Greg D. Andres
Antonio J. Perez-Marques
Craig T. Cagney
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
luca.marzorati@davispolk.com

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

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

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

WHATSAPP LLC and META PLATFORMS, INC., a Delaware corporation,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

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

**PLAINTIFFS' NOTICE OF MOTION AND MOTION FOR PARTIAL SUMMARY JUDGMENT**

Date: November 1, 2024
Time: 1:30 p.m.
Ctrm: 3
Judge: Hon. Phyllis J. Hamilton
Action Filed: October 29, 2019

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

CASES

STATUTES & RULES

**NOTICE OF MOTION AND MOTION FOR SUMMARY JUDGMENT**

PLEASE TAKE NOTICE THAT, on November 1, 2024 at 1:30 pm in Courtroom 3 of the U.S. District Court for the Northern District of California, Plaintiffs WhatsApp LLC ("WhatsApp") and Meta Platforms, Inc. ("Meta"; together with WhatsApp, "Plaintiffs") will and hereby do move for partial summary judgment pursuant to Federal Rule of Civil Procedure 56 on Defendants' liability to Plaintiffs on their claims for (1) breach of contract; (2) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; and (3) violation of the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502. This Motion is based upon this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, the Declarations of Micah G. Block and Meghan Andre and all exhibits thereto, the pleadings and papers on file in this action, and on such other written and oral argument as may be presented to the Court.

## MEMORANDUM OF POINTS AND AUTHORITIES

On October 29, 2019, Plaintiffs WhatsApp and Meta filed their Complaint against Defendants NSO Group and Q Cyber (collectively, "NSO"), alleging violations of the Computer Fraud and Abuse Act ("CFAA") and California Comprehensive Data Access and Fraud Act ("CDAFA"), and contractual breaches of WhatsApp's Terms of Service. By its Order dated July 16, 2020, the Court held that Plaintiffs' allegations, if proven, sufficed to establish liability on those claims, as well as personal jurisdiction. Now, with fact discovery completed, the undisputed evidence—including the deposition testimony of Defendants' own percipient and corporate representative witnesses, and Defendants' limited production of internal documents[1]—has confirmed the truth of those allegations. Because the undisputed evidence establishes Defendants' liability on all claims, summary judgment should be entered for Plaintiffs, leaving only the amount of damages to be tried.

As a threshold matter, NSO admits that it developed and sold the spyware described in the Complaint, and that NSO's spyware—specifically its zero-click installation vector called "Eden," which was part of a family of WhatsApp-based vectors known collectively as "Hummingbird" (collectively, the "Malware Vectors")—was responsible for the attacks described in the Complaint. NSO's Head of R&D has confirmed that those vectors worked precisely as alleged by Plaintiffs. Defendants have admitted that they developed those exploits by extracting and decompiling WhatsApp's code, reverse-engineering WhatsApp, and designing and using their own "WhatsApp Installation Server" (or "WIS") to send malformed messages (which a legitimate WhatsApp client could not send) through WhatsApp servers and thereby cause target devices to install the Pegasus spyware agent—all in violation of federal and state law and the plain language of WhatsApp's Terms of Service. NSO's documents reflect that it was well aware of WhatsApp's prohibition on

[1] Subject to further conferring with NSO, Plaintiffs intend to file a separate motion for sanctions in light of NSO's violation of the Court's discovery orders, including through its failure to produce categories of documents, such as source code, which the Court ordered Defendants to produce. Because summary judgment is warranted on the undisputed facts, Plaintiffs' motion is not contingent on the Court granting the relief in Plaintiffs' anticipated sanctions motion. Nonetheless, sanctions are warranted given the scope of NSO's misconduct and its prejudicial impact on Plaintiffs' ability to prosecute this case.

reverse-engineering, and NSO's Head of R&D admits NSO made no effort to comply with WhatsApp's Terms of Service in developing the Malware Vectors.

The purpose of NSO's conduct is also undisputed: to extract valuable information from WhatsApp servers and target devices, and do so secretly, in a manner intentionally designed to deceive and evade detection by not only the owners of the target devices, but by WhatsApp itself. NSO has admitted that it never sought or obtained authorization from WhatsApp to engage in this conduct, and it knew full well that if WhatsApp detected NSO's conduct, it would put a stop to NSO's lucrative venture. Indeed, NSO has admitted that, on several occasions, WhatsApp's security updates disabled its Malware Vectors, at least temporarily. NSO also admits that in those instances, it modified the exploit or developed a new one to circumvent WhatsApp's technical restrictions and continue its unauthorized use of WhatsApp servers to install Pegasus.

Even after WhatsApp detected and blocked the exploit described in the Complaint in May 2019, NSO admits that it developed yet another installation vector (known as Erised) that also used WhatsApp servers to install Pegasus.[2] NSO continued to use and make Erised available to customers even after this litigation had been filed, until changes to WhatsApp blocked its access sometime after May 2020. NSO's witnesses have refused to answer whether it developed further WhatsApp-based Malware Vectors thereafter. All of these facts are undisputed, drawn principally from the corporate representative testimony of NSO's own witnesses, which is binding on Defendants.

These undisputed facts, and others set forth herein, leave no triable issue as to Defendants' liability on any claim. NSO's admitted actions in developing and deploying the Malware Vectors violate the plain terms of the WhatsApp Terms of Service and constitute contractual breaches as a matter of law. The undisputed evidence establishes that NSO accepted those Terms, on dozens of occasions, in creating WhatsApp accounts to develop, test, and deploy its spyware. The admitted

[2] These newly discovered facts stand in stark contrast to NSO's arguments, in seeking dismissal of Plaintiffs' claims for injunctive relief, that Plaintiffs faced no continuing risk of harm following the May 2019 security update, because the Complaint alleged "only past conduct that will not—cannot—reoccur" and that "WhatsApp is once again secure." (Dkt. No. 105 at 1-3).

operation of NSO's spyware–including through its admitted intent to evade detection by WhatsApp or target device owners, to extract valuable information, and to circumvent WhatsApp security updates—establishes violations of the CFAA and CDAFA. NSO's access to WhatsApp servers and the target devices was unauthorized and exceeded any authorized access, and NSO knew it. And as to Plaintiffs' claim under CFAA § 1030(a)(6), for trafficking in password or similar information, NSO admits the access afforded by its spyware is tantamount to having a target device's password.

In short, discovery confirmed the very allegations this Court already ruled were sufficient for liability—as well as revealing new, undisputed facts further establishing liability. Judgment as a matter of law should be entered in Plaintiffs' favor as to liability on all their claims.

## BACKGROUND

WhatsApp provides an encrypted communication service available on mobile devices and desktop computers.[3] *See* Ex. 1 (Youssef Rep.) at 10.[4] WhatsApp users must first install the legitimate WhatsApp client application ("Official Client"), and agree to the WhatsApp Terms of Service ("Terms") before using WhatsApp. Ex. 2 (Lee Dep.) at 176:5-179:4; *see also* Ex. 3 (Woog Dep.) at 177:7-23; Ex. 1 (Youssef Rep.) at 26-27. WhatsApp signaling servers authenticate the Official Client based on an encrypted key created during registration, and then provide a temporary token used to access WhatsApp's relay servers. Ex. 4 (Gheorghe Dep.) at 117:21-119:25, 136:5-137:13. The signaling servers start the call between users, and the relay servers "handl[e] the realtime traffic between devices during a call." *Id.* at 31:14-17, 33:10-21.

NSO's principal spyware product is called "Pegasus." *See, e.g.*, (Dkt. No. 182-1, Ex. Q) (noting NSO's "key surveillance product" is Pegasus). NSO uses Pegasus as a trade name to refer to several component pieces of software used collectively. Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 6-13. A Pegasus "agent" is the software that runs on the target devices to collect and extract information. Ex. 6 (Gazneli Dep.) at 42:23-43:5. The Malware Vectors are the software

[3] Meta served as WhatsApp's service provider, which entails providing both infrastructure and security for WhatsApp. *See* Ex. 4 (Gheorghe Dep.) at 36:17-37:9; 92:18-21.

[4] Citations to "Ex_" refer to the exhibits submitted in connection with the Declaration of Micah G. Block filed contemporaneously herewith, except as otherwise noted.

used to install the Pegasus agent, *id.* at 30:3-31:13; Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 9-13, which NSO's documents characterize as the "heart of any intelligence operation." Ex. 7 (PX2032) at -687; Ex. 6 (Gazneli Dep.). at 97:17-22, 113:3-115:3.

Prior to April 2018, NSO researched, developed, and tested potential installation vectors using WhatsApp by creating an internal environment replicating WhatsApp's servers and by "decompiling" the Official Client's code to understand how to circumvent the security measures built into it.[5] Ex. 6 (Gazneli Dep.) at 70:2-15, 226:17-227:14. Based on this reverse-engineering work, NSO developed an installation vector called "Heaven" that used NSO's own modified client application called the "WhatsApp Installation Server" (or "WIS"). *Id.* at 157:7-164:9. The WIS was able to impersonate the Official Client to access WhatsApp's servers and send messages, including call settings, that the Official Client could not. *Id.* at 237:10-238:16, 278:16-279:6. NSO began testing Heaven on WhatsApp servers around April 2018, and began distributing it to customers shortly afterward. *Id.* at 76:12-22, 87:9-18. NSO created WhatsApp accounts to use with the WIS because it could not access WhatsApp's servers without the authentication key created during registration. *Id.* at 278:16-23. NSO also set up anonymized WhatsApp accounts and server infrastructure for its customers. *See* Ex. 8 (Eshkar Dep.) at 39:15-17, 151:3-153:8.

Heaven had used manipulated messages to force WhatsApp's signaling servers to direct target devices to a third-party relay server controlled by NSO. *Id.* at 196:2-6. In September 2018 and again in December 2018, Plaintiffs made security updates to WhatsApp's servers that prevented NSO's access to the servers and target devices. *See* Ex. 1 (Youssef Rep.) at 38; Ex. 6 (Gazneli Dep.) at 254:14-17. The server changes permanently disabled the Heaven Malware Vector. *See* Ex. 9 (PX2007).

By February 2019, NSO developed a new exploit called "Eden" to circumvent those security updates. Ex. 6 (Gazneli Dep.) 256:16-258:5. The primary difference was that Eden "need[ed] to go through WhatsApp relay servers," not NSO's own relay server. *Id.* at 258:17-22;

[5] "Decompiling" and "reverse engineering" the Official Client are expressly prohibited by the Terms. Ex. 11 (WA-NSO-00014825) at -827.

*see also* Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 8. NSO admits its Eden technology was responsible for the attacks against the approximately 1,400 devices that Plaintiffs observed in May 2019, as described in the Complaint. *See* Ex. 10 (Shohat Dep.) at 69:13-18.

After detecting NSO's malicious messages in May 2019, Plaintiffs' employees invested significant time investigating the source of the exploit and remediating it by making changes to its servers and the Official Client. Ex. 4 (Gheorghe Dep.) at 29:22-25; Ex. 12 (Trexler Rep.) at 21-31. These changes permanently disabled the Eden Malware Vector. Ex. 13 (PX2058) ("Eden/ Heaven/ Hummingbird R.I.P. announcement"); Ex. 14 (PX2039) ("Eden has finished its duty with us"). Plaintiffs also disabled NSO's WhatsApp accounts, *see, e.g.*, Ex. 15 (SHANER_WHATSAPP_00001480), and filed this lawsuit. (Dkt. No. 1). NSO then developed a new Malware Vector called "Erised" that continued using WhatsApp as an installation vector through at least May 2020—even after this litigation had been filed—until changes to WhatsApp eventually disabled that Malware Vector, too. Ex. 6 (Gazneli Dep.) at 45:15-46:16, 267:2-10. NSO refused to state whether it developed further WhatsApp-based Malware Vectors after May 10, 2020. *Id.* at 47:2-6.

## LEGAL STANDARD

A motion for summary judgment must be granted where there is "no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a), (c). As the party bearing the burden of proof at trial, Plaintiffs "must affirmatively demonstrate that no reasonable trier of fact could find other than for the moving party." *Soremekun v. Thrifty Payless, Inc.*, 509 F.3d 978, 984 (9th Cir. 2007). In response to such showing, NSO must set forth "*specific facts* showing that there is a genuine issue for trial." *T.W. Elec. Serv., Inc. v. Pac. Elec. Contractors Ass'n*, 809 F.2d 626, 630 (9th Cir. 1987) (quoting Fed. R. Civ. P. 56(e)).

## ARGUMENT

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

There is no genuine dispute as to any element of Plaintiffs' breach of contract claim, which requires proof of: "(1) the existence of the contract, (2) plaintiff's performance or excuse for nonperformance, (3) defendant's breach, and (4) the resulting damages to plaintiff." *E.D.C. Techs., Inc. v. Seidel*, 216 F. Supp. 3d 1012, 1015 (N.D. Cal. 2016). NSO admits it created WhatsApp

accounts, and thus agreed to the Terms by doing so. NSO reverse-engineered WhatsApp's servers and the Official Client, impermissibly collected information on other users, and accessed WhatsApp's systems without authorization and for illegal purposes, which all violate the Terms. NSO's breaches indisputably damaged Plaintiffs, and Plaintiffs are entitled to summary judgment.

**A. NSO Agreed to the Terms**

NSO admits its employees created and used WhatsApp accounts while developing and using NSO's Malware Vectors. *See, e.g.*, Ex. 6 (Gazneli Dep.) at 272:9-276:18; Ex. 8 (Eshkar Dep.) at 17:13-23, 21:13-24; Ex. 14 (PX2039) at -490. There is no genuine dispute that the employees agreed to the Terms, a necessary step in the WhatsApp registration process, which is sufficient to have bound NSO to the Terms. *See AWR Corp. v. ZTE*, *Corp.*, 2011 WL 13217534, at *2–3 (C.D. Cal. June 13, 2011) (employees can bind employers to agreements "incidental to and reasonably proper in the performance of an assigned task." (citation omitted)).

Plaintiffs have established—and NSO does not dispute—that agreeing to the Terms is necessary to create a WhatsApp account and use WhatsApp. During the registration process, a prospective user is notified about and required to consent to the Terms. *See* Ex. 2 (Lee Dep.) at 176:5-1:4 ("[I]n order to proceed with the registration flow, you have to click a button . . . to demonstrate agreement of the terms of service, and to continue with the registration process."); *accord* Ex. 3 (Woog Dep.) at 177:7-23; Ex. 1 (Youssef Rep.) at 26-27; *see Tompkins v. 23andMe, Inc.*, 2014 WL 2903752, at *8-9 (N.D. Cal. June 25, 2014) (parties "accepted the TOS when they created accounts" by "click[ing] a box . . . that appeared near a hyperlink to the TOS to indicate acceptance of the TOS"). There is no genuine dispute that NSO followed this required process. *See* Ex. 8 (Eshkar Dep.) at 70:16-72:25; Ex. 16 (Shaner Dep.) at 326:9-327:9. In addition, the Terms provide that a user "agrees to [WhatsApp's] Terms of Service by installing, accessing, or using our apps [and] services." Ex. 11 (WA-NSO-00014825) at -825; *see Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014) ("explicit textual notice that continued use will act as a manifestation of the user's intent to be bound" suffices).

*First*, it is undisputed that NSO employees created WhatsApp accounts for NSO and its customers for business purposes. NSO created WhatsApp accounts because legitimate WhatsApp

authentication keys were necessary for NSO's Malware Vectors to gain access to the WhatsApp servers. *See* Ex. 6 (Gazneli Dep.) at 278:16-279:6. NSO created at least 50 WhatsApp accounts on "company owned devices" around April 2018 to test its Malware Vectors on WhatsApp's servers. *See id.* at 80:2-81:7; 83:12-21; 86:23-87:18; 223:4-224:14. NSO's documents identify at least another 41 devices "owned and controlled" by NSO on which WhatsApp had been installed and which were used by NSO to test Malware Vectors through at least May 2020. Ex. 6 (Gazneli Dep.) at 272:9-276:18; Ex. 17 (NSO_WHATSAPP_00044814).[6] NSO also admits it had a "White Services Department" dedicated to creating WhatsApp accounts for customers to use when deploying Pegasus. *See* Ex. 8 (Eshkar Dep.) at 17:13-23, 21:13-24; Ex. 6 (Gazneli Dep.) at 188:12-25. According to WhatsApp's business records, NSO registered the phone numbers used in the May 2019 attacks with WhatsApp from October 2018 to May 2019. Ex. 18 (WA-NSO-00192176).

*Second*, NSO's employees created and used WhatsApp accounts to send and receive NSO business-related communications. *See* Ex. 20 (Defs.' Resp. to Pls.' First RFAs) at 22-23 (admitting certain NSO employees "used WhatsApp in 2019"); Ex. 8 (Eshkar Dep.) at 65:10-66:20 (NSO's VP of Client Executives "communicate[s] with [] coworkers" using WhatsApp); Ex. 21 (Gil Dep.) at 91:10-92:4 (NSO's VP of Global Business Operations uses WhatsApp "for work purposes"); Ex. 6 (Gazneli Dep.) at 252:12-253:14 (NSO's customer support team used WhatsApp to report on updates to installation vectors). Messages sent by various NSO employees using WhatsApp indicated that they used WhatsApp to discuss business matters directly relevant to this case. For example, on December 5, 2018, after the changes that disabled Heaven, a member of NSO's "support team" for "Q [Cyber Technologies]," Ex. 10 (Shohat Dep.) at 175:19-176:14, reported to other NSO employees *via WhatsApp* that "WhatsApp had made changes in their servers that currently fail all installations and can cause crashes." Ex. 9 (PX2007) at -098. On May 12, 2019, after WhatsApp began to remediate the May 2019 attacks, the same employee informed other NSO

[6] NSO designated the phone numbers HC-AEO and refused to allow Plaintiffs to obtain their WhatsApp registration information. But versions of WhatsApp released only after January 2020 were installed on some devices, indicating NSO's consent to the 2020 amended Terms. *See* Andre Decl. ¶ 9, Ex. A; Block Decl. ¶ 18 Ex. 23 (WA-NSO-00195067); Ex. 17 (NSO_WHATSAPP_00044814).

employees *via WhatsApp* that "Eden will not work" because "per r&d they [WhatsApp] close [the] vector from the server side." Ex. 22 (PX2057) at -488. In another *WhatsApp message* that same day, Tomer Timor, the manager of NSO's "pre-sales team," Ex. 8 (Eshkar Dep.) at 84:14-85:1, reported that "Eden has finished its duty with us as a patch was done on the server side with the application it works with," but NSO has "the resources to find some thing [sic] new in a relatively short time." Ex. 14 (PX2039) at -490. At least 50 NSO employees involved in these messages agreed to the Terms between 2016 and 2017. Block Decl. ¶¶ 36-37; Andre Decl. ¶¶ 3-8, Ex. A.

**B. NSO Breached the Contract**

The undisputed facts show that NSO violated the Terms in multiple ways. Indeed, NSO's head of R&D Tamir Gazneli—who was "in charge of developing the installation vector[s]" using WhatsApp—admitted he did not "make an effort to comply with the WhatsApp terms of service." Ex. 6 (Gazneli Dep.) at 222:1-224:16. It is therefore unsurprising that nearly every aspect of NSO's development, testing, sale, and use of its Malware Vectors breached those Terms.

***Reverse-Engineering***: The Terms prohibit, "directly or through automated means . . . reverse engineer[ing], alter[ing], modify[ing], creat[ing] derivative works from, decompil[ing], or extract[ing] code from [WhatsApp's] Services." Ex. 11 (WA-NSO-00014825) at -827. NSO violated these provisions by "decompiling" the Official Client and reverse engineering the functionality and architecture of WhatsApp's servers to develop a modified client application—the WIS—to carry out NSO's exploit. *See* Ex. 6 (Gazneli Dep.) at 66:2-77:2, 226:2-227:5; Ex. 1 (Youssef Rep.) at 34-36 (opining that NSO engaged in reverse-engineering to gain sophisticated "non-public" understanding of WhatsApp); *infra* § II.A.2.a. Mr. Gazneli admitted NSO engaged in "reverse engineering," as he understood the term, by "us[ing] all the tools it should use in order to be able to find the vulnerabilities" in WhatsApp and to "learn the mechanisms and the way [the] client functions." Ex. 6 (Gazneli Dep.) at 144:10-15; 146:18-147:23. According to an internal NSO document, NSO knew that "WhatsApp explicitly claim[ed] against reversing their app," and would ban anyone it discovered doing so, Ex. 24 (PX2033) at -959, but NSO did so anyway.

***Sending Harmful Computer Code***: The Terms prohibit "directly or through automated means . . . send[ing], stor[ing], or transmit[ting] viruses or other harmful code through or onto

[WhatsApp's] Services." Ex. 11 (WA-NSO-00014825) at -827. By its own admission, NSO violated this provision by sending messages containing hidden computer code, such as malicious bash or shell scripts,[7] designed to take over a target device through the WhatsApp service. *See* Ex. 6 (Gazneli Dep.) at 300:16-19 (admitting NSO "would insert a bash script in the connecting tone desc field"); *id.* at 311:13-312:15 (admitting NSO's exploit installed and activated the bash script on the target device); *see also* Ex. 5 (Defs.' Supp. Resps. to Pls' First Interrogs.) at 11 (same).

***Collecting User Information***: The Terms prohibit, "directly or through automated means," using or assisting others in using WhatsApp to "collect the information of or about [WhatsApp's] users in any impermissible or unauthorized manner." Ex. 11 (WA-NSO-00014825) at -827. The undisputed facts show that NSO violated this term. NSO admits that it used WhatsApp to install Pegasus, *see* Ex. 8 (Eshkar Dep.) at 122:24-125:24, 134:11-136-16, and that it developed, designed, and marketed Pegasus "to collect information from a Device." Ex. 20 (Defs.' Resps. to Pls.' First RFAs) at 10-11, 17-19. NSO admits the type of information Pegasus collects is "generally the same information that you could access if you had a password to the device" itself. Ex. 6 (Gazneli Dep.) at 247:4-17. And NSO admits it sold Pegasus to customers so they could obtain that information. *Id.* at 111:3-112:14 ("[T]his is information that customers would like to get access to. That is why we developed the capabilities.").

NSO concedes it never asked WhatsApp or targets for their permission or authorization to collect this information. *See* Ex. 10 (Shohat Dep.) at 49:13-18. NSO knew WhatsApp would block NSO if it had discovered NSO's conduct. Ex. 24 (PX2033) at -958-60 (identifying WhatsApp as a "Threat Actor[]," along with the "target" itself); Ex. 6 (Gazneli Dep.) at 206:12-208:1 (admitting "Threat Actors" are "parties that might detect and seek to prevent the exploit" including "WhatsApp itself"). And WhatsApp users could not have consented because NSO concedes that Pegasus "does not require any interaction from the target," Ex. 6 (Gazneli Dep.) at 37:24-38:1, and "the target is not aware that the agent is being installed," *id.* at 98:8-11.

[7] A bash script is a common form of program on Android devices that is comprised of "a series of commands to be interpreted by the operating system." Ex. 1 (Youssef Rep.) at 14, n.42

***Accessing or Attempting to Access WhatsApp Without Authorization***: The Terms state that WhatsApp must be accessed and used "only for legal, authorized, and acceptable purposes." Ex. 11 (WA-NSO-00014825) at -827. The terms also prohibit "gain[ing] or attempt[ing] to gain unauthorized access to [WhatsApp's] Services or systems." *Id.* As demonstrated below, *see infra* § II.A.2, the undisputed facts show that NSO violated these terms.

NSO admits it accessed WhatsApp's servers using its own fake client—the WIS—to send messages that are not permitted by the Official Client. *See, e.g.*, *infra* § II.A.2.a; Ex. 6 (Gazneli Dep.) at 298:12-299:20 (Official Client cannot use XOR cipher); *id.* at 299:21-300:23 (cannot use connecting_tone_desc field); *id.* at 301:18-302:19 (cannot send oversized bit width detection package); *id.* at 304:23-305:19 (cannot send duplicate call offer message). NSO knew using a fake client was unauthorized and banned. *See* Ex. 24 (PX2033) at -959.

WhatsApp also implemented security measures in September and December 2018 that blocked NSO's unauthorized access to and use of WhatsApp's servers and target devices. *See infra* § II.A.2.b; Ex. 1 (Youssef Rep.) at 38; Ex. 25 (Vance Rep.) at 6-10. Collectively, these changes disabled NSO's Heaven Malware Vector. *See* Ex. 6 (Gazneli Dep.) at 256:23-25, 258:6-8. Yet NSO developed a new installation vector to circumvent those changes. *Id.* at 254:2-258:16.

There is no dispute that NSO continued to access WhatsApp after it was on clear notice its access was unauthorized. *See infra* § II.A.2.c. As part of remediating NSO's May 2019 attacks, Plaintiffs "purge[d]" the WhatsApp accounts of the attacker phone numbers used in the May 2019 attacks, as well as other accounts affiliated with NSO. *See* Exs. 18 & 19 (WA-NSO-00192176); *see* Ex. 15 (SHANER_WHATSAPP_00001480) at -481 (acknowledging that WhatsApp had blocked the account credentials). Plaintiffs then filed this lawsuit alleging that NSO's access was unauthorized and violated the Terms and federal and state law. (Dkt. No. 1). Yet, NSO admits it continued using WhatsApp for its Malware Vectors afterward. *See* Ex. 6 (Gazneli Dep.) at 270:16-271:13. There is thus no genuine dispute NSO "gain[ed] or attempt[ed] to gain unauthorized access to [WhatsApp's] Services" in violation of the Terms. Ex. 11 (WA-NSO-00014825) at -827.

***Using WhatsApp for Illegal Purposes***: Finally, the Terms prohibit using WhatsApp in ways that "are illegal." *Id.* As explained in Section II and III, *infra*, NSO's use of WhatsApp

violated the CFAA and CDAFA, and breached the Terms for that reason as well.

**C. Plaintiffs Fulfilled Their Obligations and Suffered Damages From NSO's Breaches**

There is no genuine dispute that WhatsApp fulfilled its contractual obligations by providing its services, *Facebook, Inc. v. Sluchevsky*, 2020 WL 5823277, at *7 (N.D. Cal. Aug. 28, 2020), and suffered damages from NSO's breaches. Plaintiffs incurred costs investigating and remediating NSO's breaches, *see, e.g.*, Ex. 33 (Robinson Dep.) at 287:2-295:11; *infra* § II.D, which are recoverable as damages. *See Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress*, 402 F. Supp. 3d 615, 659 (N.D. Cal. 2019). NSO realized millions of dollars in unlawful gains from its breaching conduct, *see* Ex. 26 (Trexler Supp. Rep.) at 2-3; Ex. 27 (PX2045); which Plaintiffs are entitled to have disgorged as contract damages. *See, e.g.*, *Artifex Software, Inc. v. Hancom, Inc.*, 2017 WL 4005508, at *4 (N.D. Cal. Sept. 12, 2017). And California law permits recovery of nominal damages based on the breach alone. *See Silicon Image, Inc. v. Analogix Semiconductor*, 642 F. Supp. 2d 957, 964 (N.D. Cal. 2008). Thus, for the foregoing reasons, the Court should grant partial summary judgment finding NSO liable on Plaintiffs' claim for breach of contract.

**II. NSO IS LIABLE ON PLAINTIFFS' CFAA CLAIMS**

The undisputed facts show that Defendants violated the CFAA. NSO admits that (1) it developed, tested, and licensed Pegasus; (2) Pegasus was used as alleged in the Complaint; (3) NSO developed and used multiple methods to install Pegasus on a target device that relied on WhatsApp servers and the Official Client; (4) NSO circumvented multiple WhatsApp security measures, including multiple server updates implemented by Plaintiffs that at various times prevented NSO's access; (5) Pegasus obtains valuable information from devices on which it is installed, including encrypted WhatsApp messages, and (6) the access afforded by Pegasus is similar to the access one could obtain with the device's password. NSO is therefore liable for knowingly and intentionally accessing WhatsApp's servers and users' devices without authorization or in excess of any purported authorization; conspiring with its customers to do the same; and trafficking in password-like information that provided such unauthorized access.

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

Section 1030(a)(2) prohibits "intentionally access[ing] a computer without authorization or

exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Section 1030(a)(4) prohibits "knowingly and with intent to defraud, access[ing] a protected computer without authorization or exceed[ing] authorized access" and thereby furthering "the intended fraud and obtain[ing] anything of value." 18 U.S.C. § 1030(a)(4). The undisputed facts show NSO violated both provisions.

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

There is no genuine dispute that NSO knowingly and intentionally accessed WhatsApp's servers and the target devices using the Malware Vectors. *See Van Buren v. United States*, 593 U.S. 374, 387 (2021) ("'[A]ccess' references the act of entering a computer 'system itself' . . . .").

As to WhatsApp's servers, Mr. Gazneli explained that Pegasus is installed through a WhatsApp voice call, and admitted that "every transmission" had "to be transmitted through WhatsApp servers." Ex. 6 (Gazneli Dep.) at 184:6-10. Accessing the servers was therefore necessary for NSO's exploit. *See id.* at 277:17-278:2; 282:1-10; 325:23-326:19 (admitting that Heaven and Eden were designed to "[c]ommunicate through that WhatsApp signaling server"). To design the Malware Vectors, NSO admits that it researched WhatsApp's servers to understand "[t]he required server functionality that enables you to send messages from one side to another," *id.* at 68:10-69:21, and the "limitations in terms of sending messages from peer to peer," *id.* at 145:23-146:12. NSO hardcoded the WhatsApp's signaling servers' domain names into its source code to "direct the communication to that server specifically," *id.* at 276:19-278:2; and designed a computer script to use WhatsApp's internal, proprietary "FunXMPP" protocol for the sole purpose of "communicat[ing] with WhatsApp servers," Ex. 6 (Gazneli Dep.) at 279:16-282:10 ("There is no other way to communicate."). NSO also created WhatsApp accounts to leverage the Official Client's authentication keys, *see id.* at 81:3-15, because without them NSO could not access the servers and "would be unable to communicate . . . [w]ith WhatsApp at all," *id.* at 278:16-279:6.

NSO also admits it deliberately designed "Eden" to use WhatsApp's relay servers to circumvent the security updates WhatsApp implemented in 2018 that blocked NSO's initial method to install Pegasus on a target device. *See id.* at 254:2-260:2 (admitting NSO "had to use" WhatsApp's relay servers). The undisputed evidence shows that NSO used U.S.-based WhatsApp

relay servers at least 176 times in May 2019 alone, including relay servers in San Jose and Los Angeles, California. *See* Ex. 28 (WA-NSO-00166473); Ex. 4 (Gheorghe Dep.) at 206:8-17 (explaining that servers located in "the San Jose and Los Angeles metro areas . . . were involved in [the] attacks."). NSO knew which relay servers it used to install Pegasus, because it logged the IP addresses for those servers. *See* Ex. 1 (Youssef Rep.) at 37; Ex. 29 (Youssef Rebuttal) at 21.

NSO refused to produce documents regarding Pegasus's full functionality, in violation of this Court's Orders (Dkt. Nos. 292, 358), including the code that relates to stages after the WhatsApp installation process is completed. NSO admits, however, that Pegasus was designed and marketed as "capable of collecting information from mobile devices." Ex. 20 (Defs.' Resps. to Pls.' First RFAs) at 18-19. Indeed, accessing target devices to extract information is "why [NSO] developed the capabilities" and why customers "are willing to buy the software." Ex. 6 (Gazneli Dep.) at 111:21-112:14. NSO also admits the Malware Vectors were used to successfully install Pegasus on "between hundreds and tens of thousands" of devices. *Id.* at 82:14-83:11.

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

The undisputed evidence demonstrates that NSO accessed WhatsApp's servers and user devices "without authorization," or at least exceeded any alleged authorization NSO purports to have had. 18 U.S.C. § 1030(a)(2) & (a)(4).

"The 'without authorization' clause . . . protects computers themselves by targeting so-called outside hackers—those who 'acces[s] a computer without any permission at all.'" *Van Buren*, 593 U.S. at 389-90 (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)). "[T]he CFAA's prohibition on accessing a computer 'without authorization' is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1201 (9th Cir. 2022). By contrast, "the 'exceeds authorized access' clause . . . target[s] so-called inside hackers—those who access a computer with permission, but then 'exceed the parameters of authorized access by entering an area of the computer to which [that] authorization does not extend.'" *Van Buren*, 593 U.S. at 389-90 (quoting *United States v.*

*Valle*, 807 F.3d 508, 524 (2d Cir. 2015)). "[A]n individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." *Id.* at 396.

"[L]iability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system," based on either "technological (or 'code-based') limitations on access," or "limits contained in contracts or policies." *Id.* at 390 & n.8. "The operative question is whether 'the conduct at issue is analogous to 'breaking and entering.'" (Dkt. No. 111 at 35); *accord hiQ Labs*, 31 F.4th at 1197. "[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," and "[o]nce permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067-68 (9th Cir. 2016); *see also United States v. Nosal* ("*Nosal II*"), 844 F.3d 1024, 1035-36 (9th Cir. 2016) ("unauthorized access" includes "getting into the computer after categorically being barred from entry"). Furthermore, "deceit vitiates consent" if the deceptive conduct "relates to the essential nature of his access." *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1073-74 (9th Cir. 2004) ("us[ing] someone else's password to break into a mail server and then claim[ing] the server 'authorized' his access" is "the paradigm of what [the CFAA] sought to prohibit").

The undisputed evidence demonstrates that NSO was not an authorized WhatsApp user "send[ing] messages using the WhatsApp app" (Dkt. No. 111 at 37), but rather an "outside hacker[]," *Van Buren*, 593 U.S. at 389-90, accessing WhatsApp's servers and target devices "without authorization." NSO admits it misappropriated legitimate WhatsApp account authentication keys to gain access to WhatsApp's servers and send messages that the Official Client could not send. *See infra* § II.A.2.a. The record further demonstrates that WhatsApp server updates made in September and December 2018 blocked NSO's ability to access and use WhatsApp's servers and the Official Clients operating on target devices. *See infra* § II.A.2.b. NSO admits that it intentionally circumvented those 2018 updates to restore its Malware Vectors' functionality, regain access to WhatsApp's servers, and continue its attacks, including those alleged

in the complaint. *See id*. Additionally, NSO now admits that after Plaintiffs remediated the May 2019 attacks, disabled NSO's accounts, and filed this litigation—all clearly revoking any purported authorization—NSO developed another WhatsApp-specific Malware Vector that NSO used even after this litigation was filed. *See infra* § II.A.2.c. NSO's access was without authorization under well-established precedent,[8] but at a minimum, exceeded any authorization NSO purportedly had.

***a) NSO Bypassed the Restrictions Built Into the Official Client***

The undisputed evidence demonstrates that NSO circumvented technological limitations built into the Official Client and gained unauthorized access to WhatsApp's servers. *See Theofel*, 359 F.3d at 1073 ("deceit vitiates consent" if it "relates to the essential nature of his access").

WhatsApp's "client application is an official application built by WhatsApp to run on mobile devices." Ex. 4 (Gheorghe Dep.) at 78:23-79:1. The Official Client accesses WhatsApp's signaling servers using a "proprietary . . . noise protocol" that authenticates the Official Client based on "an identity key that's stored on the client device" and "obtained through the registration process to WhatsApp," which should "never leave the client device." *Id.* at 135:20-140:1. Once authenticated by the signaling servers, the Official Client receives a temporary authorization token that permits access to WhatsApp's relay servers. *See id.* at 134:20-135:19. Due to these access restrictions, NSO concedes that it "need[ed] WhatsApp credentials in order to connect to the real WhatsApp environment," because "[w]ithout those credentials [NSO] would be unable to communicate . . . [w]ith WhatsApp at all." Ex. 6 (Gazneli Dep.) at 278:16-279:6.

As this Court recognized previously, "[b]y creating WhatsApp accounts and accepting the terms of service, defendants, as is true of any WhatsApp user, had authorization to send messages

---

[8] The Court's order on NSO's motion to dismiss concluded that the complaint did not state a "without authorization" claim, based on the understanding that NSO implemented its attacks by "sen[ding] messages using the WhatsApp app." (Dkt. No. 111 at 37.) But discovery has revealed NSO implemented its attacks using the WIS, not via the Official Client, *see infra* § II.A.2.a, which proves Plaintiffs' allegation that NSO "reverse-engineered the WhatsApp app and developed a program to enable them to emulate legitimate WhatsApp network traffic." (Dkt. No. 1 ¶ 35). These facts, and the newly discovered evidence that NSO circumvented additional technological barriers, *see infra* § II.A.2.b-c, demonstrate NSO's liability on Plaintiffs' "without authorization" claim. (Dkt. No. 1 ¶¶ 53-54). To the extent pursuing that claim now requires reconsidering the Court's prior order or deeming the pleadings amended to conform to the evidence, Plaintiffs respectfully request that the Court construe this motion as seeking that relief.

***using the WhatsApp app***, which would be transmitted over WhatsApp's servers." (Dkt. No. 111 at 37 (emphasis added)). Here, NSO did not use the Official Client to install Pegasus, nor could it because the Official Client is the first line of defense for WhatsApp's servers. WhatsApp "designed it[s code] and . . . wrote it, assuming that the messages being sent are a part of the WhatsApp network and that they're official clients built by the WhatsApp team." Ex. 4 (Gheorghe Dep.) at 279:25-280:10. As NSO admits, the Official Client did not enable WhatsApp users to set the values of various call settings or send the manipulated messages necessary for NSO's exploit. *Compare* Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 11 ("Eden would also enable the XOR cipher"), *with* Ex. 6 (Gazneli Dep.) at 298:12-299:20 ("Q: Can WhatsApp user[s] using the standard WhatsApp client app send a call offer using an XOR cipher? A: No."); *compare* Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 11 ("Eden set the value of the 'connecting_tone_desc' parameter to a string defining a shell script and executable"), *with* Ex. 6 (Gazneli Dep.) at 299:21-300:23 ("Q: And WhatsApp users using the official WhatsApp client app could not use the connecting tone desc field . . . [,] right? A: Right."); *compare* Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 11 ("These messages included oversized bandwidth estimation packets that caused the callee device to overwrite certain pointers."), *with* Ex. 6 (Gazneli Dep.) at 301:18-302:19 ("Q: WhatsApp users using the official WhatsApp client could not send an oversized bit width detection packet, correct? A: Correct."); *compare* Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 11 ("After Eden determined whether the callee device was 32-bit or 64-bit, it would send a duplicate call offer message . . . to do a transport restart."), *with* Ex. 6 (Gazneli Dep.) at 304:23-305:19 ("Q: And WhatsApp users using the official WhatsApp client could not send the duplicate call offer message. Right? A: Right.").

To circumvent these technical limitations, NSO designed its own version of the Official Client—the WIS—to generate the malformed messages needed to install Pegasus. *See* Ex. 6 (Gazneli Dep.) at 157:7-20, 186:10-17 ("The messages are built and sent from the WIS client."). NSO admits that WIS "is not an actual WhatsApp client." *Id.* at 161:20-162:3. Instead, it "uses part of the protocol capabilities" of the Official Client to leverage its authentication keys to gain unauthorized access to WhatsApp's servers. *Id.* at 161:20-162:3; *see also id.* at 187:1-5 ("WIS has

a connection to a [WhatsApp] client which is activated through the normal procedures of client activation."). NSO's circumvention of the "technological (or 'code-based') limitations on access" built into the Official Client was without authorization. *See Van Buren*, 593 U.S. at 390 n.8.

Like in *Nosal II*, it is no defense that NSO used "legitimate access credentials" (in this case, real authentication keys taken from a registered Official Client), because NSO "had no mantle or authority to override [WhatsApp's] authority to control access to its computers and confidential information" and transfer the authentication keys to the WIS. *Nosal II*, 844 F.3d at 1035. NSO knew doing so and using WIS to access WhatsApp's servers was deceptive and unauthorized. *Cf. Theofel*, 359 F.3d at 1073-74 (concluding "Defendants had at least constructive knowledge" that subpoena used to procure emails was "invalid" and "deceptive"). In a document evaluating how to maintain the secrecy of NSO's use of Heaven, NSO noted that WhatsApp would detect and ban "***us[e of a] third-party modified WhatsApp***," Ex. 24 (PX2033) at -959, and identified the "non-standard requests sent by the WIS server" and the "non-standard activity of WIS client," *id.*, as "[c]reating a risk of potential detection" by WhatsApp, Ex. 6 (Gazneli Dep.) at 153:2-17, 231:22-25. The document suggested ways to avoid these security "mechanisms . . . implemented on the server side," *id.* at 235:19-236:7, some of which NSO admits it implemented—further demonstrating NSO's knowing and deliberate circumvention of WhatsApp's security measures. *See id.* at 236:8-237:1. NSO also extensively researched WhatsApp's servers to craft messages that would avoid being blocked by WhatsApp security features. *See id.* at 145:23-146:12.

***b) NSO Circumvented Plaintiffs' 2018 Security Updates***

Despite NSO's attempts to avoid detection, the undisputed evidence shows that in 2018, Plaintiffs blocked NSO's unauthorized access to WhatsApp's servers and target devices. Specifically, in September and again in December 2018, Plaintiffs implemented security updates to WhatsApp's server code which caused WhatsApp's servers to block attempts to send certain messages, and returned a "403" error code "that was sent to the attackers, providing notice that their access was forbidden." *See* Ex. 25 (Vance Rep.) at 8-10; Ex. 1 (Youssef Rep.) at 37-39. NSO's own expert admits the 403 error "'indicates that the server understood the request but refuses to authorize it.'" Ex. 30 (McGraw Rebuttal) at 26-27 (citation omitted). Log files obtained

from NSO's AWS Servers, which NSO admits it controlled at the relevant time (Dkt. No. 339-1), record the 403 errors that NSO received from WhatsApp's servers in response to its attempts to gain access on December 5 and 6, 2018. *See* Ex. 25 (Vance Rep.) at 8-10; Ex. 1 (Youssef Rep.) at 37-39. In response, on December 5, 2018, NSO's customer support team announced via WhatsApp that "WhatsApp had [sic] made changes in their servers that currently fail all installations." Ex. 9 (PX2007) at -098. Mr. Gazneli explained that Heaven previously forced WhatsApp's signaling servers to direct target devices to a relay server controlled by NSO, but the 2018 server changes prevented NSO from "controlling the target's WhatsApp client to choose that specific relay server." Ex. 6 (Gazneli Dep.) at 254:2-23. As a result, "NSO customers couldn't use the 0 click Android installation vectors," *id.* at 258:6-9, and the Heaven exploit was "not operational," *id.* at 256:23-25.

Nevertheless, after Plaintiffs' security updates further confirmed that NSO's access was unauthorized, NSO circumvented them so it could continue accessing WhatsApp's servers without authorization, including in May 2019. Specifically, NSO developed a new Malware Vector called Eden, which restored NSO's zero-click functionality, with the "main difference" being that NSO intentionally shifted to using WhatsApp's own relay servers (including those in California) to send malicious messages to the target devices. *See id.* at 256:16-259:9; Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 10-11. NSO admits Eden was responsible for the May 2019 attacks described in the Complaint. Ex. 10 (Shohat Dep.) at 69:13-18 ("NSO developed the technology that was used in the event that the complaint refers to."). Because "technological gamesmanship . . . will not excuse liability" after authorization has been clearly revoked, *Power Ventures*, 844 F.3d at 1067, NSO had no authorization for the May 2019 attacks.

***c) NSO Developed, Tested, and Used a WhatsApp Malware Vector After Plaintiffs Filed This Action and Revoked NSO's Access***

NSO admits it continued accessing WhatsApp after Plaintiffs remediated the May 2019 attacks, and again revoked any purported authorization NSO had. *See* Ex. 6 (Gazneli Dep.) at 269:19-271:13. In remediating the May 2019 attacks, Plaintiffs disabled the attackers' WhatsApp accounts, as well as all Meta-affiliated accounts associated with known NSO employees. *See* Ex. 18 (WA-NSO-00192176) (identifying 58 accounts purged in June and July 2019); (Dkt. No. 221-2

(identifying litigation filed in Israel over Plaintiffs disabling NSO employee accounts)). Plaintiffs also filed this litigation alleging NSO's access was unauthorized and seeking to permanently enjoin NSO from accessing WhatsApp. (Dkt. No. 1). Yet, NSO now admits it developed, tested, accessed, and used a new WhatsApp Malware Vector while this litigation was pending. *See* Ex. 6 (Gazneli Dep.) at 269:19-271:13. That continued access and circumvention of the May 2019 security updates, after Plaintiffs expressly revoked NSO's access, was, again, unauthorized in the context of the CFAA. *See Nosal II*, 844 F.3d at 1035-36; *Power Ventures*, 844 F.3d at 1067.

***d) NSO Exceeded Any Purported Authorization to Access WhatsApp's Servers***

Setting aside that NSO had no authorization to access WhatsApp's servers for its Malware Vectors, summary judgment would still be warranted because NSO exceeded any purported authorized access by circumventing WhatsApp's "technological (or 'code-based') limitations on access" and "limits contained in contracts or policies." *See Van Buren*, 593 U.S. at 390 n.8.

There is no dispute that NSO "created a program that went beyond [the server's] restrictions by evading WhatsApp's security features and manipulating the technical call settings." (Dkt. No. 111 at 37). As explained above, the Official Client contains technological, code-based limitations preventing users from sending the types of messages that NSO needed for its exploit, which NSO circumvented by developing its own modified application with greater functionality. *See supra* § II.A.2.a. NSO knew that doing so was prohibited by WhatsApp's Terms and policies, *see* Ex. 24 (PX2033) at -959, and has admitted that using its modified client allowed it to send messages that, in numerous respects, the Official Client was prevented from sending, *see supra* § II.A.2.a.

NSO also deliberately circumvented technological, code-based limitations on WhatsApp's servers. As demonstrated above, NSO knew by at least 2018 that "WhatsApp had [sic] made changes in their servers that currently fail all installations." Ex. 9 (PX2007) at -098. NSO then developed new ways to circumvent these changes to continue its exploit. As the Ninth Circuit has made clear, "[o]nce permission has been revoked, technological gamesmanship . . . will not excuse liability." *Power Ventures*, 844 F.3d at 1067. Thus, the mere fact that NSO was able to send messages for a time before WhatsApp discovered and blocked NSO again does not mean its access was within the scope of any purported authorization. *See United States v. Phillips*, 477 F.3d 215,

220 (5th Cir. 2007) ("[C]onduct, like 'password guessing' or finding 'holes in ... programs,' that uses computer systems not 'in any way related to their intended function' amounts to obtaining unauthorized access." (quoting *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991))).

***e) NSO Accessed Target Devices Without Authorization***

There is no genuine dispute that NSO caused target devices to be accessed without authorization. Any claim by NSO that it never used its technology itself on devices it did not own or control is legally irrelevant. First, because NSO's access to WhatsApp servers was without authorization, the fact that it obtained data from a target device it controlled is not a defense to liability. Once NSO's access to WhatsApp's servers is shown to be without authorization, the source of the information obtained does not matter. *See* 18 U.S.C. § 1030(a)(2), (4); *see also Morris*, 928 F.2d at 511. Moreover, NSO exclusively decided *how* its customers installed Pegasus on target devices, "[b]ecause customers don't care which vector they use, as long as they get the intelligence they need." Ex. 10 (Shohat Dep.) at 68:1-16 ("That's a matter for NSO and the system to take care of, not a matter for customers to operate[.]") NSO's documents explain its installation method is "invisible to the target," "doesn't require their engagement," and "cannot be stopped." Ex. 7 (PX2032) at -687, -689; Ex. 6 (Gazneli Dep.) at 97:23-99:20; Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 9-11. Furthermore, the agent is "persistent," and "designed to withstand aggressive" efforts to remove it, including factory resets. Ex. 7 (PX2032) at -688. NSO included those features because ***NSO designed*** Pegasus to be installed without authorization.

**3. NSO Obtained Information in Violation of § 1030(a)(2)**

NSO used its unauthorized access to obtain "information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). A "protected computer" is one "used in or affecting interstate or foreign commerce or communication," *id.* § 1030(e)(2)(B), and includes "effectively any computer connected to the Internet." *hiQ Labs*, 31 F.4th at 1195. WhatsApp's servers and the target devices were indisputably connected to the internet. *See* Ex. 6 (Gazneli Dep.) at 107:5-18.

The undisputed evidence shows that NSO did obtain information from the WhatsApp servers and target devices by means of its unauthorized access. NSO admits it obtained information regarding whether a user has an active WhatsApp account directly from WhatsApp's

servers. *See id.* at 294:10-15. NSO also obtained information "[v]ia the WhatsApp servers" from the target device, such as the structure of its operating system, *see id.* at 300:24- 304:22, and the location of crucial memory files, which "a regular WhatsApp user using the WhatsApp client app cannot obtain," *id.* at 306:12-307:15. NSO also caused WhatsApp's servers to send messages that only the server can send, *see id.* at 158:14-160:17, and to direct targets to a malicious relay server controlled by NSO, rather than a WhatsApp relay server, *see id.* at 189:25-194:5.

NSO also admits the Malware Vectors were designed to install Pegasus to extract information from target devices. *Id.* at 83:22-84:11 ("Pegasus eventually delivers the data to the customers which are sent to the customers by the [Pegasus] agent."). The product description for Pegasus (Dkt. No. 1-1, Ex. 10), which NSO authenticated, Ex. 20 (Defs.' Resps. to Pls.' First RFAs) at 13-16, describes the many types of data and information Pegasus exfiltrates from target devices. And images of the Pegasus "Installation Status" panel produced in discovery show the same target device phone numbers that were recorded in Plaintiffs' server logs being successfully compromised with Pegasus. Ex. 25 (Vance Rep.) at 13-20. A sales representative for NSO's U.S. reseller affiliate confirmed these installations resulted in extracting information from target devices. *See* Ex. 16 (Shaner Dep.) at 123:3-23, 193:4-195:14, 296:6-298:16 ("[W]ould you similarly demonstrate the ability to extract information from the devices? . . . THE WITNESS: Yes.").

It makes no difference whether the information came from the servers or the target devices, because Section 1030(a)(2)(C) prohibits "access[ing] ***a computer***" and "thereby" obtaining information "from ***any protected computer***," not the same computer. "It is a well-established canon of statutory interpretation that the use of different words or terms within a statute demonstrates that Congress intended to convey a different meaning for those words." *SEC v. McCarthy*, 322 F.3d 650, 656 (9th Cir. 2003). By requiring unauthorized access to "a ***computer***," but information from "any ***protected computer***," Congress made clear the "protected computer" need not be the same "computer" accessed without authorization. *See Theofel*, 359 F.3d at 1078 ("The civil remedy extends to '[a]ny person,'" and "'any' has an expansive meaning, that is, 'one or some indiscriminately of whatever kind.'" (quoting first 18 U.S.C. § 1030(g), then *HUD v. Rucker*, 535 U.S. 125, 131 (2002))); *Morris*, 928 F.2d at 511 ("Congress was punishing those . . .

who, with access to some computers that enable them to communicate on a network linking other computers, gain access to other computers to which they lack authorization . . . .").

Furthermore, the term "computer" is not limited to a single device, but "includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(1). Given this broad definition, "[t]he CFAA's restrictions have been applied to computer networks, databases and cell phones." *Nosal II*, 844 F.3d at 1032 n.2. There is no genuine dispute that WhatsApp is a communications network, and NSO obtained information from devices "related to or operating in conjunction with" WhatsApp's servers.

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

Section 1030(a)(4) requires proof that a defendant accessed a computer "with intent to defraud" and "by means of such conduct furthers the intended fraud and obtains anything of value," which may include the use of a computer if valued at "more than $5,000 in any 1-year period." 18 U.S.C. § 1030(a)(4). "[F]raud 'under the CFAA only requires a showing of unlawful access; there is no need to plead the elements of common law fraud to state a claim under the Act.'" *Facebook, Inc. v. MaxBounty*, *Inc.*, 274 F.R.D. 279, 284 (N.D. Cal. 2011) (citations omitted); *see Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000) ("fraud" means "wrongdoing" and does not require proof of common law fraud). For example, in *Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887 (N.D. Cal. 2010), a former employee acted with "intent to defraud" when he used a co-worker's passwords to access Cisco's computer network, with knowledge of Cisco's policy prohibiting such access. *Id.* at 892-94.

There is no dispute that NSO's exploit was designed to deceive WhatsApp's servers and target devices into believing NSO's messages were legitimate traffic from the Official Client. *See* Ex. 6 (Gazneli Dep.) at 278:16-23 (NSO "connect[s] to the real WhatsApp environment as a legitimate client. Q: As if you were a legitimate client? A: Yes."). NSO admits it understood WhatsApp would shut down NSO's exploit "[i]f it discovered it," and sought to avoid that. *Id.* at 208:2-209:5. By means of this deceptive conduct, NSO obtained both valuable information from the target devices, *see id.* at 111:7-112:14 ("Because [customers] value the information they are willing to buy the software in order to use it."); Ex. 31 (WA-NSO-00004162) (advertising brochure

claiming NSO spyware will "Turn Your Target's Smartphone into an Intelligence Gold Mine"), and the valuable use of WhatsApp servers necessary to the exploit. *See* Ex. 6 (Gazneli Dep.) at 325:23-326:19 ("And it was necessary for the operation of Heaven and Eden? A: Yes."). NSO charged clients up to $6.8 million to use its WhatsApp Malware Vectors on a one-year license, and received at least $31 million in revenue in 2019 from its WhatsApp Malware Vectors, demonstrating their value easily exceeded $5,000 in any one year. *See* Ex. 12 (Trexler Rep.) at 46; Ex. 26 (Trexler Supp. Rep.) at Supp. Ex. 1; Ex. 27 (PX2045); Ex. 21 (Gil Dep.) at 181:21-183:1.

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

NSO cannot evade liability by hiding behind its customers' use of NSO's products. Section 1030(b) imposes liability on any person that conspires to commit or attempts to commit a CFAA violation. *See* 18 U.S.C. § 1030(b). A conspiracy "requires 'specific allegations of an agreement and common activities.'" *In re: Lenovo Adware Litig.*, 2016 WL 6277245, at *6 (N.D. Cal. Oct. 27, 2016) (quoting *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 835 (N.D. Cal. 2014)). There is no dispute that NSO agreed with and supported its clients' use of the Malware Vectors.

NSO admits it entered into licensing agreements permitting clients to use NSO's technology to extract information from WhatsApp users' devices without their consent. *See* Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 15-16. NSO admits Pegasus was designed and marketed for that very purpose. Ex. 20 (Defs.' Resps. to Pls.' First RFAs) at 20-21. And NSO admits that is why customers "are willing to buy the software." Ex. 6 (Gazneli Dep.) at 111:7-112:14.

NSO also engaged in "common activities" that furthered the CFAA violations. *Lenovo*, 2016 WL 6277245, at *6. In addition to developing and providing the technology, NSO admits it set up the infrastructure necessary to extract information from users' devices, including creating WhatsApp accounts.[9] *See* Ex. 8 (Eshkar Dep.) at 39:15-17, 151:3-153:8. NSO also admits it provided training and ongoing technical support, including upgrading the technology to circumvent new security measures and maintain its functionality to "do[ ] our job to deliver[ ] the customers the

[9] That infrastructure included at least one California-based server, the IP address of which had been hardcoded into NSO's malicious code. *See* Dkt. 55-6 (Mornin Decl.) ¶ 2; Dkt. No. 55-2 (Gheorge Decl.) ¶¶ 3-4; Ex. 29 (Youssef Rebuttal) at 22.

software they needed." Ex. 6 (Gazneli Dep.) at 258:1-5; Ex. 5 (Defs.' Supp. Resps. to Pls.' First Interrogs.) at 15-16. NSO is thus liable for its customers' actions as a co-conspirator.

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

CFAA Section 1030(a)(6) prohibits "knowingly and with intent to defraud" trafficking "in any password or similar information through which a computer may be accessed without authorization."[10] The CFAA defines "traffic" as to "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." 18 U.S.C. § 1029(e)(5).

NSO's technology constitutes "password or similar information." Indeed, NSO admits that it permits a user to access the "same information [in a target device] that you could access if you had a password to the device." Ex. 6 (Gazneli Dep.) at 247:4-17. NSO also admits that it created real WhatsApp accounts for its customers, *see* Ex. 8 (Eshkar Dep.) at 39:15-17, which was necessary for its technology to gain access to WhatsApp's servers. *See* Ex. 6 (Gazneli Dep.) at 278:16-279:6. Courts have deemed technologies circumventing similar access restrictions to be "password or similar information" under the CFAA. *See Temurian v. Piccolo*, 2019 WL 5963831, at *6 (S.D. Fla. Nov. 13, 2019) ("(API) information" transmitted to "gain access" to bitcoin account); *Mobile Active Def., Inc. v. L.A. Unified Sch. Dist.*, 2016 WL 7444876, at *7 (C.D. Cal. Apr. 6, 2016) ("top secret, confidentially held URL"); *MetroPCS v. Rivera*, 220 F. Supp. 3d 1326 (N.D. Ga. 2016) (unlocked mobile devices); *see also Van Buren*, 593 U.S. at 390 n.9 (§ 1030(a)(6) "turns on whether a user's credentials allow him to proceed past a computer's access gate").

There is also no genuine dispute that NSO trafficked the Malware Vectors designed to provide unauthorized access to WhatsApp's servers and users' target devices. NSO marketed and demonstrated its products globally, including in the United States and California. *See* Ex. 8 (Eshkar Dep.) at 81:5-86:25 (discussing sales teams in various regions); Ex. 16 (Shaner Dep.) at 45:22-46:18, 204:19-205:15 (NSO "authorized to sell in the United States," without restrictions);

[10] Although the Complaint did not identify § 1030(a)(6), "[a] complaint need not identify the statutory or constitutional source of the claim." *Alvarez v. Hill*, 518 F.3d 1152, 1157 (9th Cir. 2008). Defendants were on notice Plaintiffs were pursuing claims under the CFAA, and based on "knowingly and without permission provid[ing] and assist[ing] in providing a means of accessing Plaintiffs' computers, computer systems, and computer networks." (Dkt. No. 1 ¶¶ 24, 29, 61).

*id.* at 200:3-14, 211:4-21 (admitting to "marketing NSO products to agencies in California"); Ex. 32 (DIVITTORIO_WHATSAPP_00000003). And NSO sold its Malware Vectors to 45 customers for millions of dollars. Ex. 10 (Shohat Dep.) at 70:5-71:21; Ex. 5 (Defs. Supp. Resps. to Pls.' First Interrogs.) at 15-16; Ex. 27 (PX2045) (45 customers with "Covert Android" Malware Vector).

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

Plaintiffs have standing for a civil claim because they suffered at least $5,000 of "loss." *See* 18 U.S.C. §§ 1030(g), (c)(4)(A)(i)(I). "Loss" includes "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." *Id.* § 1030(e)(11); *Power Ventures*, 844 F.3d at 1066 (concluding time "analyzing, investigating, and responding to [defendant's] actions" was "loss"). The undisputed evidence shows that Plaintiffs' employees worked tirelessly to investigate the exploit and develop fixes for WhatsApp's servers and the Official Client to block NSO's unauthorized access. *See* Ex. 4 (Gheorghe Dep.) at 208:19-209:11, 272:13-280:12; Ex. 33 (Robinson Dep.) at 287:2-295:11. The undisputed cost exceeded $5,000. *See* Ex. 12 (Trexler Rep.) at 21-31; Ex. 34 (Pinsonneault Rebuttal) at 29.

**III. NSO IS LIABLE ON PLAINTIFFS' CDAFA CLAIM**

Plaintiffs also are entitled to summary judgment on their CDAFA claim. *See* Cal. Pen. Code § 502. CDAFA is "a state law counterpart to the CFAA." *Meta Platforms, Inc. v. Brand-Total Ltd.*, 605 F. Supp. 3d 1218, 1260 (N.D. Cal. 2022). While "[t]he statutes are different," and CDAFA is broader in many respects, *see United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2016), a CFAA violation will establish a CDAFA violation "because the necessary elements of [CDAFA] do not differ materially from the necessary elements of the CFAA." *BrandTotal*, 605 F. Supp. 3d at 1260 (quoting *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 131 (N.D. Cal. 2020)). For the reasons described in Section II *supra*, the undisputed facts show NSO willfully and fraudulently violated CDAFA, and Plaintiffs are entitled to summary judgment on that claim, too.

**CONCLUSION**

For the foregoing reasons, Plaintiffs respectfully request that the Court grant their motion for partial summary judgment.

Dated: September 27, 2024

Respectfully Submitted,

DAVIS POLK & WARDWELL LLP

By: */s/ Micah G. Block*

Greg D. Andres
Antonio J. Perez-Marques
Craig T. Cagney
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
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.*