to expose how Plaintiffs’ platform is used as a safe space for terrorists and other
19 criminals to operate without fear of detection by law enforcement.⁴ In May 2019, for example,
20 Facebook notified 1,400 users that their WhatsApp accounts may have been compromised by

21 _____
22 ⁴ In one survey of 32 police forces in the United Kingdom and Wales, the National Society for the
23 Prevention of Cruelty to Children (“NSPCC”) found that Plaintiffs’ products were used repeatedly
24 in crimes against children, including “2,009 instances reported on Instagram, 1,719 on Facebook
25 or Facebook Messenger, and almost 300 on WhatsApp.” According to the NSPCC, “Facebook,
26 Instagram and WhatsApp were used in child abuse image and online child sexual offences . . . an
27 average of 11 times a day.” NSPCC, *Facebook Must Be Stopped from Creating Hiding Places for*
28 *Child Abuse* (Dec. 5, 2019), <https://bit.ly/2TxrtfH>. NSPCC is not alone: a coalition of 129 child-
protection services recently confronted Facebook about its decision to “allow child predators to
operate with impunity across the company’s apps.” Katie Benner & Mike Isaac, *Child-Welfare*
Activists Attack Facebook over Encryption Plans, N.Y. Times (Feb. 5, 2020),
<https://nyti.ms/2Isrn2t>.

1 government actors relying on NSO’s technology. (Compl. ¶ 44.) At least one of the users Facebook
2 alerted was an Islamic State terrorist who was using WhatsApp to plan an attack during the winter
3 holiday season. Dov Lieber et al., *Police Tracked a Terror Suspect—Until His Phone Went Dark*
4 *After a Facebook Warning*, Wall St. J. (Jan. 2, 2020, 3:29 pm), <https://on.wsj.com/38uXk5s>.
5 Facebook’s warning “killed” an investigation into the terrorist by a “team of European law-
6 enforcement officials” who had been monitoring the terrorist’s WhatsApp messages with NSO’s
7 technology. *Id.*

8 **C. Alleged Use of Plaintiffs’ Services**

9 Plaintiffs mistakenly allege in their Complaint that Defendants obtained “unauthorized
10 access [to] and abuse[d] . . . the WhatsApp Service and computers.” (Compl. ¶ 1.) Those
11 allegations are false in two fundamental respects: Defendants did not commit the alleged acts, and
12 the alleged acts did not involve unauthorized access to WhatsApp computers.

13 Most significantly, Plaintiffs conflate the actions of Defendants with the actions of NSO’s
14 sovereign customers (as other portions of the Complaint recognize, *e.g.*, ¶ 29). Plaintiffs’ pleadings
15 show that Defendants license NSO’s Pegasus technology to government law enforcement and
16 intelligence agencies and assist with the training, setup, and installation of the Pegasus technology.
17 Defendants do not operate the Pegasus technology—their government customers do that, making
18 all decisions about how to use the Pegasus technology. (Compl. Exh. 10 at 55 (“NSO is responsible
19 to deploy and configure the Pegasus hardware and software at the customer premises”), 58 (“All
20 the necessary hardware is supplied with the system upon deployment and may require local
21 customization that has to be handled by the customer”), 61 (“We [NSO] are responsible for the
22 system setup and training before its hand-over to the customer”); Hulo Decl. ¶ 14)

23 If anyone installed Pegasus on any alleged “Target Devices” (Compl. ¶ 1) it was not
24 Defendants. It would have been an agency of a sovereign government. (Hulo Decl. ¶ 15.)
25 Defendants’ business model consists of selling NSO’s Pegasus technology to governments and
26 providing basic technical support for them. All support activities by NSO are performed entirely
27 at NSO’s customers’ direction. (Hulo Decl. ¶ 14; Compl. ¶ 29 (describing Defendants’ role as
28 licensing, selling support services and offering technical support).) Contrary to Plaintiffs’ salacious

1 allegations (Compl. ¶ 42), any government agencies that used NSO’s Pegasus technology acted
2 within the scope of their sovereign authority to investigate crimes and prevent acts of terror. (Hulio
3 Decl. ¶¶ 14-15); *see* Lieber et al., *supra*.

4 Defendants did not target anyone, and in fact contractually prohibit their customers from
5 using NSO’s Pegasus technology against people who are not suspected terrorists or criminals.
6 (Hulio Decl. ¶ 17.) If a government ever misused NSO’s Pegasus technology to monitor WhatsApp
7 users other than criminals or terrorists, Defendants have no knowledge of that misuse, which would
8 be a violation of that government’s contract with NSO. (*Id.*)

9 In short, all of the alleged conduct Plaintiffs challenge was conducted by sovereign
10 governments outside of the United States. (Hulio Decl. ¶¶ 13-14; *see* Compl. ¶ 43). To challenge
11 that conduct, Plaintiffs must ask this Court to declare illegal the sovereign acts of those
12 governments. For that reason, permitting this litigation to proceed would infringe critical national
13 security and foreign policy concerns of sovereign governments.

14 Even if Defendants (as opposed to government agencies) had sent messages to WhatsApp
15 users in the manner alleged by Plaintiffs,⁵ it would have been within the scope of conduct
16 authorized by Plaintiffs. Plaintiffs allege that Defendants’ employees used WhatsApp subject to
17 WhatsApp’s Terms of Service (“TOS”). (Compl. ¶ 30.) The TOS grant users a “license to use
18 [WhatsApp’s] Services,”⁶ which requires sending messages through WhatsApp’s servers. (*See*
19 Compl. ¶ 36 (explaining that WhatsApp’s servers “facilitate[] the initiation of calls between
20 different devices” and “facilitate[] certain data transmissions over the WhatsApp Service”).)
21 Plaintiffs do not contend that Defendants had no right to use WhatsApp’s servers. Instead,
22 Plaintiffs claim that Defendants “were not authorized to use [the] servers in the[] manner” that
23 they allegedly used them. (Compl. ¶ 36; *see id.* ¶¶ 21–23.)

24
25 ⁵ This allegation is false, but the Court is required to indulge it as true for purposes of Defendants’
26 Rule 12(b)(6) motion. *Depot, Inc. v. Caring for Montanans, Inc.*, 915 F.3d 643, 653 (9th Cir.
2019).

27 ⁶ <https://www.whatsapp.com/legal?eea=0#terms-of-service>. Plaintiffs incorporate the TOS by
28 reference in the Complaint. (Compl. ¶ 19.)

1 Yet Plaintiffs do not allege Defendants used the servers for anything other than to send
2 messages. Plaintiffs do not allege Defendants stole data from Plaintiffs, altered data on Plaintiffs’
3 servers, or obtained information from the servers. And Plaintiffs do not allege Defendants have
4 done anything since May 2019, when Plaintiffs contend they closed the “vulnerability” that
5 Defendants allegedly used to send messages. (Compl. ¶ 44.)

6 **II. THE COURT SHOULD DISMISS THE COMPLAINT FOR LACK OF SUBJECT-**
7 **MATTER JURISDICTION BECAUSE DEFENDANTS HAVE DERIVATIVE**
8 **FOREIGN SOVEREIGN IMMUNITY**

9 Plaintiffs seek to hold Defendants liable for alleged national-security and law enforcement
10 operations performed by sovereign governments. Plaintiffs mistakenly allege that Defendants
11 performed those operations, but that is contradicted by the Plaintiffs’ own pleadings, and it is false.
12 Because the alleged conduct was carried out by sovereign governments, the Foreign Sovereign
13 Immunities Act divests this Court of subject-matter jurisdiction.

14 Even if the Court accepts Plaintiffs’ allegations as true,⁷ the Court would still lack subject-
15 matter jurisdiction because Defendants are protected by derivative foreign sovereign immunity. If
16 Plaintiffs were suing the sovereign governments directly, those governments would be immune.
17 Defendants, as agents of those governments who acted at their direction, are derivatively immune.

18 **A. This Court Lacks Subject-Matter Jurisdiction Under the FSIA**

19 Defendants did not conduct any of the activities that form the basis of Plaintiffs’ claims.
20 Most importantly, Defendants did not use WhatsApp’s servers to install NSO’s Pegasus
21 technology on any WhatsApp user’s device. (Hulio Decl. ¶¶ 14-15, 17). As described above and
22 in the accompanying declaration of NSO CEO Shalev Hulio, if any entity did so, it was a sovereign
23 government acting to protect its own interests. *Supra* Part I.C; (Hulio Decl. ¶ 15).⁸

24 Those sovereign governments, however, cannot be sued in this Court. The FSIA “sets forth

25 ⁷ The Court may consider extrinsic evidence in support of Defendants’ Rule 12(b)(1) motion and
26 need not accept the allegations in the Complaint as true. *Safe Air for Everyone v. Meyer*, 373 F.3d
1035, 1039 (9th Cir. 2004).

27 ⁸ All of Defendants’ customers are sovereign governments. (Hulio Decl. ¶ 9; Falek Decl. Exh. 1.)
28 Plaintiffs make no credible allegation that any customer was not a sovereign government; nor
could they.

1 the general rule that foreign states are immune from the jurisdiction of both federal and state courts
2 in the United States.” *Siderman de Blake v. Rep. of Argentina*, 965 F.2d 699, 706 (9th Cir. 1992).
3 Unless one of the FSIA’s exceptions apply, “[a] federal court lacks subject matter jurisdiction over
4 a claim against a foreign state.” *Id.*; see 28 U.S.C. § 1604.

5 There is no plausible argument that any of the FSIA’s exceptions apply in this case. The
6 “commercial activity” exception, 28 U.S.C § 1605(a)(2), does not apply because using technology
7 in the manner alleged in the complaint is not “the type of action by which private, commercial
8 enterprises typically engage in trade or commerce.” *Broidy Capital Mgmt., LLC v. Qatar*, 2018
9 WL 6074570, at *8–9 (C.D. Cal. Aug. 8, 2018); see *DNC v. Russian Fed’n*, 392 F. Supp. 3d 410,
10 429 (S.D.N.Y. 2019) (holding hacking by foreign government not commercial activity). And the
11 “noncommercial tort” exception, 28 U.S.C § 1605(a)(5), does not apply because it requires “one
12 entire tort”—“not only the injury but also the act precipitating that injury”—to have occurred in
13 the United States. *Broidy*, 2018 WL 6074570, at *4–5. Plaintiffs do not and cannot allege that any
14 entire tort occurred in the United States.

15 Because sovereign governments were the operators of NSO technology and no FSIA
16 exception applies, the FSIA bars this action.⁹ *Siderman de Blake*, 965 F.2d at 706; 28 U.S.C.
17 § 1604.

18 **B. This Court Also Lacks Subject-Matter Jurisdiction Under the Doctrine of**
19 **Derivative Foreign Sovereign Immunity**

20 It is well-settled that private agents of the United States have derivative sovereign
21 immunity when they are acting within the scope of their employment. *Campbell-Ewald Co. v.*
22 *Gomez*, 136 S. Ct. 663, 672 (2016); *Yearsley v. W.A. Ross Constr. Co.*, 309 U.S. 18, 21–22 (1940);

23 _____
24 ⁹ To the extent Plaintiffs challenge actions by foreign government officials, this Court lacks
25 jurisdiction under common-law sovereign immunity, which “extends to individual foreign officials
26 for ‘acts performed in [their] official capacity if the effect of exercising jurisdiction would be to
27 enforce a rule of law against the state[.]’” *Doğan v. Barak*, 932 F.3d 888, 893–94 (9th Cir. 2019).
28 That is the case here because foreign countries use Defendants’ technology “to advance their own
sovereign interests of fighting terrorism and serious crime.” (Hulio Decl. ¶ 14.) Those are
“irrefutably ‘official public acts.’” *Doğan v. Barak*, 2016 WL 6024416, at *9 (C.D. Cal. Oct. 13,
2016), *aff’d*, 932 F.3d 888.

1 *Ackerson v. Bean Dredging LLC*, 589 F.3d 196, 206 (5th Cir. 2009); *Myers v. United States*, 323
2 F.2d 580, 583 (9th Cir. 1963). The same principle applies to private agents acting on behalf of
3 foreign sovereigns. *Butters v. Vance Int’l, Inc.*, 225 F.3d 462, 466 (4th Cir. 2000).

4 The Ninth Circuit has yet to address derivative foreign sovereign immunity, but the Fourth
5 Circuit held in *Butters* that private actors are derivatively immune for actions that they take at the
6 direction of foreign sovereigns. *Id.* at 466. The plaintiff in that case was employed by a company
7 hired by Saudi Arabia. Saudi Arabian officials ordered the company not to promote the plaintiff,
8 and the company complied with the order. The plaintiff sued for gender discrimination, and the
9 Fourth Circuit held that the company was immune because it “was following Saudi Arabia’s
10 orders.” *Id.* at 466. The court relied on the rule that domestic contractors enjoy derivative immunity
11 when acting for the United States, finding that “[i]t is but a small step to extend this privilege to
12 the private agents of foreign sovereigns.” *Id.*¹⁰

13 Here, Defendants are entitled to derivative sovereign immunity under *Butters*. To the extent
14 they have any role in sovereign governments’ use of NSO’s technology, such as by setting up the
15 Pegasus technology for their sovereign customers and providing support services, Defendants act
16 “entirely at the direction of their government customers,” and “follow those directions
17 completely.” (*See* Hudio Decl. ¶ 14; *see also* Compl. ¶ 29 (describing Defendants’ role as licensing,
18 selling support services and offering technical support).)¹¹ Therefore, Defendants are derivatively
19 immune. *Butters*, 255 F.3d at 466.¹²

20
21 ¹⁰ Other courts have reached the same conclusion. *E.g.*, *Ivey v. Lynch*, 2018 WL 3764264, at *6-
22 *7 (M.D.N.C. Aug. 8, 2018) (following *Butters* to find private agent of foreign official immune);
23 *Moriah v. Bank of China Ltd.*, 107 F. Supp. 3d 272, 277 (S.D.N.Y. 2015) (holding that foreign
24 sovereign immunity “extends beyond current and former government officials to individuals acting
25 as an agent for the government”); *Alicog v. Kingdom of Saudi Arabia*, 860 F. Supp. 379, 384 (S.D.
26 Tex. 1994), *aff’d*, 79 F.3d 1145 (5th Cir. 1996) (affirming district court holding that agents enjoy
27 derivative immunity when following commands of foreign sovereign employer).

28 ¹¹ For that reason, the exception to derivative immunity for agents who do not follow a
government’s instructions, *Campbell-Ewald*, 136 S. Ct. at 672; *Cabalce v. Thomas E. Blanchard
& Assocs., Inc.*, 797 F.3d 720, 732 (9th Cir. 2015), does not apply.

¹² In addition, Plaintiffs’ claims would eventually have to be dismissed under the act of state
doctrine, which bars lawsuits that “question the legality of the sovereign acts of foreign states.”

1 **III. THE COURT SHOULD DISMISS THE COMPLAINT BECAUSE IT LACKS**
2 **PERSONAL JURISDICTION OVER DEFENDANTS**

3 This Court may exercise personal jurisdiction over Defendants only if they would be
4 subject to personal jurisdiction in California under both California’s long-arm statute and federal
5 due process. *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800–01 (9th Cir. 2004).
6 California’s long-arm statute “is coextensive with federal due process requirements,” so “the
7 jurisdictional analyses under state law and federal due process are the same.” *Id.* As a matter of
8 federal due process, jurisdiction exists only if Defendants’ alleged contacts with California support
9 either general or specific personal jurisdiction, *id.* at 801–02, or if Defendants consented to
10 personal jurisdiction in California. Plaintiffs have the burden to prove that personal jurisdiction
11 exists. *Id.* at 800. Plaintiffs cannot carry that burden here because Defendants did not consent to
12 jurisdiction, and Plaintiffs do not plead sufficient contacts between Defendants and California.
13 This Court therefore should dismiss for lack of personal jurisdiction under Rule 12(b)(2).

14 **A. Defendants Did Not Consent to Personal Jurisdiction in California**

15 Plaintiffs wrongly contend that Defendants consented to personal jurisdiction by accepting
16 the WhatsApp TOS. (Compl. ¶ 12.) At the time Plaintiffs allege Defendants joined WhatsApp,
17 however, the TOS did not require users to consent to personal jurisdiction in California in lawsuits
18 filed by WhatsApp. The TOS provided only that users must consent to jurisdiction in California if
19 a user sues WhatsApp. Between August 2016 and January 2020, the TOS’s “Forum and Venue”
20 provision provided:

21 [Y]ou agree that *you will resolve any Claim you have with us ... exclusively in the*
22 *United States District Court for the Northern District of California or a state court*
23 *located in San Mateo County in California, and you agree to submit to the personal*
24 *jurisdiction of such courts for the purpose of litigating all such Disputes.*

25 (Declaration of Joseph N. Akrotirianakis (“Akro. Decl”) Exh. 6 at 8 (emphasis added).) The

26 _____
27 *IAM v. OPEC*, 649 F.2d 1354, 1359 (9th Cir. 1981). The alleged actions challenged by Plaintiffs
28 were conducted by sovereign governments acting under their own law. (Hulio Decl. ¶ 14.)
Although the Court may not consider declarations or other extrinsic evidence on a motion to
dismiss based on the act of state doctrine, *Sea Breeze Salt, Inc. v. Mitsubishi Corp.*, 2016 WL
8648638, at *2 (C.D. Cal. Aug. 18, 2016), the doctrine will later pose an insurmountable bar for
Plaintiffs, *see Royal Wulff Ventures LLC v. Primero Mining Corp.*, 938 F.3d 1085, 1092-95 (9th
Cir. 2019).

1 provision unambiguously applies only to “any Claim *you* have with *us*”—meaning claims by a
2 user *against* WhatsApp. It does not apply to claims by WhatsApp against its users.¹³

3 **B. The Court Lacks General Jurisdiction Over Defendants**

4 General personal jurisdiction, which allows “a defendant to be haled into court in the forum
5 state to answer for any of its activities anywhere in the world,” *Schwarzenegger*, 374 F.3d at 801,
6 exists only when the defendant’s contacts with the forum state “are so constant and pervasive as to
7 render it essentially at home” there, *Daimler AG v. Bauman*, 571 U.S. 117, 122 (2014) (cleaned up).
8 The “‘paradigm’ fora for general jurisdiction are a corporation’s place of incorporation and
9 principal place of business. Only in an ‘exceptional case’ will general jurisdiction be available
10 anywhere else.” *Martinez v. Aero Caribbean*, 764 F.3d 1062, 1070 (9th Cir. 2014) (citations
11 omitted).

12 Defendants are not subject to general jurisdiction because Defendants are incorporated and
13 have their principal places of business in Israel. (Compl. ¶¶ 5–6; Hulo Decl. ¶ 4.) And this is not
14 the kind of “exceptional case” in which Defendants could be subject to general jurisdiction outside
15 of Israel.¹⁴ Defendants have no offices or employees in California and do no business of any kind
16 there. (Hulo Decl. ¶ 4); see *Martinez*, 764 F.3d at 1070 (finding no general jurisdiction over
17 corporation with “no offices, staff, or other physical presence in California” despite corporation
18 doing some business in California). Plaintiffs do not and could not allege otherwise. Defendants
19 are not “at home” in California.

20
21 ¹³ Even if the TOS’s forum-selection clause were ambiguous, any ambiguity in a consent-to-
22 jurisdiction clause must be “construed against the drafter.” *Pam Int’l, Inc. v. James*, 2006 WL
23 8455280, at *4 (S.D. Cal. Aug. 3, 2006). “Unless the document signed by the defendant clearly
24 informs him that his signature subjects him to the jurisdiction of California courts, the courts will
25 not infer that he consented to jurisdiction.” *Id.* (quoting *Hunt v. Super. Ct.*, 81 Cal. App. 4th 901,
26 908 n.5 (2000)) (cleaned up). WhatsApp drafted its TOS, so any ambiguities must be resolved in
27 Defendants’ favor. So construed, the TOS does not clearly provide that users consent to personal
28 jurisdiction in California for claims brought by WhatsApp.

26 ¹⁴ The only case the Supreme Court has described as sufficiently “exceptional” is *Perkins v.*
27 *Benguet Consolidated Mining Co.*, 342 U.S. 437 (1952). *Daimler*, 571 U.S. at 139 n.19. The
28 defendant in *Perkins* was a Philippines company that transferred its principal place of business to
Ohio during World War II. *Id.* at 129-30.

1 **C. The Court Lacks Specific Jurisdiction Over Defendants**

2 To establish specific jurisdiction, “the defendant must either ‘purposefully direct his
3 activities’ toward the forum or ‘purposefully avail[] himself of the privileges of conducting
4 activities in the forum.’” *Axiom Foods, Inc. v. Acerchem Int’l, Inc.*, 874 F.3d 1064, 1068 (9th Cir.
5 2017). The “purposeful direction analysis” applies in tort cases, while the “purposeful availment
6 analysis” applies in contract cases. *Schwarzenegger*, 374 F.3d at 802. Even if the defendant has
7 sufficient contacts with the forum state, specific jurisdiction does not exist unless the plaintiff’s
8 claim “arises out of or relates to the defendant’s forum-related activities.” *Id.* And in all events, a
9 court cannot exercise specific jurisdiction if “the exercise of jurisdiction would not be reasonable.”
10 *Id.* (internal quotation marks omitted).

11 Plaintiffs assert claims that sound in both tort and contract, but they cannot establish
12 specific jurisdiction under either the “purposeful direction” or “purposeful availment” tests.
13 Plaintiffs do not plead any case-related actions by Defendants within or targeted toward California.
14 Even if they had, exercising jurisdiction over Defendants would not be reasonable.

15 **1. Plaintiffs Do Not Allege That Defendants Purposefully Directed Their
16 Alleged Activities Toward California**

17 To satisfy the purposeful direction test, also known as the “effects” test, Plaintiffs must
18 show that Defendants “(1) committed an intentional act, (2) expressly aimed at the forum state, (3)
19 causing harm that [they] kn[ew] [wa]s likely to be suffered in the forum state.” *Axiom Foods*, 874
20 F.3d at 1069. This analysis focuses on “the defendant’s contacts with the forum State itself, not
21 the defendant’s contacts with persons who reside there.” *Walden v. Fiore*, 571 U.S. 277, 285
22 (2014). As a result, “a defendant’s relationship with a plaintiff or third party, standing alone, is an
23 insufficient basis for jurisdiction.” *Id.* at 286. “Due process requires that a defendant be haled into
24 court in a forum State based on his own affiliation with the State, not based on the ‘random,
25 fortuitous, or attenuated’ contacts he makes by interacting with other persons affiliated with the
26 State.” *Id.* In this case, there is no claim that any relevant conduct occurred in California, which is
27 convenient for Plaintiffs only because it is their home base.

28 Plaintiffs allege that Defendants “targeted their actions at . . . [California] residents,
WhatsApp and Facebook” (Compl. ¶ 11), but “targeting” a forum resident alone is not sufficient

1 to show purposeful direction. *Axiom Foods*, 874 F.3d at 1069–70. So even if Defendants targeted
2 Plaintiffs, and even if Defendants knew Plaintiffs are California residents, that would not show
3 that Defendants targeted *California*. *Id.*; *Walden*, 571 U.S. at 288-89.

4 Plaintiffs also claim that Defendants “targeted their actions at California” (Compl. ¶ 11),
5 but none of their factual allegations support that conclusion. As an initial matter, none of the
6 actions Plaintiffs’ challenge was committed by Defendants. Those alleged actions were committed
7 (if at all) solely by sovereign governments using a technological tool licensed from Defendants.
8 (Hulio Decl. ¶ 14).¹⁵ Defendants’ only involvement would have been licensing NSO’s technology
9 to those governments and helping to install it for their use. (Hulio Decl. ¶ 14). All of that conduct
10 would have occurred in foreign countries.

11 Even if the Court assumes the truth of Plaintiffs’ allegations (which it is not required to do,
12 *Stewart*, 81 F. Supp. 3d at 951), Plaintiffs do not allege that any of Defendants’ relevant conduct
13 occurred in or was targeted at California.

14 Plaintiffs allege that Defendants’ WhatsApp “accounts were created using telephone
15 numbers registered in different count[r]ies, including Cyprus, Israel, Brazil, Indonesia, and the
16 Netherlands.” (Compl. ¶ 33.) Plaintiffs also allege that Defendants “leased servers and internet
17 hosting services in different countries, including the United States” (*id.* ¶ 34), but they do not allege
18 that any of those servers were in California. In any event, courts have uniformly “rejected the
19 notion that the mere location of a server may give rise to personal jurisdiction.” *Rosen v. Terapeak,*
20 *Inc.*, 2015 WL 12724071, at *9 (C.D. Cal. Apr. 28, 2015) (citing cases); *accord Hungerstation*
21 *LLC v. Fast Choice LLC*, 2020 WL 137160, at *5 (N.D. Cal. Jan. 13, 2020). Nothing in the
22 Complaint suggests that Defendants knew or cared where the alleged servers were located, so the
23 presence of a server in California would be entirely “fortuitous.” *Rosen*, 2015 WL 12724071, at *9.

24 The same is true of the alleged use of Plaintiffs’ servers to distribute Pegasus code.
25 Plaintiffs do not allege that any code was routed through Plaintiffs’ California servers. (*Id.* ¶¶ 1,
26

27 ¹⁵ The Court can consider extrinsic evidence on Defendants’ motion to dismiss for lack of personal
28 jurisdiction. *Stewart v. Screen Gems–EMI Music, Inc.*, 81 F. Supp. 3d 938, 951 (N.D. Cal. 2015).

1 32, 36–42.) Plaintiffs do not even allege that they *have* California servers. But even if Plaintiffs do
2 have California servers that Pegasus code happened to pass through, that still would not show that
3 Defendants purposefully targeted California. A “server’s location” cannot establish personal
4 jurisdiction “where there is no allegation, argument, or evidence that the defendants played any
5 role in selecting the server’s location—or that its location was selected with the purpose or intent
6 of facilitating the defendants’ business in the forum.” *GreatFence.com, Inc. v. Bailey*, 726 F.
7 App’x 260, 261 (5th Cir. 2018).¹⁶ That is the case here, since Plaintiffs decide where to put their
8 servers and which servers WhatsApp messages pass through. Plaintiffs do not allege that
9 Defendants had any knowledge of or control over those decisions. (*See* Hulo Decl. ¶ 16.) Such
10 “‘unilateral activity’ of a plaintiff” cannot support specific jurisdiction. *Walden*, 571 U.S. at 286.

11 Furthermore, “the level of contact created by the connection between an out-of-state
12 defendant and a web server located within a forum” is “de minimis.” *Carefirst of Md., Inc. v.*
13 *Carefirst Pregnancy Ctrs., Inc.*, 334 F.3d 390, 402 (4th Cir. 2003). The transfer of information
14 from one phone to another, via a server, is “analogous to forwarding calls to a desired phone
15 number through a switchboard.” *Amberson Holdings LLC v. Westside Story Newspaper*, 110 F.
16 Supp. 2d 332, 336 (D.N.J. 2000). And the Ninth Circuit has held that “use of the mails, telephone,
17 or other international communications simply do not qualify as purposeful activity” sufficient to
18 create specific jurisdiction. *Joseph Saveri Law Firm, Inc. v. Criden*, 696 F. App’x 189, 192 (9th
19 Cir. 2017) (quoting *Peterson v. Kennedy*, 771 F.2d 1244, 1262 (9th Cir. 1985)). So, even if some
20 of Defendants’ WhatsApp messages were transferred through servers in California, and even if
21 Defendants knew that, such contact with California would still be too insignificant to establish
22 purposeful direction. *Carefirst*, 334 F.3d at 402; *Amberson Holdings*, 110 F. Supp. 2d at 336.

23 Finally, the Defendants’ alleged intrusion upon WhatsApp users’ devices does not show
24

25 ¹⁶ Cases have upheld specific jurisdiction based on a defendant’s use of a plaintiff’s servers *when*
26 *the defendant controlled the location of the server*. *See DEX Sys., Inc. v. Deutsche Post AG*, 727
27 F. App’x 276, 278 (9th Cir. 2018) (approving specific jurisdiction because defendant’s “software
28 was located on California servers pursuant to an agreement reached by the parties”). If a defendant
cannot control which server it uses, the server’s location is irrelevant to specific jurisdiction.
GreatFence.com, 726 F. App’x at 261.

1 that Defendants targeted California. (Compl. ¶¶ 37–42.) Plaintiffs allege that the targeted users
2 were located in foreign countries, not in California. (*Id.* ¶ 43.) Indeed, NSO’s technology *cannot*
3 be used to monitor U.S. devices or any device within the geographic bounds of the United States.
4 (Compl. Exh. 11 at Exhibit D [Dkt. No. 1-1 at p. 111]; Hulo Decl. ¶ 13.)

5 **2. Plaintiffs Do Not Allege That Defendants Purposefully Availed**
6 **Themselves of the Privilege of Conducting Activities in California**

7 Plaintiffs cannot satisfy the purposeful availment test because they cannot show that
8 Defendants took any “actions in the forum, such as executing or performing a contract there.”
9 *Schwarzenegger*, 374 F.3d at 802. As already noted, Plaintiffs do not allege that Defendants have
10 any offices or employees in California or conduct any business in this state. None of Defendants’
11 alleged conduct took place in California. *Supra* Part III.B.1. And while Plaintiffs allege that NSO
12 once “obtained financing from California” (Compl. ¶ 11), that cannot support specific jurisdiction
13 because Plaintiffs’ claims do not “arise[] out of or relate[] to” this alleged financing.
14 *Schwarzenegger*, 374 F.3d at 802.

15 Nor did Defendants “execut[e] or perform[] a contract” in California. *Id.* Plaintiffs allege
16 that Defendants agreed to WhatsApp’s TOS (Compl. ¶ 30), but “a contract alone does not
17 automatically establish minimum contacts in the plaintiff’s home forum.” *Boschetto v. Hansing*,
18 539 F.3d 1011, 1017 (9th Cir. 2008) (*citing Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 478
19 (1985)). Instead, Plaintiffs must allege that Defendants “performed some type of affirmative
20 conduct which allow[ed] or promote[d] the transaction of business within the forum state.” *Picot*
21 *v. Weston*, 780 F.3d 1206, 1212 (9th Cir. 2015) (internal quotation marks omitted). Plaintiffs have
22 not done so. They do not allege that creating a WhatsApp account “created any ongoing obligations
23 with [Plaintiffs] in California” or “require[d] the Defendants to engage in any substantial business
24 in California.” *Boschetto*, 539 F.3d at 1017. Without such allegations, Plaintiffs cannot show
25 purposeful availment.

26 **3. Exercising Jurisdiction Over Defendants in California Would Be**
27 **Unreasonable**

28 Even if Defendants’ alleged contacts with California were sufficient to support specific
jurisdiction, exercising jurisdiction over Defendants in California would be unreasonable. The

1 Ninth Circuit analyzes seven factors to assess reasonableness: “(1) the extent of a defendant’s
2 purposeful interjection into the forum state’s affairs; (2) the burden on the defendant of defending
3 in the forum; (3) the extent of conflict with the sovereignty of the defendant’s home state; (4) the
4 forum state’s interest in adjudicating the dispute; (5) the most efficient judicial resolution of the
5 controversy; (6) the importance of the forum to the plaintiff’s interests in convenient and effective
6 relief; and (7) the existence of an alternative forum.” *Glencore Grain Rotterdam B.V. v. Shivnath*
7 *Rai Harnarain Co.*, 284 F.3d 1114, 1125 (9th Cir. 2002). Here, “[e]ven a cursory glance at the
8 factors reveals the unreasonableness of exercising jurisdiction” over Defendants. *Id.*

9 First, for the reasons given above, Defendants’ “purposeful interjection into [California’s]
10 affairs” is negligible at best. *Id.*

11 Second, the burden on Defendants to litigate in California would be “great, given that it is
12 incorporated in [Israel], owns no property in the forum, and has no employees or persons
13 authorized to act on its behalf there.” *Id.* at 1125-26 (Hulio Decl. ¶ 4); and “its potential witnesses
14 and evidence” are “half a world away.” *Id.* at 1126 (Hulio Decl. ¶ 4).

15 Third, any exercise of personal jurisdiction over an Israeli corporation that conducts no
16 operations in California conflicts with Israel’s sovereignty. The Ninth Circuit has held that when
17 “the defendant is from a foreign nation rather than another state, the sovereignty barrier is high
18 and undermines the reasonableness of personal jurisdiction.” *Id.* at 1126 (quoting *Amoco Egypt*
19 *Oil Co. v. Leonis Navigation Co.*, 1 F.3d 848, 852 (9th Cir. 1993)). The conflict is even greater
20 here, where the conduct alleged to have been committed by Defendants was conducted by
21 governments to advance their sovereign interests. (Hulio Decl. ¶ 14.)

22 Fourth, while California may have a form of interest in hearing claims brought by
23 companies that operate in this state, this case’s only connection with California is that Plaintiffs
24 have their principal places of business there. Defendants did not target California as a state in any
25 way, and any effect Defendants’ alleged conduct had on California-based servers was incidental.
26 None of the WhatsApp users Defendants allegedly targeted are California residents. In contrast,
27 Israel has a strong interest in this dispute because Defendants are Israeli corporations regulated
28 under Israeli law. (Hulio Decl. ¶¶ 4-5.)

1 Fifth, the most efficient place to resolve a dispute about NSO’s conduct would be in Israel,
2 where Defendants are based and all of their witnesses and evidence located. (Hulio Decl. ¶¶ 4, 19.)

3 Sixth, Plaintiffs do not require a home-court forum to achieve effective relief. While
4 Plaintiffs may be able to litigate more easily in California, the convenience of plaintiffs is an
5 “insignificant” factor in deciding whether to find jurisdiction. *Core-Vent Corp. v. Nobel Indust.*
6 *AB*, 11 F.3d 1482, 1490 (9th Cir. 1993). Although Plaintiffs’ businesses are based in California,
7 they are massive international corporations with offices in other countries, including Israel. *See*
8 *Facebook, Join Us in Facebook Israel as We Bring the World Closer Together*,
9 <https://bit.ly/3dkyhoC>. Defendants, in contrast, are Israeli corporations with no presence in any
10 country other than Israel. (Hulio Decl. ¶ 4.)

11 Seventh, Israel is an available alternative forum. Plaintiffs “ha[ve] the burden of proving
12 the unavailability of an alternative forum,” *Leonis*, 1 F.3d at 853, and they have not tried to satisfy
13 that burden. “Courts routinely hold that Israel is a proper forum and dismiss cases on the grounds
14 that it would be more appropriate to hear a case in Israel.” *Israel Discount Bank Ltd. v. Schapp*,
15 505 F. Supp. 2d 651, 659 (C.D. Cal. 2007) (citing cases); *Interface Partners Int’l Ltd. v. Hananel*,
16 575 F.3d 97, 103 (1st Cir. 2009) (same, finding Israel provided adequate remedy for breach of
17 contract). Moreover, Plaintiffs are presently litigating a case against NSO employees in Israel,
18 (Dkt. No. 18 at 9) and can likewise pursue their claims in this case in Israel. *See Leonis*, 1 F.3d at
19 853 (finding alternative forum adequate where plaintiffs were defending related case in forum).

20 The seven reasonableness factors, therefore, overwhelmingly favor a finding that
21 exercising jurisdiction over Defendants would be unreasonable.

22 **IV. THE COURT SHOULD DISMISS THE CASE UNDER RULE 12(B)(7) FOR**
23 **FAILURE TO JOIN A NECESSARY PARTY**

24 The Court should dismiss the Complaint because Plaintiffs did not join Defendants’
25 foreign-sovereign customers under Rule 19. A Court must dismiss an action for failure to join a
26 “required party” when the party cannot be joined and the action, “in equity and good conscience,
27 . . . should be dismissed.” Fed. R. Civ. P. 19; *see* Fed. R. Civ. P. 12(b)(7). Defendants’
28 customers are required parties, they cannot be joined, and the action should not proceed without them.

1 Defendants' customers are required parties because, in their absence, "the court cannot
2 accord complete relief among existing parties." Fed. R. Civ. P. 19(1)(A). Plaintiffs seek an
3 injunction against Defendants "and all other persons acting in concert with or conspiracy with any
4 of them" from accessing WhatsApp or Facebook, impairing their systems, or violating their TOS.
5 (Compl. Request for Relief ¶ 2.) But Defendants' customers, not Defendants, are the entities that
6 accessed Plaintiffs' services.¹⁷ If the customers are not parties, this Court cannot issue an
7 injunction that binds them, and Plaintiffs cannot receive the injunctive relief they seek. *See*
8 *Dawavendewa v. Salt River Project Agric. Improvement & Power Dist.*, 276 F.3d 1150, 1155-56
9 (9th Cir. 2002) (holding parties are required if injunction will be ineffective without them); *Otani*
10 *Props., L.P. v. Centerline Tool, Inc.*, 2016 WL 10999268, at *1 (C.D. Cal. Mar. 28, 2016) (same);
11 *Friends of Amador Cty. v. Salazar*, 2011 WL 4709883, at *2 (E.D. Cal. Oct. 4, 2011) (same).

12 Defendants' customers cannot be joined because they are foreign sovereigns immune from
13 suit. *Rep. of the Philippines v. Pimentel*, 553 U.S. 851, 865 (2008). That immunity also requires
14 dismissal. Under *Pimentel*, "[a] case may not proceed when a required-entity sovereign is not
15 amenable to suit." 553 U.S. at 867. That is the case here. Defendants' customers use NSO's
16 technology to advance their own sovereign interests. They are entitled to have the legality of their
17 actions determined in their own courts. *Pimentel*, 553 U.S. at 866. Litigating Plaintiffs' claims in
18 the United States would thus prejudice Defendants' customers by ignoring "their sovereign status"
19 and "bypass[ing] [their] courts without right or just cause." *Id.* at 866-67; *see also* Fed. R. Civ. P.
20 19(b)(1) (suggesting dismissal when judgment "might prejudice" the absent "person or the existing
21 parties").¹⁸

22
23
24 ¹⁷ The Court may consider extrinsic evidence under Rule 12(b)(7). *Estate of Burkhart v. United States*, 2008 WL 4067429, at *2 (N.D. Cal. Aug. 26, 2008).

25 ¹⁸ Proceeding without Defendants' customers as parties would also prejudice Defendants.
26 Defendants do not know which if any of their customers used NSO's technology to monitor the
27 alleged 1,400 WhatsApp users mentioned in the Complaint (Hulio Decl. ¶ 15), and any discovery
28 into that question would be barred by the customers' sovereign immunity, *see Moriah*, 107 F.
Supp. 3d at 277-78. Without that discovery, Defendants will not be able to defend themselves at
trial by proving they did not monitor the allegedly targeted WhatsApp users.

1 **V. THE COURT SHOULD DISMISS PLAINTIFFS' CFAA AND TRESPASS TO**
2 **CHATTELS CLAIMS FOR FAILURE TO STATE A CLAIM UNDER RULE**
3 **12(B)(6)**

4 Defendants did not operate NSO technology to monitor any WhatsApp users. (Hulio Decl.
5 ¶ 14). Plaintiffs' allegations to that effect are contradicted by other information in their own
6 Complaint. But even if the Court assumes that NSO did use the technology in the manner Plaintiffs
7 allege, Plaintiffs do not state a claim for relief under the CFAA or for trespass to chattels. So even
8 if the Court does not dismiss the entire Complaint on jurisdictional grounds, it should still dismiss
9 those claims under Rule 12(b)(6).

10 **A. Plaintiffs Cannot State a CFAA Claim**

11 Plaintiffs assert claims under three provisions of the CFAA. (Compl. ¶¶ 53–55.) First, they
12 sue under 18 U.S.C. § 1030(a)(2)(C), which applies to defendants who “intentionally access[] a
13 computer without authorization or exceed[] authorized access, and thereby obtain[] . . .
14 information from any protected computer.” (*Id.* ¶ 53.)¹⁹ Second, they sue under 18 U.S.C.
15 § 1030(a)(4), which applies to defendants who “knowingly and with intent to defraud, access[] a
16 protected computer without authorization, or exceed[] authorized access, and by means of such
17 conduct further[] the intended fraud and obtain[] anything of value.” (*Id.* ¶ 54.) Third, they sue
18 under 18 U.S.C. § 1030(b), which prohibits conspiracies and attempts. (*Id.* ¶ 55.)

19 Plaintiffs cannot state a CFAA claim under any of these provisions. They cannot state any
20 claim based on Defendants' alleged access to WhatsApp's servers because Defendants had
21 authorization to access those servers. Plaintiffs also cannot state a claim based on Defendants'
22 alleged access to WhatsApp users' phones because that did not cause *Plaintiffs'* alleged injury.
23 Because Plaintiffs cannot plead a violation, they cannot plead a conspiracy or attempt to violate
24 the CFAA.

25 **1. Plaintiffs Cannot State a Claim Based on Defendants' Alleged Access**
26 **to Plaintiffs' Servers Because They Cannot Plead That Defendants**
27 **Accessed the Servers Without Authorization**

28 Plaintiffs claim that that Defendants violated the CFAA by accessing WhatsApp's servers

¹⁹ For the purposes of this motion only, Defendants assume without conceding that WhatsApp's servers and its users' devices are “protected computers” under the CFAA. (Compl. ¶¶ 51–52.)

1 “without authorization,” (Compl. ¶¶ 53–54), but WhatsApp’s TOS explicitly authorized
2 Defendants to access those servers. Because Defendants had authority to access the servers, they
3 did not violate the CFAA by allegedly using the servers in a way forbidden by the TOS.

4 The Ninth Circuit has held that “a person uses a computer ‘without authorization’ under
5 §§ 1030(a)(2) and (4) when the person has not received permission to use the computer *for any*
6 *purpose.*” *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009) (emphasis added).
7 As long as a defendant “is authorized to use a computer for certain purposes,” its access to the
8 computer cannot be “without authorization”—even if the defendant violates limits the computer’s
9 owners placed on the defendant’s access. *Id.* at 1133.

10 That rule forecloses Plaintiffs’ claims. The TOS expressly grant users a “license to use
11 [WhatsApp’s] Services.” (Akro. Decl. Exh. 6 at 6.) To use WhatsApp’s services, users must send
12 information through WhatsApp’s servers. (Compl. ¶ 36). Defendants were, therefore, “authorized
13 to use [WhatsApp’s servers] for certain purposes,” and their alleged access to those servers was
14 not “without authorization” under the CFAA.” *Brekka*, 581 F.3d at 1133-35.

15 Plaintiffs do not allege that Defendants lacked authorization to use WhatsApp’s servers.
16 Instead, they allege that Defendants “were not authorized to use Plaintiffs servers *in th[e] manner*”
17 they used them, *i.e.*, in violation of the TOS. (Compl. ¶ 36 (emphasis added); *see id.* ¶¶ 21–22
18 (quoting allegedly violated terms).) But *Brekka* is clear that the violation of a company’s terms of
19 service does not render access to a computer “unauthorized.” When a company “authorizes [a
20 person] to use a company computer subject to certain limitations, the [person] remains authorized
21 to use the computer even if the [person] violates those limitations.” *Brekka*, 581 F.3d at 1133. So
22 even if Defendants violated the TOS’s limits on their access to WhatsApp’s servers, they still did
23 not access the servers “without authorization” under the CFAA.

24 Nor can Plaintiffs argue that Defendants “exceed[ed] authorized access” to WhatsApp’s
25 servers. 18 U.S.C. § 1030(a)(2)(C), (a)(4). The Complaint does not allege that Defendants
26 exceeded authorized access. (Compl. ¶¶ 53–54 (alleging only that Defendants accessed computers
27 “without authorization”).) Even if it did, the Ninth Circuit has held that the CFAA’s prohibition
28 on “exceed[ing] authorized access” does not apply to “violations of corporate computer use

1 restrictions.” *United States v. Nosal*, 676 F.3d 854, 862–63 (9th Cir. 2012). Such violations are
2 “governed by tort and contract law,” not the CFAA. *Id.* at 860; *see Facebook, Inc. v. Power*
3 *Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016) (“[A] violation of the terms of use of a
4 website—without more—cannot establish liability under the CFAA.”).

5 **2. Plaintiffs Cannot State a Claim Based on Defendants’ Alleged Access**
6 **to WhatsApp Users’ Phones Because It Did Not Harm Plaintiffs**

7 Plaintiffs have no basis under the CFAA to challenge anyone’s alleged access to foreign
8 cell phones. The CFAA limits its private right of action to “[a]ny person who suffers damage or
9 loss by reason of a violation,” 18 U.S.C. § 1030(g), and defines loss as “any reasonable cost to any
10 victim,” *id.* § 1030(e)(11). This “is a narrow conception of ‘loss,’” and a plaintiff’s “theory of loss
11 must conform to the limited parameters of the CFAA’s definition.” *Andrews v. Sirius XM Radio*
12 *Inc.*, 932 F.3d 1253, 1262–63 (9th Cir. 2019). In particular, the loss must be “caused by computer
13 intrusions, not general injuries unrelated to the hacking itself.” *Id.* at 1263.

14 The losses alleged by Plaintiffs—“expenditure of resources to investigate and remediate
15 Defendants’ conduct, damage to [their] reputation, and damage to the relationships and goodwill
16 between [them] and their users and potential users” (Compl. ¶ 73)—were not caused by anyone’s
17 access to WhatsApp users’ devices. If WhatsApp users’ devices had been accessed through some
18 other messaging service, like Signal or Apple iMessage, the effect on the devices would have been
19 identical without any injury to Plaintiffs. Contrast that with a case in which a plaintiff *would* be
20 injured by a defendant’s access to a third party’s device, such as if the plaintiff “ha[d] rights to data
21 stored on [the device].” *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2004). That is not what
22 Plaintiffs allege happened here.

23 According to Plaintiffs’ theory of the case, they incurred losses because Defendants
24 allegedly exploited a “vulnerability” in WhatsApp’s product. (*Id.* ¶ 44.) That vulnerability—not
25 anything to do with the devices of WhatsApp’s users—is what Plaintiffs had to “investigate and
26 remediate.” (*Id.* ¶ 73.) And the disclosure of that vulnerability—not merely access to user’s
27 devices—was responsible for any loss to Plaintiffs. Plaintiffs’ alleged losses, therefore, were not
28 “caused by” Defendants’ alleged intrusions into WhatsApp’s users’ devices. *Andrews*, 932 F.3d at

1 1263. Plaintiffs were not “victim[s]” of that alleged access, and they cannot sue Defendants for it.
2 18 U.S.C. § 1030(e)(11), (g).

3 **3. Plaintiffs Cannot State a Claim for Conspiracy Because They Do Not**
4 **Plead Any Conduct That Would Violate Section 1030(a)**

5 Because Plaintiffs do not adequately plead violations of sections 1030(a)(2)(C) or
6 1030(a)(4), their claim that Defendants “conspir[ed] and attempt[ed]” to violate those sections
7 necessarily fails. (Compl. ¶ 55.) Section 1030(b) applies only when there is an underlying “offense
8 under subsection (a).” 18 U.S.C. § 1030(b). Plaintiffs do not plead any such “offense under
9 subsection (a),” so their claim under section 1030(b) should be dismissed. *See Walenco, Inc. v.*
10 *Corbell*, 126 F. Supp. 3d 1154, 1176 (E.D. Cal. 2015) (granting summary judgment on section
11 1030(b) claim because plaintiff did not introduce evidence that defendant “exceeded or attempted
12 to exceed his authorized access” under section 1030(a)).

13 **B. Plaintiffs Cannot State a Claim for Trespass to Chattels Because the Alleged**
14 **Actions Did Not Damage WhatsApp’s Servers**

15 Plaintiffs’ claim that Defendants committed trespass to chattels against WhatsApp’s servers
16 should be dismissed because Plaintiffs do not plead an essential element: that Defendants’ conduct
17 damaged Plaintiffs’ servers. *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1347 (2003).

18 In *Hamidi*, the California Supreme Court held that a defendant’s use of a company’s email
19 system to send mass emails did not “damage” the company’s computer system or “interfere[] with
20 its ordinary and intended operation.” *Id.* at 1353. To state a claim for trespass to chattels based on
21 an electronic communication, the Court held, the plaintiff must show the communication
22 “damage[d] the recipient computer system” or “interfere[d] with the intended functioning of the
23 system, as by significantly reducing its available memory and processing power” or by
24 “prevent[ing]” the owner “from using its computers for any measurable length of time.” *Id.* at
25 1347, 1353, 1356.

26 Here, Plaintiffs do not allege that Defendants’ access to WhatsApp’s servers damaged the
27 servers or interfered with their operation. Their alleged “expenditure of resources to investigate
28 and remediate Defendants’ conduct” (Compl. ¶ 78) is not damage to their *servers*. Neither is the
alleged harm to their reputation, relationships, or goodwill. (*Id.*); *see Hamidi*, 30 Cal. 4th at 1357-

1 58 (rejecting company’s argument that defendant’s conduct harmed its goodwill).

2 Plaintiffs allege, in passing, that Defendants’ alleged conduct “burdened Plaintiffs’
3 computer network” (Compl. ¶ 46), but such a “conclusory statement[,]” unsupported by any
4 specific factual allegations, should be disregarded. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).
5 Plaintiffs do not quantify the alleged “burden” or allege facts showing, as *Hamidi* requires, that
6 they were “dispossessed” of WhatsApp’s servers or that Defendants “prevent[ed]” them from
7 using the servers “for any measurable length of time” or “significantly reduce[d]” the servers’
8 “available memory and processing power.” 30 Cal. 4th at 1353, 1356; see *Mount v. PulsePoint,*
9 *Inc.*, 2016 WL 5080131, at *9 (S.D.N.Y. Aug. 17, 2016) (dismissing trespass to chattels claim in
10 absence of “particularized allegations of diminished device performance” because “plaintiffs must
11 do more than simply claim an unspecified demand on their devices’ resources”); *In re iPhone App.*
12 *Litig.*, 844 F. Supp. 2d 1040, 1069 (N.D. Cal. 2012) (dismissing trespass to chattels claim because
13 allegations that defendants “have taken up valuable bandwidth and storage space” on devices and
14 “shortened [their] battery life” did not “plausibly establish a significant reduction in service
15 constituting an interference with the intended functioning of the system”).

16 In any event, the allegation that Defendants’ conduct “burdened” WhatsApp’s servers
17 should be disregarded as implausible. See *Iqbal*, 556 U.S. at 679 (allowing courts to use “common
18 sense” to disregard implausible allegations). Plaintiffs allege WhatsApp’s servers support “1.5
19 billion people in 180 countries” (Compl. ¶ 17), and Defendants allegedly used them to send
20 “approximately 1,400” messages (*id.* ¶ 42). The idea that 1,400 messages could significantly
21 impair servers designed to support 1.5 billion users is fanciful. See *Hamidi*, 30 Cal. 4th at 1356
22 (rejecting idea that plaintiff sending “thousands of copies of the same message on six occasions”
23 could burden company’s computers because “that number is miniscule compared to the amounts
24 of mail sent by commercial operations”).

25 Plaintiffs thus do not allege any harm to or interference with WhatsApp servers. Their
26 trespass-to-chattels claim should be dismissed. See *Synopsis, Inc. v. Ubiquiti Networks, Inc.*, 313
27 F. Supp. 3d 1056, 1080 (N.D. Cal. 2018) (dismissing trespass to chattels counterclaim because
28 defendant did not allege plaintiffs’ access “impaired the intended functioning of [their] systems”);

1 *Hiossen, Inc. v. Kim*, 2016 WL 10987365, at *10 (C.D. Cal. Aug. 17, 2016) (dismissing trespass
2 to chattels claim because plaintiff did not allege that defendants' hacking of plaintiff's servers
3 "interfer[ed] with the intended functioning of the system").

4 **VI. CONCLUSION**

5 The Court should dismiss Plaintiffs' claims with prejudice.

6
7 Dated: April 2, 2020

KING & SPALDING LLP

8
9 By: /s/ Joseph N. Akrotirianakis

10 JOSEPH N. AKROTIRIANAKIS

AARON S. CRAIG

11 Attorneys for Defendants NSO GROUP

12 TECHNOLOGIES LIMITED and Q

13 CYBER TECHNOLOGIES LIMITED
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28