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

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

*Attorneys for Plaintiffs*
*WhatsApp LLC and Meta Platforms, Inc.*

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

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

## TABLE OF CONTENTS

PAGE

PRELIMINARY STATEMENT ....................1

LEGAL STANDARD ....................1

ARGUMENT ....................1

I. THE COURT HAS PERSONAL JURISDICTION OVER NSO ....................1

II. NSO IS LIABLE ON PLAINTIFFS' BREACH OF CONTRACT CLAIM ....................2

A. NSO Agreed to the Terms ....................2

B. NSO Breached the Contract ....................3

C. Plaintiffs Did Not "Waive" Any Known Rights ....................5

D. Plaintiffs Suffered Damages ....................5

III. NSO IS LIABLE ON PLAINTIFFS' CFAA CLAIMS ....................5

A. NSO Violated § 1030(a)(2) and § 1030(a)(4) of the CFAA ....................5

1. NSO Intentionally Accessed WhatsApp's Servers and the Target Devices ....................5

2. NSO Accessed WhatsApp Servers and the Official Client on Target Devices Without Authorization or Exceeded Any Purported Authorized Access ....................7

*a)* The Terms of Service Did Not Authorize NSO's Access ....................7

*b)* NSO Bypassed the Restrictions Built Into the Official Client ....................9

*c)* NSO Used WhatsApp After Plaintiffs Revoked NSO's Access ....................10

*d)* NSO Exceeded Any Purported Authorization ....................11

3. NSO Defrauded Plaintiffs and WhatsApp Users in Violation of § 1030(a)(4) ....................12

B. NSO Conspired with Its Clients to Use Its Technology in Violation of § 1030(b) ....................13

C. NSO Trafficked in Password-Like Information in Violation of § 1030(a)(6) ....................14

D. NSO Caused Plaintiffs a Loss of More than $5,000 ....................15

IV. NSO IS LIABLE ON PLAINTIFFS' CDAFA CLAIM ....................15

V. NSO PROVIDES NO EVIDENCE SUPPORTING AN UNCLEAN HANDS DEFENSE ....................15

CONCLUSION ....................15

## TABLE OF AUTHORITIES

### Cases

Page(s)

*Andrews v. Sirius XM Radio Inc.*,
932 F.3d 1253 (9th Cir. 2019) .......... 15

*In re Apple Inc. Device Performance Litig.*,
347 F. Supp. 3d 434 (N.D. Cal. 2018) .......... 14

*Artifex Software, Inc. v. Hancom, Inc.*,
2017 WL 4005508 (N.D. Cal. Sept. 12, 2017) .......... 5

*Auntie Anne's, Inc. v. Wang*,
2014 WL 11728722 (C.D. Cal. July 16, 2014) .......... 5

*Berman v. Freedom Fin. Network, LLC*,
30 F.4th 849 (9th Cir. 2022) .......... 3

*Cahill v. Golden Gate Bridge, Highway & Transp. Dist.*,
2016 WL 1070655 (N.D. Cal. Mar. 18, 2016) .......... 2

*Cannon v. Santos*,
2009 WL 10701940 (N.D. Ga. Aug. 6, 2009) .......... 3

*CBS, Inc. v. Merrick*,
716 F.2d 1292 (9th Cir. 1983) .......... 5

*Creative Computing v. Getloaded.com, L.L.C.*,
386 F.3d 930 (9th Cir. 2004) .......... 5, 15

*Facebook, Inc. v. Power Ventures, Inc.*,
844 F.3d 1058 (9th Cir. 2016) .......... 4, 9, 10, 11, 15

*Guangzhou Yuchen Trading Co. v. Dbest Prods. Inc.*,
2023 WL 2626373 (C.D. Cal. Feb. 24, 2023) .......... 9

*Hansen v. United States*,
7 F.3d 137 (9th Cir. 1993) .......... 9

*Ingram v. Pac. Gas & Elec. Co.*,
2014 WL 295829 (N.D. Cal. Jan. 27, 2014) ..........15

*Jackson v. Amazon.com, Inc.*,
65 F.4th 1093 (9th Cir. 2023) .......... 3

*Laatz v. Zazzle, Inc.*,
2024 WL 377970 (N.D. Cal. Jan. 9, 2024) .......... 3

*Mahoney v. DePuy Orthopaedics, Inc.*,
2007 WL 3341389 (E.D. Cal. Nov. 7, 2007) .......... 5

*Martinez v. Mcnabb*,
2004 WL 103541 (Cal. Ct. App. Jan. 23, 2004) .......... 5

*Marshall v. Hipcamp Inc.*,
2024 WL 2325197 (W.D. Wash. May 22, 2024) ........ 3

*Meta Platforms, Inc. v. BrandTotal Ltd.*,
605 F. Supp. 3d 1218 (N.D. Cal. 2022) ........ 5, 15

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

*Nguyen v. Barnes & Noble Inc.*,
763 F.3d 1171 (9th Cir. 2014) ........ 3

*Nissan Fire & Marine Ins. Co. v. Fritz Cos.*,
210 F.3d 1099 (9th Cir. 2000) ........ 1, 3

*Norse v. City of Santa Cruz*,
629 F.3d 966 (9th Cir. 2010) ........ 2

*Perez-Encinas v. Amerus Life Ins. Co.*,
468 F. Supp. 2d 1127 (N.D. Cal. 2006) ........ 4

*Persian Gulf Inc. v. BP W. Coast Prods. LLC*,
632 F. Supp. 3d 1108 (S.D. Cal. 2022) ........ 2

*Plumley v. S. Container, Inc.*,
2001 WL 1188469 (D. Me. Oct. 9, 2001), *aff'd*, 303 F.3d 364 (1st Cir. 2002) ........ 2

*Rainey v. Am. Forest & Paper Ass'n*,
26 F. Supp. 2d 82 (D.D.C. 1998) ........ 9

*Ryanair DAC v. Booking Holdings Inc.*,
636 F. Supp. 3d 490 (D. Del. 2022) ........ 6

*Ryanair DAC v. Booking Holdings Inc.*,
2024 WL 3732498 (D. Del. June 17, 2024) ........ 15

*S.F. Baykeeper v. W. Bay Sanitary Dist.*,
791 F. Supp. 2d 719 (N.D. Cal. 2011) ........ 2

*Sellers v. JustAnswer LLC*,
73 Cal. App. 5th 444 (2021) ........ 3

*Sylabs, Inc. v. Gregory Rose*,
2024 WL 4312719 (N.D. Cal. Sept. 26, 2024) ........ 15

*Theofel v. Farey-Jones*,
359 F.3d 1066 (9th Cir. 2004) ........ 8, 10

*Total Coverage, Inc. v. Cendant Settlement Servs. Grp., Inc.*,
252 F. App'x 123 (9th Cir. 2007) ........ 3

*United States v. Christensen*,
828 F.3d 763 (9th Cir. 2016) ........ 6

*United States v. Morris*,
928 F.2d 504 (2d Cir. 1991) ........ 14

*United States v. Nosal*,
676 F.3d 854 (9th Cir. 2012) ........ 6

*United States v. Nosal*,
844 F.3d 1024 (9th Cir. 2016) ........ 8, 11

*United States v. Phillips*,
477 F.3d 215 (5th Cir. 2007) ........ 12

*United States v. Saini*,
23 F.4th 1155 (9th Cir. 2022) ........ 12

*Van Buren v. United States*,
593 U.S. 374 (2021) ........ 7, 11, 14, 15

*Wages v. I.R.S.*,
915 F.2d 1230 (9th Cir. 1990) ........ 2

STATUTES & RULES

Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030........ *passim*

28 U.S.C. § 1605(a)(2), (5) ........ 14

Cal. Civ. Code § 1638 ........ 4

California Comprehensive Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502........ 14

Fed. R. Civ. P. 30(b)(6) ........ 2, 9

Fed. R. Civ. P. 56(e) ........2

There is no genuine dispute regarding NSO's liability under the CFAA and CDAFA, and for contractual breaches of WhatsApp's Terms. NSO admits that it designed, tested, sold, maintained, and supported the Pegasus spyware that carried out the attacks at issue. NSO admits the spyware operated as Plaintiffs alleged, using NSO's customized fake client application to send messages that neither a legitimate WhatsApp user nor the Official Client application could send. NSO admits that, in developing and deploying Pegasus, it created numerous WhatsApp accounts for itself and its customers, thereby accepting WhatsApp's Terms. NSO admits that, to develop and maintain its installation vectors, it decompiled WhatsApp code and reverse-engineered the Official Client, all in violation of those Terms. NSO admits that it engaged in similar attacks before and after those described in the complaint, including after this litigation was filed, and repeatedly circumvented WhatsApp's security measures. These facts are undisputed and dispositive. The Court has already ruled that they suffice to establish liability. NSO is liable as a matter of law.

In its opposition, NSO raises no genuine dispute regarding the facts that establish its liability. Instead, NSO asserts legal arguments unsupported by evidence and contrary to controlling law. Moreover, for the reasons presented in Plaintiffs' Motion for Sanctions, Dkt. No. 406, NSO should not be allowed to oppose summary judgment via self-serving declarations or a purported lack of evidence when it has withheld the underlying evidence in violation of the Court's orders.

## LEGAL STANDARD

Because Plaintiffs have carried their "burden of production" to show that there is no genuine dispute as to NSO's liability, summary judgment must be granted if NSO "fails to produce enough evidence to create a genuine issue of material fact." *Nissan Fire & Marine Ins. Co. v. Fritz Cos.*, 210 F.3d 1099, 1103 (9th Cir. 2000) (citations omitted).

## ARGUMENT

### I. THE COURT HAS PERSONAL JURISDICTION OVER NSO

The undisputed evidence cited in Plaintiffs' Motion establishes jurisdiction over NSO for the reasons explained in Plaintiffs' opposition, Dkt. No. 422, to NSO's cross-motion, Dkt. No. 397. If NSO is permitted to incorporate its personal-jurisdiction arguments by reference, the Court should also permit Plaintiffs to do the same. In any event, the Court can reach the merits before resolving personal jurisdiction. *See Wages v. I.R.S.*, 915 F.2d 1230, 1235 (9th Cir. 1990).

## II. NSO IS LIABLE ON PLAINTIFFS' BREACH OF CONTRACT CLAIM

### A. NSO Agreed to the Terms

NSO contends that the "evidence is not sufficient to prove NSO agreed to the WhatsApp [Terms]" because there is supposedly "no evidence" NSO had actual knowledge of the Terms. Opp. 3. That argument is contrary to the undisputed facts and foreclosed by controlling law. NSO's documents and testimony show that it had notice of the Terms, and of the specific provisions it was violating. Moreover, the legal sufficiency of "clicking" to manifest consent is well established.

Plaintiffs have carried their burden of producing undisputed facts sufficient to show that users must accept the Terms to create a WhatsApp account, and that NSO agreed to the Terms accordingly. Mot. 6-8. After downloading and opening the Official Client, "[t]he welcome screen includes links to the terms of service and the privacy policy," and "[t]he user is then given the opportunity to agree to the terms of service[] and continue with the registration flow." Ex. 2 (Lee Dep.) at 174:4-13. At that point in the account-creation process, "in order to proceed with the registration flow, you have to click a button . . . to demonstrate agreement of the terms of service." *Id.* at 180:4-12. Only "[i]f the user chooses to agree to the terms of service and continue" would they be able to register a phone number and create an account. *Id.* at 174:4-21.[1] NSO admits it followed these necessary steps to create WhatsApp accounts, Ex. 8 (Eshkar Dep.) at 70:16-72:25, and WhatsApp's business records show at least 50 NSO employees agreed to the Terms, Dkt No. 401-3 (Andre Decl.) ¶¶ 3-8, Ex. A.[2]

These undisputed facts suffice to bind a user to the Terms under controlling case law. *See*

[1] Plaintiffs can rely on Jonathan Lee's Rule 30(b)(6) testimony at summary judgment. *See Plumley v. S. Container, Inc.*, 2001 WL 1188469, at *4 (D. Me. Oct. 9, 2001), *aff'd*, 303 F.3d 364 (1st Cir. 2002). Lee testified to "the company's knowledge," *Persian Gulf Inc. v. BP W. Coast Prods. LLC*, 632 F. Supp. 3d 1108, 1127-28 (S.D. Cal. 2022), which Plaintiffs "will be able to prove through admissible evidence" at trial, if necessary. *Norse v. City of Santa Cruz*, 629 F.3d 966, 973 (9th Cir. 2010). If necessary, Plaintiffs request the opportunity to do so now. *See* Fed. R. Civ. P. 56(e).

[2] NSO's suggestion that Plaintiffs needed to add Meghan Andre to their initial disclosures is "unreasonable and burdensome (and rarely, if ever, done in practice)." *S.F. Baykeeper v. W. Bay Sanitary Dist.*, 791 F. Supp. 2d 719, 734-35 (N.D. Cal. 2011). Plaintiffs' experts already submitted declarations verifying their reports and curing any admissibility concerns. *See* Dkt. Nos. 422-3, 422-4, 422-5; *Cahill v. Golden Gate Bridge, Highway & Transp. Dist.*, 2016 WL 1070655, at *5 (N.D. Cal. Mar. 18, 2016) ("subsequent verification" permits use of expert reports).

*Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849, 856 (9th Cir. 2022) (contract enforceable when "users must check a box explicitly stating 'I agree' in order to proceed"); *see also Laatz v. Zazzle, Inc.*, 2024 WL 377970, at *7 (N.D. Cal. Jan. 9, 2024) ("hyperlinks constitute reasonably conspicuous notice of terms" and "clicking a button such as the 'Create Account' button is sufficient to manifest assent"); *Sellers v. JustAnswer LLC*, 73 Cal. App. 5th 444, 471-72 (2021) (surveying "overall trend" that where a user is "signing up for an ongoing account," "any textual notice [is] sufficient to bind a consumer").[3] Further, NSO's documents show NSO's actual knowledge of the prohibition on reverse-engineering that it breached. *Compare* Ex. 24 at -959[4] *with* Ex. 11 at -827.

NSO fails to produce any *evidence* creating any material dispute about its knowledge of the Terms, which it "must" do to defeat summary judgment. *Nissan Fire*, 210 F.3d at 1103. There is no *evidence* that NSO was unaware that it was agreeing to the Terms when it followed a process that required it to agree to them in the course of creating nearly a hundred WhatsApp accounts for its own use, *see* Ex. 6 (Gazneli Dep.) at 81:3-7; Ex. 17, and an undisclosed number for its customers, *see* Ex. 27.[5] In fact, in opposing summary judgment on the CFAA claims, NSO asserts it *did* agree to the Terms. Opp. 10-11. NSO cannot argue inconsistent facts at summary judgment. *See, e.g.*, *SEC v. Johnson,* 2022 WL 423492, at *5 (C.D. Cal. Jan. 26, 2022) ("[T]he Court cannot consider any inconsistent facts Defendant produces to establish a genuine dispute of material facts."); *cf. Total Coverage, Inc. v. Cendant Settlement Servs. Grp., Inc.*, 252 F. App'x 123, 126 (9th Cir. 2007).

### B. NSO Breached the Contract

Plaintiffs' Motion showed that NSO breached numerous provisions of the Terms. Mot. 8-10. NSO cannot avoid summary judgment by contorting the Terms' plain meaning, because the contract language should be given "the meaning a layperson would ordinarily attach to it." *Perez-Encinas v.*

[3] NSO's cases are inapposite. *See Marshall v. Hipcamp Inc.*, 2024 WL 2325197, at *5 (W.D. Wash. May 22, 2024) (allowing users to continue using Apple or Facebook); *Jackson v. Amazon.com, Inc.*, 65 F.4th 1093, 1098 (9th Cir. 2023) (addressing amended terms); *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014) (browsewrap agreement); *Berman*, 30 F.4th at 856-58 (same).

[4] Unless otherwise indicated, all emphases have been added.

[5] If NSO believed the appearance of the "button" created a genuine dispute, it could have obtained a publicly available screenshot and submitted it with its opposition. *See* Youssef Decl. 4-6. It did not, because the appearance makes clear NSO had adequate notice it was consenting to the Terms.

*AmerUs Life Ins. Co.*, 468 F. Supp. 2d 1127, 1133 (N.D. Cal. 2006) (citing Cal. Civ. Code § 1638).

**1.** The Terms prohibit, "**reverse engineer[ing]"** and "**decompil[ing], or extract[ing] code** from [WhatsApp's] Services." Ex. 11 at -827. NSO has admitted it breached these terms, acknowledging, for instance, that it "decompil[ed] [WhatsApp's] code" to create a modified application. Ex. 6 (Gazneli Dep.) at 66:2-77:2, 225:5-227:5. And although NSO argues the term "reverse-engineering" is ambiguous, Opp. 6, its corporate representative understood it when he admitted that NSO engaged in "reverse-engineering." Ex. 6 (Gazneli Dep.) at 144:10-147:9. NSO's own documents show the term is not ambiguous, noting that "WhatsApp *explicitly claim against reversing their app*" to develop a "third-party modified WhatsApp" application. Ex. 24 at -959. NSO understood that this conduct violated the Terms, and subjected NSO to risk of detection. *Id.*; Ex. 6 (Gazneli Dep.) at 153:2-17, 231:22-25. NSO also *argues* that it engaged in reverse-engineering (suggesting it does understand the term) only before it agreed to the Terms. Opp. 6. But it provides no *evidence* to substantiate that claim. To the contrary, NSO said its reverse engineering was part of a process "between April 29, 2018 and May 10, 2020," and that it decompiled WhatsApp code after the 2018 security updates. Ex. 6. (Gazneli Dep.) at 66:19-71:5, 246:7-247:1.

**2.** The Terms prohibit using, "or assisting others in using," WhatsApp (i) to "**collect the information of or about [WhatsApp's] users in any impermissible or unauthorized manner**," (ii) to "**gain or attempt to gain unauthorized access** to [WhatsApp's] Services or systems," or (iii) in ways that "**are illegal.**" Ex. 11 at -827. NSO argues that it never operated Pegasus itself. Opp. 7. That is false, but also not a defense, because the Terms prohibit "assist[ing] others to" breach the Terms. Ex. 11 at -827; *see* Mot. 23-24 (citing evidence of NSO assisting its customers). "Impermissible" and "unauthorized" are not vague, as NSO claims (Opp. 7), but require WhatsApp's or users' permission. *See Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067-68 (9th Cir. 2016). NSO provides no evidence it had either. *See* Mot. 9-11; *infra* § III.A.1.

**3.** The Terms prohibit sending "**viruses or other harmful code"** via WhatsApp. Ex. 11 at -827. NSO admits sending Pegasus code, but argues that "'harmful code' is a subjective term." Opp. 7. It is not, and easily covers code designed to take over and extract all information from a device without the user's knowledge (and in violation of the Terms and federal and state law). Ex. 6 (Gazneli

Dep.) at 300:16-19; 311:13-312:15; Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 11.

### C. Plaintiffs Did Not "Waive" Any Known Rights

NSO's waiver argument is meritless. Waiver requires an "intentional relinquishment of a known right with knowledge of its existence and the intent to relinquish it." *CBS, Inc. v. Merrick*, 716 F.2d 1292, 1295 (9th Cir. 1983). Selective enforcement is not a waiver. *See Mahoney v. Depuy Orthopaedics, Inc.*, 2007 WL 3341389, at *9 (E.D. Cal. Nov. 8, 2007); *Martinez v. McNabb*, 2004 WL 103541, at *8 (Cal. Ct. App. Jan. 23, 2004). Plaintiffs could not waive before learning of NSO's breaches, and NSO cites no evidence they waived after. NSO's cases concerning parties that waived after learning of a breach do not apply. Opp. 8. Moreover, NSO's records show it knew Plaintiffs would enforce against NSO if they became aware of NSO's conduct. *See* Ex. 24 at -958-60; Ex. 6 (Gazneli Dep.) at 206:12-208:1. The non-waiver provision, *see* Ex. 11 at -832, also precludes a waiver. *See Auntie Anne's, Inc. v. Wang*, 2014 WL 11728722, at *14 (C.D. Cal. July 16, 2014).

### D. Plaintiffs Suffered Damages

NSO's breaches damaged Plaintiffs. *See* Mot. 11. NSO does not dispute Plaintiffs incurred investigation costs, but argues that they were not foreseeable or caused by NSO. Opp. 8-9. That claim is meritless. NSO knew WhatsApp would remediate NSO's breaches once detected. Ex. 37 (Gazneli Dep.) at 214:12-18. That NSO exploited preexisting code does not break the "causal chain." *See Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935–36 (9th Cir. 2004). NSO also concedes (Opp. 9) that disgorgement "can satisfy the 'damages' element," which only requires that NSO "obtained a benefit they would not have otherwise obtained and profited from that benefit without providing a corresponding benefit to" Plaintiffs. *Artifex Software, Inc. v. Hancom, Inc.*, 2017 WL 4005508, at *4 (N.D. Cal. Sept. 12, 2017); *see* Mot. 11. Finally, even if there were "no appreciable detriment" to WhatsApp (which there was), Plaintiffs would be entitled to nominal damages. *Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1258 (N.D. Cal. 2022).

## III. NSO IS LIABLE ON PLAINTIFFS' CFAA CLAIMS

### A. NSO Violated § 1030(a)(2) and § 1030(a)(4) of the CFAA

#### 1. NSO Intentionally Accessed WhatsApp's Servers and the Target Devices

Plaintiffs' Motion showed that NSO intentionally accessed WhatsApp's servers and the target devices. Mot. 12-13. NSO offers two responses. Both lack merit.

First, NSO claims it lacked intent because it believed its access was authorized (Opp. 22), but it provides no *evidence* that anyone had authorized such access. NSO admits it did not seek permission from WhatsApp or owners of target devices, and knew WhatsApp would ban NSO if it got caught. Mot. 9. NSO points to its CEO's claim that Israel regulates NSO's export of Pegasus, but provides no evidence that Israel authorized NSO to develop, test, or use Pegasus, or could authorize NSO's access to WhatsApp's U.S. computers. Opp. 22 (citing Akro Decl., Ex. H). NSO also points to its customers' purported agreements to use Pegasus only for law enforcement purposes, *id.*, but NSO's customers could not authorize NSO's own development of Pegasus or use of WhatsApp either. Even as to the customers' use of Pegasus, NSO provides no contract in which any customer actually agreed to NSO's use-restrictions, and provides no proof customers used Pegasus only for law enforcement (the undisputed evidence shows they did not[6]) or that any had lawful authorization to access target devices. NSO's belief that its customers would obtain such authorization is not a defense. *See United States v. Christensen*, 828 F.3d 763, 794 (9th Cir. 2015).

Second, NSO contends there is "no evidence NSO 'accessed . . . target devices.'" Opp. 10. That contention fails. NSO admits its Pegasus software used WhatsApp to install the Pegasus agent on "between hundreds and tens of thousands" of target devices that NSO did not control. Ex. 6 (Gazneli Dep.) at 82:14-83:11. NSO was the principal behind all those installations, and its customers' minimal role does not cut off NSO's liability. "Numerous courts have recognized that vicarious or indirect liability under section 1030(g) extends to parties who direct, encourage, or induce others to commit acts that violate the statute." *Ryanair DAC v. Booking Holdings Inc.*, 636 F. Supp. 3d 490, 499 (D. Del. 2022).[7] NSO admits that "[f]rom the perspective of a Pegasus user, the Hummingbird installation of Pegasus was triggered by the user entering a surveillance target's mobile telephone number into a field in a program running on the user's laptop," and "[i]n response,

[6] Ex. 38 (Shohat Dep.) at 29:24-32:14, 180:6-185:16 (admitting Pegasus was used to target Dubai's Princess Haiya, and was abused by 10 customers so severely that NSO disconnected the service).

[7] NSO relies on cases where outsiders induced insiders to obtain information from computers for them. Opp. 10 n.13 (citing cases). *United States v. Nosal* ("*Nosal I*"), 676 F.3d 854, 863 (9th Cir. 2012), concluded those cases involved no CFAA violation because the insider *had* authorization.

***the program*** would instruct a server called the WhatsApp Installation Server ('WIS') to install Pegasus on the surveillance target's device." Gazneli Decl. ¶ 4. In other words, NSO's customers only push a button to request information from a target device; the installation and extraction process, about which NSO's customers knew nothing, was "a matter for NSO and the system to take care of, not a matter for customers to operate." Ex. 10 (Shohat Dep.) at 68:1-16. NSO reverse-engineered WhatsApp to develop that capability, Ex. 6 (Gazneli Dep.) at 66:2-77:2, 226:2-227:5; NSO marketed that capability to customers, Ex. 31; NSO installed the technology for them, Ex. 38 (Shohat Dep.) at 143:15-144:23; NSO provided the server infrastructure to install Pegasus and extract information, Dkt. No. 1-1 at 37-38, 46-47; NSO provided the WhatsApp accounts used in the attack, Ex. 8 (Eshkar Dep.) at 39:15-17, 151:3-153:8; and NSO provided technical support, Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 15-16. NSO is therefore liable for every Pegasus installation.

Moreover, NSO admits to directly accessing devices "under NSO's own control." Opp. 10. That alone suffices for liability because NSO obtained information from them through unauthorized access to WhatsApp's servers, 18 U.S.C. § 1030(a)(2), and also obtained the use of WhatsApp's computers through fraud, *id.* § 1030(a)(4). The CFAA "forecloses" any "defense" that NSO "was 'entitled to obtain' the information . . . through another method," such as direct access to the device. *Van Buren v. United States,* 593 U.S. 374, 385 (2021); *see* Mot. 20-23; Dkt. No. 422 at 16-17.

### 2. NSO Accessed WhatsApp Servers and the Official Client on Target Devices Without Authorization or Exceeded Any Purported Authorized Access

NSO's access to WhatsApp's servers and user devices was unauthorized because NSO (i) used its own modified application, not the Official Client; (ii) circumvented 2018 server updates to carry out the May 2019 attacks; and (iii) continued using WhatsApp after Plaintiffs remediated those attacks, disabled NSO's accounts, and filed this lawsuit. *See* Mot. 13-20. NSO provides no evidence creating a genuine dispute as to any one of these grounds, let alone all of them.

#### *a)* The Terms of Service Did Not Authorize NSO's Access

Despite NSO's contention that there is no evidence NSO agreed to the Terms, Opp. 3, it nonetheless argues that its agreement to those Terms "forecloses" any "without authorization" claim. Opp. 10. NSO cannot have it both ways. If it did not agree, as NSO claims, it had no authorization.

But as explained above, there is no genuine dispute NSO *did* accept the Terms. *See supra* II.A.

There is no inconsistency in Plaintiffs' position that (as NSO paraphrases it) "NSO agreed to WhatsApp's [Terms] and that NSO completely lacked authorization to use WhatsApp's servers." Opp. 10. The Terms only authorize NSO "to use our Services," defined as "our ***apps***, services, features, software, or website." Ex. 11 at -825, -828. The Court recognized that WhatsApp users only have authorization to send messages "using the WhatsApp app," Dkt. No. 111 at 37, and NSO's own documents indicate NSO understood WhatsApp banned "using [a] third-party modified WhatsApp" application. *See* Ex. 24 at -959. Even on a technological level, the authentication keys needed to access WhatsApp servers are created only on the Official Client when it is downloaded, installed, and registered. Ex. 4 (Gheorghe Dep.) at 135:20-140:1. NSO admits it could not use the WIS to access WhatsApp's servers without those keys. Ex. 6 (Gazneli Dep.) at 278:16-279:6. WhatsApp's servers were also designed to work only with the Official Client. Ex. 4 (Gheorghe Dep.) at 279:25-280:10. NSO thus designed the WIS to use the same proprietary "FunXMPP" protocol as the Official Client in order to communicate with the servers. Ex. 6 (Gazneli Dep.) at 279:16-282:10.

Thus, neither NSO nor any other user ever had any "degree[ ] of authorization" to access WhatsApp's servers themselves. Opp. 11. The Terms only authorize users to use *the Official Client*, and *the Official Client* had the technological permissions necessary to access WhatsApp's servers. NSO's argument that its "limited" authorization to use the Official Client also authorized NSO to access the servers in any other manner that NSO chose is essentially the same argument the former employee made in *Nosal II* that his use of a current employee's password only violated a "limit" on that employee's authorization. *See United States v. Nosal* ("*Nosal II*"), 844 F.3d 1024, 1035-37 (9th Cir. 2016). The Ninth Circuit rejected that argument as "ignor[ing] common sense and turn[ing] the statute inside out," because the current employee "had no mantle or authority to override [the employer's] authority to control access to its computers and confidential information by giving permission to former employees." *Id.* NSO similarly had no authority to transfer the Official Client's authorization to another application. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1073-74 (9th Cir. 2004) ("us[ing] someone else's password" and "claim[ing] the server 'authorized' his access" is the "paradigm" of what the CFAA prohibits).

In addition, even if the Terms granted NSO some limited authorization to access WhatsApp's servers (they did not), that authorization can be—and in fact was, *see infra* § III.A.2.b—revoked. *Power Ventures*, 844 F.3d at 1067-68 ("[A] defendant can run afoul of the CFAA when he or she has no permission to access a computer ***or*** when such permission has been revoked explicitly.").

### *b)* NSO Bypassed the Restrictions Built Into the Official Client

The undisputed evidence demonstrates that NSO circumvented technological limitations built into the Official Client by using the WIS to access WhatsApp's servers. Mot. 15-17. NSO attempts to create a dispute of fact about its use of a fake client by presenting Tamir Gazneli's self-serving declaration, which claims that the "WIS created the WhatsApp messages," but "those messages were sent to the target device (via WhatsApp servers) using a genuine WhatsApp client and genuine WhatsApp credentials." Gazneli Decl. ¶ 5. Mr. Gazneli's declaration contradicts his own sworn testimony, in his capacity as NSO's corporate representative, that Pegasus's messages were sent by "a client that *NSO developed*," and "*not* an actual WhatsApp client." Ex. 6 (Gazneli Dep.) at 159:12-162:3. Mr. Gazneli's declaration neither addresses this contradiction, nor attaches any documentary evidence—such as the Pegasus code NSO was ordered to produce (which it did not)—to support his new contention that NSO in fact used an unadulterated Official Client. Mr. Gazneli's declaration therefore cannot create a genuine dispute of fact. *See Hansen v. United States*, 7 F.3d 137, 138 (9th Cir. 1993) ("When the nonmoving party relies only on its own affidavits to oppose summary judgment, it cannot rely on conclusory allegations unsupported by factual data to create an issue of material fact."); *Rainey v. Am. Forest & Paper Ass'n*, 26 F. Supp. 2d 82, 94 (D.D.C. 1998) (excluding affidavit at summary judgment contrary to Rule 30(b)(6) testimony); *Guangzhou Yuchen Trading Co. v. DBest Prods. Inc.*, 2023 WL 2626373, at *2 (C.D. Cal. Feb. 24, 2023) (same).

Even if Mr. Gazneli's declaration were considered, it does not create any material dispute of fact. NSO admits that the "WIS created the WhatsApp messages," Gazneli Decl. ¶ 5, and that "WhatsApp did not program" the Official Client to be able to create those kinds of messages. Opp. 14. Mr. Gazneli does not explain how the Official Client was able to send "WIS created" messages that the Official Client could not create. *Cf.* Akro. Decl., Ex. A (Palau Dep.) at 129:8-20, 131:5-23 ("[U]nder no circumstances" would "one of our official clients" "send something like that" and "[t]his is obviously a malicious client"). Taken as true, NSO either copied parts of the Official Client's code into the WIS in order to send the messages, just as Mr. Gazneli described at his deposition, Ex. 6 (Gazneli Dep.) at 159:12-162:3, or otherwise modified the Official Client so that NSO could insert the "WIS created" messages into the Official Client*, see* Youssef Decl. ¶¶ 6-13. Either way, NSO accessed WhatsApp servers by deceit, passing off "WIS created" messages as if they were Official Client messages. *Theofel*, 359 F.3d at 1072-74 (access is unauthorized if defendant knew "plaintiff was mistaken as to the nature and quality of the invasion intended" (citation omitted)).

### *c)* NSO Used WhatsApp After Plaintiffs Revoked NSO's Access

Even if NSO could credibly argue that its access was authorized at some point, Plaintiffs revoked that authorization no later than when this action was filed. NSO persisted to access WhatsApp after Plaintiffs (i) made security updates that disabled certain NSO attacks, (ii) disabled NSO's accounts, and (iii) filed this lawsuit. Contrary to NSO (Opp. 14-15), that revocation was "categorical," "explicit," "unequivocal," and "particularized."

Plaintiffs' security updates categorically prevented NSO's unauthorized access. NSO's own records show that the 2018 security updates completely disabled its Heaven Malware Vector, and "after the December 2018 update, NSO customers couldn't use the 0 click Android installation vectors" anymore. Ex. 6 (Gazneli Dep.) at 254:2-23, 256:16-25, 258:1-16. Similarly, NSO's own records show that the 2019 updates completely disabled NSO's Eden Malware Vector, and again eliminated NSO's only "0 click Android solution[ ]." *Id.* at 262:3-265:4. Those changes are no less categorical simply because they did not interfere with WhatsApp's billions of users' ability to use the Official Client to "send ordinary WhatsApp messages," Opp. 14, and did not anticipate NSO's "technological gamesmanship." *See Power Ventures*, 844 F.3d at 1067.

Plaintiffs' revocation was also explicit, unequivocal, and particularized. NSO does not dispute that NSO itself received the "403" error associated with the 2018 updates, which indicated that using the Heaven Malware Vector was "forbidden," and the servers "refuse[d] to authorize it." Mot. 17; Opp. 15. NSO immediately understood that its Malware Vector had not "merely . . . malfunctioned," as NSO now claims, Opp. 15, but that "WhatsApp has made changes in their servers that currently fail all installations." Ex. 9; Ex. 6 (Gazneli Dep.) at 254:2-23; Ex. 25 (Vance Rep.) at

7-10. Plaintiffs blocked NSO's access again in May 2019, but also disabled NSO's known accounts and filed a lawsuit alleging violations of federal and state law, and WhatsApp's Terms, and seeking to enjoin NSO from "[a]ccessing or attempting to access WhatsApp's and Facebook's service, platform, and computer systems," and from "creating or maintaining any WhatsApp or Facebook account." Dkt. No. 1 at 14; *see* Mot. 18-19. These steps are indistinguishable from the cease and desist letter and IP blocks deemed sufficient to revoke access in *Power Ventures*. *See* 844 F.3d at 1067 & n.3. Yet NSO continued accessing WhatsApp even while this litigation was pending.[8]

#### ***d)*** **NSO Exceeded Any Purported Authorization**

Even if there were a dispute of fact regarding whether NSO sent messages using the Official Client, NSO still exceeded authorized access by using the WIS to circumvent the Official Client's and the servers' technological limitations. None of NSO's arguments to the contrary have merit.

First, NSO's argument that it did not obtain information *from WhatsApp servers* that it was "not entitled so to obtain" (Opp. 16) fails. There is no requirement that the information only come from the servers. NSO's contention that Section 1030(e)(6) requires the information to come from the same computer accessed without authorization is incorrect. Regardless, NSO does not dispute that "computer" is defined to "include[ ] any data storage facility or communications facility directly related to or operating in conjunction with such device," 18 U.S.C. § 1030(e)(1), and thus includes "computer networks." *Nosal II*, 844 F.3d at 1032 n.2. NSO also does not dispute that WhatsApp is a communications network, and the target devices are "directly related to or operating in conjunction with" the servers. Mot. 22. Thus, NSO's admission that it obtained information from target devices "via the WhatsApp servers" that "a regular WhatsApp user using the WhatsApp client app cannot obtain," Ex. 6 (Gazneli Dep.) at 306:12-307:15, suffices to prove NSO exceeded authorized access.

NSO also obtained and altered information in the servers themselves. NSO claims it only obtained information from the servers that one could obtain with the Official Client. Opp. 16. Even if that were true, it is no "defense" that NSO "was 'entitled to obtain' the information . . . through

[8] Plaintiffs only learned of NSO's continuing conduct at Mr. Gazneli's deposition on September 4, 2024. If necessary, the Court should deem the complaint amended to conform to the evidence.

another method." *Van Buren*, 593 U.S. at 385. And NSO does not dispute altering information in the server by forcing it to add a sixth relay, and to send a directed, malformed response. Mot. 20-21.

Second, NSO argues it did not access areas of the servers that the Official Client could not, but that is not what the CFAA requires. *Van Buren* made clear that NSO must "obtain[ ] *information* located in particular areas of the computer—such as files, folders, or databases—that are off limits to" NSO. 593 U.S. at 396. As shown above, NSO did obtain information from areas of the WhatsApp network (a "computer" within the meaning of the CFAA) that were "off limits."

Third, NSO argues it did not circumvent any technological limitations. NSO is wrong. NSO admits the Official Client could not send the messages that Pegasus depended on, *see* Mot. 16, and its contention that the Official Client did not "prohibit[ ] sending those messages" and was only "a purpose-based 'use restriction'" ignores NSO's own admission that "WhatsApp did not *program*" the Official Client to send those messages. Opp. 13-14; *see* Akro. Decl., Ex. A (Palau Dep.) at 129:8-20, 131:5-23 ("[U]nder no circumstances" would the Official Client "send something like that" and "[t]his is obviously a malicious client"). The Official Client could not *technologically* do what NSO wanted to do, so NSO had to circumvent that "*technological* bar on *access*" (Opp. 13) for its attack.

NSO also circumvented technological limitations on the servers, by circumventing the 2018 and 2019 server changes that WhatsApp made to block NSO's access, *see supra* § III.A.2.c, and the servers' anti-spam filters, *infra* § III.A.3. "[F]inding 'holes in . . . programs,' . . . amounts to obtaining unauthorized access," *United States v. Phillips*, 477 F.3d 215, 220 (5th Cir. 2007), not "compl[ying] with" WhatsApp's technological restrictions, as NSO claims. Opp. 17-18.

### 3. NSO Defrauded Plaintiffs and WhatsApp Users in Violation of § 1030(a)(4)

Plaintiffs' Motion established that NSO violated CFAA § 1030(a)(4). Mot. 22-23. NSO argues that "intent to defraud" should be construed as requiring "an intent to deceive and cheat," as in other statutes, meaning "the intent to deprive a victim of money or property by deception." Opp. 22-23 (citing *United States v. Saini*, 23 F.4th 1155, 1160 (9th Cir. 2022)). NSO cites no case applying that standard to the CFAA. Even if it does apply, it is easily met.

NSO claims its messages were not deceitful, because "WhatsApp *could* detect Pegasus messages *if* it looked for them." Opp. 12. This argument is misleading and does not create a dispute of fact. NSO knew that WhatsApp searched for suspicious or malicious messages, *see, e.g.*, Ex. 24 at -958, and took various steps to avoid its malicious messages being flagged for review, such as hiding its code in the "connecting_tone_desc" message field (which was "an old feature" that "was not in use at the time of the attack," Ex. 39 (Gheorghe Dep.) at 150:13-153:1). NSO also repeatedly changed the fields in which it hid code. *See* Ex. 25 (Vance Rep.) at 8-10 (demonstrating NSO using both "voip_settings" and "group_update" fields). NSO also identified ways to avoid detection by WhatsApp's anti-spam filters, *see, e.g.*, Ex. 24 at -961 (recommending limiting number of attempts), some of which NSO admits it adopted. Ex. 6 (Gazneli Dep.) at 236:8-237:1; *see, e.g.*, Ex. 41 at -121 (after one "Eden installation," "another 2 attempts can be sent in the next two hours" and referring to "the limitations" in an email NSO failed to produce). And if Mr. Gazneli were credited, NSO also sent the malformed messages using an Official Client to disguise their source. Gazneli Decl. ¶ 5.

NSO's reliance on Meta employee testimony that they knew Pegasus's messages were not from an Official Client once they discovered them, Opp. 13, is misplaced because it ignores that the messages were hidden in obscure fields and contained encrypted code "not meant to be easily . . . readable by a human." Ex. 39 (Gheorghe Dep.) at 198:13-25. NSO also mischaracterizes the purpose of the XOR cipher, which was not intended to conceal the buffering messages' *content* from WhatsApp's servers, but to "'camouflage' the appearance of Defendants' packets among normal network traffic, limiting the probability of detection by WhatsApp engineers and/or security mechanisms." Youssef Decl., Ex. A at 33-34; Ex. 40 at -132 ("XOR encryption obfuscated the packet type and content, made attack hard for analysis.").

NSO's contention that it did not intend to take "money or property" from WhatsApp or target users (Opp. 22-23 & n.22) is equally meritless. The "object of the fraud" can include "the use of the computer" if the value exceeds more than $5,000 in one year. 18 U.S.C. § 1030(a)(4). NSO admits using WhatsApp's servers was necessary to the success of its Malware Vectors, which it sold for millions of dollars. *See* Mot. 11. And Pegasus's purpose is to "Turn Your Target's Smartphone into an Intelligence Gold Mine," by "remotely and covertly extract[ing] *all* data." Ex. 31; Mot. 22-23.

### B. NSO Conspired with Its Clients to Use Its Technology in Violation of § 1030(b)

NSO is liable for conspiracy because it agreed with its customers to use Pegasus and supported their use. Mot. 23-24. NSO's response that it did not intend for its customers to violate the CFAA is meritless. NSO argues that it required customers to represent they would comply with applicable laws and only use Pegasus to fight crime. Opp. 18-21. But NSO relies on unsubstantiated form agreements, Akro Decl., Ex. H ¶ 12, and provides no evidence that *any* customer actually made *any* of these representations. Even if they did, the customers do not have the unilateral right to "fight crime" through illegal intrusions, and NSO does not explain how they could have installed Pegasus on user devices via WhatsApp without violating the CFAA, which has no foreign law enforcement exception. It is well established that the CFAA applies extraterritorially. *See, e.g.*, *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 448 (N.D. Cal. 2018) (citing cases). In either case, the Malware Vectors accessed WhatsApp's servers *in the United States*, including in California. Even if NSO's customers were foreign sovereigns (and NSO provides no evidence they are), the act of state doctrine does not apply because accessing WhatsApp's U.S. computers is not an official act that they took within their own borders. *See* Dkt. No. 422 at 18-20; *cf.* 28 U.S.C. § 1605(a)(2), (5) (permitting claims against foreign sovereigns for acts in the United States). NSO claims Congress did not "intend[] to criminalize all such activities by foreign governments," Opp. 20, but in fact, foreign government agents are often prosecuted under the CFAA. *See* Exs. 42-46.

### C. NSO Trafficked in Password-Like Information in Violation of § 1030(a)(6)

Plaintiffs' Motion demonstrates that NSO is also liable for trafficking in "password or similar information." Mot. 24-25.[9] NSO's only argument against liability is that Pegasus is not "a sequence of letters, numbers, symbols or other characters." Opp. 21. This argument ignores that § 1030(a)(6) "turns on whether a user's credentials allow him to proceed past a computer's access gate." *Van Buren*, 593 U.S. at 390 n.9. NSO has admitted that Pegasus provides access to the "same information [in a target device] that you could access if you had a password to the device." Ex. 6 (Gazneli Dep.) at 247:4-17. NSO also extracted authorization keys from the Official Client, and created and gave customers WhatsApp credentials to use with Pegasus to access WhatsApp's servers. Mot. 24-25.

[9] Plaintiffs repeatedly confirmed their pursuit of a claim under § 1030(a)(6). *See, e.g.*, Dkt. No. 163 at 8; Dkt. No. 236 at 12; Dkt. No. 261 at 9. If necessary, Plaintiffs request leave to amend. There is no prejudice given the identical claim under CDAFA § 502(c)(6). Dkt. No. 1 ¶ 61.

### D. NSO Caused Plaintiffs a Loss of More than $5,000

NSO argues that Plaintiffs' investigation and remediation costs do not constitute "loss" because there was no damage to WhatsApp servers and Plaintiffs purportedly "fix[ed] a preexisting vulnerability." Opp. 23-24. This argument is meritless. The Ninth Circuit has held that the "costs [of] analyzing, investigating, and responding to" a defendants' actions constitute "loss." *Power Ventures*, 844 F.3d at 1066; *see* 18 U.S.C. § 1030(e)(11).[10] Even if "damage" were required, it encompasses "impairment . . . as when an intruder retrieves password information from a computer and the rightful computer owner must take corrective measures 'to prevent the infiltration and gathering of confidential information.'" *Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 894-95 (N.D. Cal. 2010) (citing 18 U.S.C. § 1030(e)(8)). There is no genuine dispute that NSO's actions impaired the integrity of the WhatsApp program and system, and required "corrective measures 'to prevent the infiltration and gathering of confidential information.'" *Id.* The attendant costs are still "loss" even if the exploited code was preexisting. *See Creative Computing*, 386 F.3d at 935-36.

## IV. NSO IS LIABLE ON PLAINTIFFS' CDAFA CLAIM

Because Plaintiffs are entitled to summary judgment on their CFAA claims, they are also entitled to summary judgment on their parallel CDAFA claims. *See* Mot. 25.

## V. NSO PROVIDES NO EVIDENCE SUPPORTING AN UNCLEAN HANDS DEFENSE

NSO misconstrues the unclean hands defense, which requires proof that Plaintiffs acted with "fraud or deceit" in acquiring their claims or in a manner that renders it inequitable to assert them. *Ingram v. Pac. Gas & Elec. Co.*, 2014 WL 295829, at *7 (N.D. Cal. Jan. 27, 2014). NSO provides no proof of fraud or deceit. Plaintiffs did not acquire their claims by logging into an AWS server, or by asking Amazon for assistance. *See* Opp. 25. Nor would that render Plaintiffs' suit inequitable.

## CONCLUSION

For the foregoing reasons, the Court should grant summary judgment as to NSO's liability.

[10] *See also Ryanair DAC v. Booking Holdings Inc.*, 2024 WL 3732498, at *13 (D. Del. June 17, 2024) ("loss" does not require "impairment of the protected computer or loss of data"); *Sylabs, Inc. v. Rose*, 2024 WL 4312719, at *3 (N.D. Cal. Sept. 26, 2024) (same). *Van Buren* did not exclude investigative costs "that the statute specifically incorporates." *BrandTotal*, 605 F. Supp. 3d at 1265. *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1262 (9th Cir. 2019), did not involve investigation costs at all.

Dated: October 18, 2024

Respectfully Submitted,

DAVIS POLK & WARDWELL LLP

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

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

*Attorneys for Plaintiffs*
*WhatsApp LLC and Meta Platforms, Inc.*