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

Micah G. Block (SBN 270712)
DAVIS POLK & WARDWELL LLP
900 Middlefield Road, Suite 200
Redwood City, California 94063
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.

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 CONTEMPT

Date: July 16, 2026
Time: 1:30 pm
Ctrm: 3
Judge: Hon. Phyllis J. Hamilton
Action Filed: October 29, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

NOTICE OF MOTION AND MOTION FOR CONTEMPT

PLEASE TAKE NOTICE THAT, on July 16, 2026 at 1:30 pm in Courtroom 3 of the U.S. District Court for the Northern District of California in Oakland, Plaintiffs WhatsApp LLC and Meta Platforms, Inc. will and hereby do move for an order holding Defendants NSO Group Technologies Limited and Q Cyber Technologies Limited (together, "NSO") in civil contempt for failure to comply with the permanent injunction issued in a November 12, 2025 opinion, *see* Dkt. No. 809, which became enforceable on January 28, 2026. This Motion is based upon this Notice of Motion, the accompanying Memorandum of Points and Authorities, the Declaration of Andrew Blaich ("Blaich Decl.") and the exhibits thereto, the Declaration of Micah G. Block ("Block Decl.") and the exhibits thereto, the pleadings and papers on file in this action, and any such other written and oral argument as may be presented to the Court.

MEMORANDUM OF POINTS AND AUTHORITIES

This Court found NSO liable for violating the CFAA and the CDAFA, and for breach of contract. Dkt. No. 494. NSO's liability was based, in part, on its unauthorized access and use of WhatsApp to deliver spyware and extract data from targeted devices. NSO reverse-engineered WhatsApp's code, built a modified version of the WhatsApp client, and used it to transmit attack messages through WhatsApp's servers that installed spyware on target devices. *Id*. at 11; Dkt. No. 802 at 1. Each time WhatsApp detected and disabled one of NSO's installation vectors, NSO engineered another. The Court found that NSO "redesigned Pegasus to evade detection after plaintiffs first fixed the security breach," Dkt. No. 494 at 12, and that NSO made "repeated efforts to circumvent plaintiffs' security measures," Dkt. No. 802 at 9. That cycle of intrusion, detection, and redesign supported both the finding of liability and the Court's issuance of a permanent injunction.

The permanent injunction bars NSO from "[c]reating accounts . . . on the WhatsApp Platform" and from "[d]eveloping, using, selling, offering for sale, distributing, transferring, or licensing . . . any technology that interacts with or emulates any aspect of the WhatsApp Platform in any way." Dkt. No. 809 ¶¶ 3(a), 3(d). The Court found it necessary to enjoin NSO's use of WhatsApp and account creation because "such activities have been used as a precursor to illegal activities." Dkt. No. 802 at 17. The injunction also requires NSO to delete and destroy its WhatsApp-related code,

Dkt. No. 809 ¶ 4—a provision the Court found "necessary to prevent future violations, especially given the undetectable nature of defendants' technology," Dkt. No. 802 at 17–18. The injunction excludes NSO's foreign sovereign customers from its reach. Dkt. No. 809 ¶ 1. That exclusion covers the sovereign customers themselves; it does not reach NSO, which remains bound by the injunction's terms—including when it creates accounts and operates the delivery infrastructure its customers use. Accordingly, the injunction reaches not only the intrusions, but the code and the conduct that made them possible.

Clear and convincing evidence shows that NSO began violating this Court's injunction almost immediately and continues violating it today. Since the injunction went into effect on January 28, 2026, NSO has engaged in two categories of conduct that the injunction prohibits. *First*, NSO created and operated accounts on the WhatsApp platform, using them to set up groups for "testing." Blaich Decl. ¶¶ 7, 10. *Second*, in February and April 2026, NSO used WhatsApp to send one-click malicious URL links to targeted WhatsApp users. *Id.* ¶ 13, 16–17. This account creation activity and the use of WhatsApp's infrastructure violates the Court's order.

NSO should be held in civil contempt. Plaintiffs ask the Court to (i) find NSO in contempt of paragraphs 3(a), 3(d), and 4; (ii) impose coercive sanctions on an escalating schedule that runs until NSO purges its contempt, and that resumes if a compliance certification later proves inaccurate; and (iii) condition any purge on NSO's certification of compliance and its disclosure of the WhatsApp accounts it currently operates and the IP addresses it currently uses, so that compliance can be tested against the record rather than taken on assertion.

BACKGROUND

A. The Permanent Injunction

On October 17, 2025, nearly six years after this action was filed, and following summary judgment, a damages trial, and a post-trial evidentiary hearing, this Court granted Plaintiffs' motion for a permanent injunction. Dkt. No. 802. The Court found that NSO had caused ongoing irreparable harm through "the covert, undetectable nature of [its] technology" and its "repeated efforts to circumvent plaintiffs' security measures," and that NSO had admitted through its own witnesses that circumventing those measures was "our business." *Id.* at 6–9. NSO then objected to Plaintiffs'

proposed form of injunction, Dkt. No. 805, including by seeking carve-outs that would have permitted continued data collection from WhatsApp users so long as the collection did not pass through WhatsApp servers. The Court overruled those objections, holding that NSO had identified no basis to revisit issues "fully raised and considered throughout this case," Dkt. No. 808 at 1, and entered the permanent injunction on November 12, 2025, Dkt. No. 809.

The injunction binds NSO, its officers and employees, and "all other persons who are in active concert or participation with" them. *Id.* ¶ 1. Three of its provisions are particularly relevant here:

- Paragraph 3(a) prohibits NSO from "[d]eveloping, using, selling, offering for sale, distributing, transferring, or licensing . . . any technology that interacts with or emulates any aspect of the WhatsApp Platform in any way, including as a method or approach used to install and deploy the technology (an 'installation vector')."
- Paragraph 3(d) prohibits NSO from "[c]reating accounts . . . on the WhatsApp Platform, without first requesting and obtaining Plaintiffs' express written permission."
- Paragraph 4 requires NSO to "delete and destroy any and all computer code or technologies that use, access, or depend on the WhatsApp Platform," to "delete all data obtained or derived from use of or access to the WhatsApp Platform," and to "disable customer access to any and all computer code or technologies maintained by [NSO] that use, access, or depend on the WhatsApp Platform."

B. Post-Injunction Conduct

Since the injunction issued, NSO has continued to operate on the WhatsApp Platform. Plaintiffs have identified two categories of post-injunction conduct that violate this Court's orders: NSO's continued creation and operation of WhatsApp accounts, and NSO's continued use of WhatsApp to deliver one-click malicious URLs to target devices.

Creation and operation of WhatsApp accounts. According to WhatsApp data and WhatsApp user reports, between January 28, 2026 and the date of this filing, NSO created at least 23 new WhatsApp accounts and continued to operate accounts it controls on the Platform, including accounts created before the injunction. Blaich Decl. ¶ 7. NSO used those accounts to create "testing groups"—WhatsApp group chats to demonstrate, test, or confirm the functionality of the spyware.

Id. ¶ 10. On or about February 4, 2026, based on a user report, an NSO-operated account sent an image of a desktop mat displaying the NSO Group brand logo. *Id.* ¶ 12 & Ex. A. NSO has continued to create additional WhatsApp groups through June 2026. *Id.* ¶¶ 7, 10.

Deployment of one-click malicious URLs. Between February 3 and February 7, 2026, an NSO customer using NSO's spyware and NSO-operated delivery infrastructure sent one-click malicious URLs using WhatsApp to a WhatsApp user. *Id.* ¶ 16. The URLs used the domain ghazacast[.]com—part of a distinctive family of "*cast[.]com" domains that the Threat Intelligence team associates with NSO's one-click delivery infrastructure. *Id.* ¶¶ 16, 18. The WhatsApp user who received the URL used the reporting function in WhatsApp client application to report and share a portion of the WhatsApp chat thread with WhatsApp. Between April 13 and April 19, 2026, an NSO customer using NSO's spyware and NSO-operated delivery infrastructure sent additional malicious one-click URLs to multiple targets, using another domain in that same *cast[.]com family (ikhwancast[.]com). *Id.* ¶ 17. Each URL was designed so that, if the target clicked the link, malware would attempt to download and install on the device. *Id.* ¶ 14. The malicious URLs follow the distinctive infrastructure pattern, redirect behavior, and lure design that Plaintiffs have historically associated with exploit delivery infrastructure operated by NSO. *Id.* ¶ 18.

ARGUMENT

The permanent injunction expressly reserves the Court's authority to enforce its terms. It states that the "retain[s] jurisdiction to enforce the terms of this Permanent Injunction and to address other matters arising out of or regarding this Permanent Injunction, including any allegations that Defendants have failed to comply with their obligations as set forth in this Permanent Injunction, and the parties shall submit to the Court's jurisdiction for those purposes." Dkt. No. 809 at 2.

Civil contempt consists of a party's disobedience of a specific and definite court order by failure to take all reasonable steps within the party's power to comply. *Reno Air Racing Ass'n v. McCord*, 452 F.3d 1126, 1130 (9th Cir. 2006). A party's behavior "need not be willful" to justify a finding of civil contempt. *In re Crystal Palace Gambling Hall, Inc.*, 817 F.2d 1361, 1365 (9th Cir. 1987). "[T]here is no good faith exception to the requirement of obedience to a court order." *In re Dual-Deck Video Cassette Recorder Antitrust Litig.*, 10 F.3d 693, 695 (9th Cir. 1993); *see also*

McComb v. Jacksonville Paper Co., 336 U.S. 187, 191 (1949) ("[I]t matters not with what intent the [contemnor] did the prohibited act"); *Donovan v. Mazzola*, 716 F.2d 1226, 1240 (9th Cir. 1983) ("Intent is not an issue in civil contempt proceedings. The sole question is whether a party complied with the district court's order."). "The moving party has the burden of showing by clear and convincing evidence that the contemnors violated a specific and definite order of the court." *FTC v. Enforma Nat. Prods., Inc.*, 362 F.3d 1204, 1211 (9th Cir. 2004). "The burden then shifts to the contemnors to demonstrate why they were unable to comply." *Id*. That standard is satisfied here.

I. NSO Violated the Injunction By Creating and Operating WhatsApp Accounts

The injunction is unambiguous: NSO may not create accounts on the WhatsApp Platform without WhatsApp's express written permission, and may not use any technology that interacts with the WhatsApp Platform. Dkt. No. 809 ¶¶ 3(a), 3(d). NSO has not sought or obtained that permission. NSO has nonetheless created at least 23 new WhatsApp accounts since January 28, 2026, and used WhatsApp accounts it operates to create at least 34 groups, at least 20 of which are "testing groups." Blaich Decl. ¶¶ 7, 10.

The accounts are operated by NSO. Plaintiffs identified the NSO accounts through a combination of technical signals and infrastructure attributable to NSO. *Id.* ¶¶ 8–9. A user report further confirms attribution: an image sent within one of the testing groups on February 4, 2026 and reported to WhatsApp depicts a desktop mat bearing the NSO Group logo—branding that appears in NSO testing account messages. *Id.* ¶ 12 & Ex. A. This Court previously admitted similar evidence—messages containing images of NSO-branded materials on desks alongside test devices—as demonstrating NSO testing activity on Plaintiffs' platforms. *See* Block Decl. Ex. A (Aug. 28, 2025 Hr'g Tr.) at 38, 46, 51 (admitting Exhibits A, B, and C); Dkt. No. 802 at 6–7.

This conduct violates two distinct provisions of the permanent injunction. Account creation is prohibited under paragraph 3(d) without qualification: the injunction does not turn on what the account is used for, only on whether NSO created it. Use of the WhatsApp Platform is independently prohibited under paragraph 3(a), which covers any "technology that interacts with or emulates any aspect of the WhatsApp Platform." Every WhatsApp account—whether the user runs the official client or an unofficial client built to mimic it—sends messages through and exchanges data with the

Platform. Operating a WhatsApp account therefore necessarily involves using technology that interacts with the Platform within the meaning of paragraph 3(a). NSO's continued operation of testing accounts violates paragraph 3(a) regardless of when the underlying accounts were created, and the accounts created after January 28, 2026 separately violate paragraph 3(d).

NSO's testing accounts are how it confirms that its spyware functions properly. Blaich Decl. ¶ 8. This is the same kind of testing conduct through which NSO developed the WhatsApp installation vectors the Court found it used to deploy Pegasus. And the Court enjoined exactly this activity knowing it might otherwise be lawful: "while it may remain legal to create new Whatsapp accounts and to use Whatsapp, the facts in this case show that such activities have been used as a precursor to illegal activities, and thus . . . such activity must be enjoined." Dkt. No. 802 at 17. NSO's continued operation of testing accounts is the precursor conduct the injunction was entered to reach.

II. NSO Violated the Injunction By Deploying One-Click Malicious URLs Through the WhatsApp Platform

Paragraph 3(a) prohibits NSO not only from "using" but also from "developing, . . . distributing, transferring, or licensing . . . any technology that interacts with or emulates any aspect of the WhatsApp Platform in any way." Dkt. No. 809 ¶ 3(a). Paragraph 4 requires NSO to disable customer access to any code that depends on the Platform. *Id.* ¶ 4. NSO has violated both. In the February and April 2026 campaigns, an NSO customer used NSO-operated delivery infrastructure to send one-click malicious URLs to targets through WhatsApp. Blaich Decl. ¶¶ 13, 16–17. That infrastructure is technology that interacts with the WhatsApp Platform, and NSO's development and provision of it to its customer is "using . . . [and] distributing, transferring, or licensing . . . technology that interacts with . . . the WhatsApp Platform in any way." Dkt. No. 809 ¶ 3(a). NSO does not avoid the injunction by routing the final transmission through a customer: the injunction reaches NSO's provision of the platform-interacting infrastructure, whoever sends the message.

The campaigns are well documented. In February 2026, an NSO customer used NSO's infrastructure to send one-click malicious URLs through WhatsApp to targets. Blaich Decl. ¶ 16. In April 2026, an NSO customer used NSO's infrastructure to send further one-click malicious URLs through WhatsApp to additional targets, with the most recent documented attack conducted on April

19, 2026. *Id.* ¶ 17. Both campaigns relied on the same pattern of activity that Plaintiffs have identified as signatures of exploit delivery infrastructure operated by NSO. *Id.* ¶ 18.

The conduct violates paragraph 3(a) because each delivery of a one-click malicious URL through NSO-provided infrastructure is NSO's use of "technology that interacts with . . . the WhatsApp Platform in any way"—the conduct paragraph 3(a) prohibits. Dkt. No. 809 ¶ 3(a). The technology by which those URLs are delivered interacts with the WhatsApp Platform in two respects: the messages traverse WhatsApp's servers, and they are sent through WhatsApp accounts (whether operated through the official client or through a fake client). That is the "technology that interacts with . . . any aspect of the WhatsApp Platform" paragraph 3(a) prohibits.

To the extent that NSO contends that the 2026 campaigns are its customers' conduct rather than its own, the trial record foreclosed that argument. There was overwhelming evidence that NSO designed and controls the functionality of its spyware delivery apparatus. Indeed, this Court found on summary judgment that NSO designed and operates the Pegasus delivery system. The 2019 attack vectors at issue at trial were zero-click: "every transmission" was "transmitted through WhatsApp servers" using infrastructure NSO built, Dkt. No. 796-3 at 80, and the entire process—executing the intrusion, installing the agent, and extracting data—was "a matter for NSO and the system to take care of, not a matter for customers to operate," *id*. at 136. One-click delivery is part of that same apparatus. NSO's former CEO has sworn that the technologies marketed as "Pegasus" include both "zero click" methods and methods that "require some engagement by the end user of the mobile device (i.e., 'one click')." Dkt. No. 605-2 ¶ 5; *see also* Dkt. No. 1, Ex. 10 at 12 (NSO brochure describing various zero-click and one-click installation vectors). The February and April 2026 campaigns bear the same technical and tradecraft signatures of NSO exploit delivery, this time delivered through one-click URLs designed to induce the target to click. The one-click malicious URLs follow the *cast[.]com pattern Plaintiffs associates with NSO single-click delivery, and the fr24cast[.]com matches a domain Plaintiffs confirmed in a pre-injunction campaign by the same NSO customer. Blaich Decl. ¶¶ 15, 18. That the target must click the lure does not convert NSO's conduct into the customer's. The division of labor is the one the record established at the merits stage: NSO operates the delivery infrastructure, and the customer only identifies the target.

This conduct also violates paragraph 4 of the injunction. The injunction requires NSO to "disable customer access to any and all computer code or technologies maintained by [NSO] that use, access, or depend on the WhatsApp Platform." Dkt. No. 809 ¶ 4. The record establishes that NSO operates and maintains the infrastructure through which the February and April 2026 one-click malicious URLs were transmitted. Blaich Decl. ¶¶ 18–19 (discussing infrastructure pattern, redirect behavior, and lure design that Plaintiffs have historically associated with exploit delivery infrastructure operated by NSO). The continued operation of NSO-maintained delivery infrastructure documented above is, on its face, inconsistent with the code-and-technology deletion paragraph 4 requires.

As this Court found on summary judgment, NSO maintains the spyware delivery infrastructure and controls software updates, Dkt. No. 494 at 7–8, 11–12, and NSO has admitted that the entire installation process is for "NSO and the system to take care of," Dkt. No. 796-3 at 136. NSO's own public statements confirm the same operational control. In January 2026, NSO publicly stated that it "maintains the capability to suspend or disable systems where credible concerns of misuse arise," and that its safeguards include "kill-switch capabilities" and "customer suspensions and terminations with material financial impact." NSO Group, *2025 Transparency Report* 13, 18, https://www.nsogroup.com/wp-content/uploads/2026/01/2025-Transparency-and-Responsibility-Report.pdf. NSO cannot credibly represent to the public that it *has* the capability to disable customer access and simultaneously represent to this Court that it *lacks* the capability to implement paragraph 4's disable-customer-access requirement. Moreover, to the extent NSO claims that its architecture prevents it from disabling customer access, that is the paradigm of self-induced inability, which the Ninth Circuit has long refused to credit as a defense to contempt. *See United States v. Asay*, 614 F.2d 655, 660 (9th Cir. 1980).

III. NSO's Continued Conduct Reflects a Documented Pattern of Noncompliance with This Court's Orders

Civil contempt does not require willfulness. *Crystal Palace*, 817 F.2d at 1365. But the relief warranted by contempt depends on the circumstances of the noncompliance, including whether the contemnor has a record of disregarding the Court's prior directives. *Calvillo Manriquez v. DeVos*,

411 F. Supp. 3d 535, 540 (N.D. Cal. 2019). NSO's record in this case demonstrates a pattern of noncompliance warranting significant sanctions.

Throughout this litigation, NSO has resisted and evaded this Court's authority. It has made representations the record later contradicted, transferred evidence beyond the Court's reach, and refused to produce materials the Court ordered produced. For example, in 2020, NSO represented to the Court that it had no advance knowledge of the Israeli government's seizure order that halted discovery in this case. Dkt. No. 405-2 at 16–17. In fact, NSO had approached the Israeli government months earlier about issuing such an order. *Id*. In 2023, NSO's CEO declared that the relevant Pegasus technology was "used only on Android devices and only in or around April and May 2019," and that "[e]arlier and later versions of Pegasus operated differently and are not relevant." Dkt. No. 179-3 ¶ 8. That representation was false. NSO's own corporate representative testified that NSO used WhatsApp to install Pegasus from early 2018 through at least May 2020. Dkt. No. 796-3 at 68, 77, 98. NSO represented to the Court that it had produced the Pegasus source code on its AWS server. *See* Dkt. No. 475 at 1. NSO had instead transferred the code to Israel after this litigation began, placing it beyond the Court's reach. Dkt. No. 339-1 ¶ 6. When the Court ordered the code produced, NSO refused. Dkt. No. 494 at 9.

NSO has continued the same pattern of conduct in connection with the permanent injunction. Seven days after this Court entered the injunction, NSO's CEO submitted a sworn declaration in support of NSO's motion to stay the injunction pending appeal, representing that NSO's "prior testimony that NSO no longer has any installation vectors for Pegasus that use WhatsApp, WhatsApp's servers, or WhatsApp's client application remains accurate." Dkt. No. 813-1 ¶ 46. The conduct documented above—account creation, testing operations, and malicious URL delivery through WhatsApp—has continued in the months since. A number of the accounts NSO created and operated before the injunction remained active when this motion was filed, and NSO has continued to operate them since. Blaich Decl. ¶ 7.

That history matters here in two respects. First, the violations documented in Sections I and II are not the product of confusion about what the injunction prohibits. NSO represented to the Court that no "installation vectors for Pegasus that use WhatsApp, WhatsApp's servers, or WhatsApp's

client application" remained. Dkt. No. 813-1 ¶ 46. NSO thus acknowledged what the injunction plainly requires—that it stop using the WhatsApp Platform to conduct its operations. The injunction is appropriately broader still: it bars NSO from creating accounts on the platform and from using any technology that "interacts with . . . the WhatsApp Platform in any way," whether or not that technology is an "installation vector" and whether or not it delivers Pegasus. Dkt. No. 809 ¶ 3(a). Yet NSO continues to create and operate accounts and testing groups on the platform—conduct paragraph 3(a) plainly prohibits, and conduct NSO's representation did not even purport to have stopped. Whatever NSO now says about the form its spyware delivery has taken, its post-injunction account creation and testing cannot be explained as a good-faith effort to comply. Second, the pattern bears on relief. Lesser sanctions and ordinary court orders have not produced compliance with this Court's prior directives. There is no reason to expect a different result here without a sanction calibrated to NSO's demonstrated willingness to disregard the Court's order.

IV. Maximum Coercive and Compensatory Sanctions Are Warranted

Sanctions for civil contempt serve two distinct purposes: "(1) to compel or coerce obedience to a court order, and (2) to compensate the contemnor's adversary for injuries resulting from the contemnor's noncompliance." *Shuffler v. Heritage Bank*, 720 F.2d 1141, 1147 (9th Cir. 1983). In fashioning an award of sanctions for civil contempt, the Court must examine "the harm to plaintiff; the effectiveness of any proposed sanction; defendants' financial situation; and the willfulness of defendants' violations." *U2 Home Ent., Inc. v. Avoplex Corp.*, 2006 WL 1581943, at *1 (N.D. Cal. June 6, 2006). Both forms of relief are warranted.

A. Coercive Per Diem Sanctions, Escalating Every 30 Days

A per diem fine for each day of noncompliance is "paradigmatic civil contempt" relief. *Oliner v. Kontrabecki*, 305 B.R. 510, 522 (N.D. Cal. 2004). The Ninth Circuit requires that the amount be "optimally calculated so as to deter noncompliance without imposing an excessive penalty," with consideration of "the character and magnitude of the harm threatened by the continued contumacy" and "the probable effectiveness of any suggested sanction in bringing about the result desired." *Coleman v. Newsom*, 131 F.4th 948, 965 (9th Cir. 2025); *Shuffler*, 720 F.2d at 1148. Where a defendant has shown a willingness to absorb fixed daily fines, courts have imposed escalating structures that

double at regular intervals until compliance is achieved. *See, e.g.*, *Telenor Mobile Commc'ns AS v. Storm LLC*, 587 F. Supp. 2d 594, 621 (S.D.N.Y. 2008), *aff'd*, 351 F. App'x 467 (2d Cir. 2009) (initial $100,000 per day, doubling every 30 days); *BOC Aviation Ltd. v. AirBridgeCargo Airlines, LLC*, 2022 WL 17581775, at *17 (S.D.N.Y. Dec. 12, 2022) (per diem fines doubling after two weeks and tripling after four weeks).

Two features of this case call for a substantial opening per diem and an escalating structure. First, a modest sanction is unlikely to deter NSO. NSO spent approximately $59 million on research and development in 2024 alone, much of it directed at developing new installation vectors for Pegasus. Dkt. No. 802 at 19. A sanction of $100 per day—the amount imposed in *Facebook, Inc. v. Power Ventures, Inc.*, 2017 WL 3394754, at *15 (N.D. Cal. Aug. 8, 2017)—represents less than 0.1% of NSO's daily R&D spend and would have no coercive effect.

Second, NSO has a documented history of noncompliance with this Court's orders. "Good faith—or the absence thereof—'may help to determine an appropriate sanction.'" *Calvillo Manriquez*, 411 F. Supp. 3d at 540 (quoting *Taggart v. Lorenzen*, 587 U.S. 554, 555 (2019)). Written orders, evidentiary sanctions, and a permanent injunction have not produced compliance. *See supra* Section III. The escalating per diem structure is necessary because NSO's history shows that fixed daily fines, however high, can be absorbed indefinitely. Doubling at 30-day intervals transforms the sanction from a fixed cost into a rapidly compounding one that NSO cannot rationally tolerate.

Plaintiffs request that the Court impose a coercive per diem sanction in an amount sufficient to coerce NSO's compliance, beginning to accrue on the date of the contempt order and doubling every 30 days thereafter, until NSO demonstrates that it has purged its contempt.

NSO should not be permitted to purge by certification alone. NSO's chief executive has already submitted to this Court a sworn declaration that the record contradicted. *See supra* Section III. A compliance certification from the same office, untethered to facts WhatsApp can verify, cannot establish compliance with an injunction NSO has every capability and incentive to evade. The Court should therefore condition purge on two requirements: (1) certification under penalty of perjury by NSO's chief executive officer (currently Akiva Rosner) and its executive chairman (currently David

Friedman); and (2) disclosure sufficient to let WhatsApp test that certification against its own records—specifically, identification of every WhatsApp account NSO currently operates or controls and every IP address NSO currently uses to interact with the WhatsApp platform.

Courts in this district routinely require a defendant to certify compliance in writing and under oath. *OpenAI, Inc. v. Open A.I., Inc.*, 719 F. Supp. 3d 1033, 1052 (N.D. Cal. 2024), *aff'd*, 2024 WL 4763687 (9th Cir. Nov. 13, 2024) ; *Apple, Inc. v. Psystar Corp.*, 673 F. Supp. 2d 943, 956–57 (N.D. Cal. 2009), *aff'd*, 658 F.3d 1150 (9th Cir. 2011); *Facebook, Inc. v. Power Ventures*, *Inc.*, 252 F. Supp. 3d 765, 786 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019). And courts require more—ongoing reporting, disclosure, or audit—where certification alone will not secure compliance. *See, e.g.*, *Hernandez v. Cnty. of Monterey*, 2023 WL 6299863, at *16 (N.D. Cal. Sept. 26, 2023) (requiring defendants to grant access to independent monitors who submitted periodic reports of compliance with the court order); *Parsons v. Ryan*, 2018 WL 3239691, at *12 (D. Ariz. June 22, 2018) (requiring defendant to file monthly reports reflecting every instance of noncompliance), *aff'd*, 949 F.3d 443 (9th Cir. 2020); *California v. Del Rosa*, 2025 WL 2808444, at *4 (E.D. Cal. Oct. 2, 2025) (requiring defendant to submit all purchase and sales records to plaintiff biweekly to ensure compliance, with $10,000-per-day penalty for noncompliance with reporting schedule). The additional disclosure is warranted here, where NSO's operations are built on concealment and its prior sworn assurances have not held up.

A certification of compliance should not end the matter if it later proves inaccurate. The Court should provide that, if NSO certifies compliance and the Court later finds NSO was not in compliance during any period in which the contempt order was in effect, the per diem sanction accrues for that period at the level the doubling schedule had then reached. Because the order and its escalating sanction will be in place throughout, NSO will have notice of the precise consequence of noncompliance, and accrual for a period of concealed noncompliance is thus a permissible coercive remedy. *See Taggart*, 587 U.S. at 561. This denies NSO any benefit from a premature or inaccurate compliance claim: a certification that halts accrual, followed by a finding of continued violation, restores the sanction as if accrual had never stopped.

B. Compensatory Sanctions

Compensatory contempt relief covers the costs the moving party has incurred as a result of the contempt, including attorneys' fees for the contempt motion itself. *Perry v. O'Donnell*, 759 F.2d 702, 705-06 (9th Cir. 1985). Plaintiffs request that the Court order NSO to pay Plaintiffs' reasonable attorneys' fees and costs incurred in bringing this motion. *See U2 Home Ent.*, 2006 WL 1581943, at *1 (ordering defendants to "pay attorney's fees and costs in connection with plaintiff's prosecution of the instant [civil contempt] motion"). Plaintiffs will submit a supplemental declaration quantifying those costs if the Court grants this motion.

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court find NSO in contempt of the permanent injunction, impose coercive sanctions in the form of a per diem fine, doubling periodically as set forth above, and award compensatory sanctions covering Plaintiffs' attorneys' fees and costs.

Dated: June 8, 2026

Respectfully Submitted,

DAVIS POLK & WARDWELL LLP

By: */s/ Micah G. Block*

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

Micah G. Block (SBN 270712)
DAVIS POLK & WARDWELL LLP
900 Middlefield Road, Suite 200
Redwood City, California 94063
Telephone: (650) 752-2000
Facsimile: (650) 752-2111
Email: micah.block@davispolk.com

Attorneys for Plaintiffs
WhatsApp LLC and Meta Platforms, Inc.