Greg D. Andres
Antonio J. Perez-Marques
Gina Cora
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
gina.cora@davispolk.com
craig.cagney@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 PERMANENT INJUNCTION** Date: April 10, 2025 Time: 9:30 am Ctrm: 3 Judge: Hon. Phyllis J. Hamilton Action Filed: October 29, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES & RULES

OTHER AUTHORITIES

NOTICE OF MOTION AND MOTION FOR PERMANENT INJUNCTION

PLEASE TAKE NOTICE THAT, on April 10, 2025 at 9:30 a.m. in Courtroom 3 of the U.S. District Court for the Northern District of California, Plaintiffs WhatsApp LLC ("WhatsApp") and Meta Platforms, Inc. ("Meta," and together with WhatsApp, "Plaintiffs") will and hereby do move for a permanent injunction. This Motion is based upon this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, the Declaration of Micah G. Block in Support of Plaintiffs' Motion ("Block Decl.") 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 December 20, 2024, this Court held Defendants NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. (together, "NSO") liable for violating the Computer Fraud and Abuse Act ("CFAA") and the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), and for breaching the WhatsApp Terms of Service. Dkt. No. 494 at 10–15. Plaintiffs now move for a permanent injunction to ensure that NSO does not continue these violations.

NSO spent years violating the WhatsApp Terms of Service in almost every conceivable way and, in the process, violated the CFAA and the CDAFA, all in furtherance of targeting WhatsApp users. To gain access to Plaintiffs' servers and to users' devices, NSO reverse-engineered WhatsApp code to build a modified version of the WhatsApp client application, which NSO called the WhatsApp Installation Server ("WIS"). *Id*. at 2, 14. NSO used the WIS to create messages that concealed malicious code and sent those messages through WhatsApp servers. Those messages were ultimately used to install Pegasus on target devices. And NSO expended significant resources to evade detection and circumvent Plaintiffs' security updates that repeatedly blocked NSO's illegal conduct. *Id*. at 12.

NSO's violations of the computer hacking laws and breaches of the WhatsApp Terms of Service give rise to irreparable harm that goes beyond the money damages that NSO should pay. And the evidence establishes that NSO—[redacted]. Dkt. No. 399-4, Ex. 6 at 83:10–

11. NSO's business model is to develop and license covertly installed spyware, and there is no reason to believe it will stop trying to circumvent Plaintiffs' security measures. In fact, discovery revealed that NSO continued to attack Plaintiffs' servers *after* Plaintiffs filed this lawsuit. And after this Court's summary judgment ruling, NSO's founder publicly stated that "justice was not served" in this case and that the Court's ruling "doesn't prove that we did anything wrong, because we really didn't." Block Decl., Ex. A (Vas Panagiotopoulos, *NSO Group Owner: "We Will Appeal, Justice Was Not Served"*, Substack (Jan. 8, 2025), https://vaspanagiotopoulos.substack.com/p/nso-group-owner-we-will-appeal-justice) at 1–2. Without a meaningful permanent injunction, any damages awarded risk being little more than a speeding ticket for NSO, insufficient to halt its illegal activity.

Based on its ruling finding NSO liable, the Court should prohibit NSO and its related parties[1] from: (a) using Plaintiffs' Platforms[2] in any way, including as an installation vector; (b) emulating Plaintiffs' Platforms, including by using the WIS; (c) collecting data from Plaintiffs' Platforms; (d) reverse-engineering or decompiling Plaintiffs' Platforms; (e) sending harmful code through Plaintiffs' Platforms; (f) using Plaintiffs' Platforms for illegal purposes; and (g) creating accounts on Plaintiffs' Platforms. The Court should also order NSO to delete all computer code that uses Plaintiffs' Platforms and all information improperly obtained from Plaintiffs and Plaintiffs' users, and cut off customer access to the same. NSO should also affirm its compliance with the injunction by filing a certification on the public docket of this action.

Because the Court already found that NSO conducted the activities covered by the proposed injunction, there is no additional evidence required to evaluate Plaintiffs' request and there are no obstacles to issuing a permanent injunction now. If the Court grants Plaintiffs' request for injunctive relief, Plaintiffs ask that the Court order the parties back to mediation with Magistrate Judge Kim so

---

[1] Specifically, consistent with Federal Rule of Civil Procedure 65, the proposed injunction binds NSO; NSO's officers, agents, servants, employees, and attorneys; and all other persons who are in active concert or participation with NSO and NSO's officers, agents, servants, employees, and attorneys. *See* Proposed Order § 1.

[2] The proposed injunction defines "Plaintiffs' Platforms" as Plaintiffs' computer systems and platforms, which include but are not limited to the WhatsApp, Facebook, Instagram, Messenger, Meta AI, Threads, and Meta Horizon platforms, as well as each of those platforms' related client applications. *See* Proposed Order § 2.

that the parties may attempt to reach an agreement on the proper monetary award in order to avoid the need for a jury trial.

BACKGROUND

A. Plaintiffs Discover NSO's Attack in May 2019

[redacted] *See* Dkt. No. 400-2, Ex. 4 at 210:6–8. [redacted] *See id*., Ex. 4 at 274:6–8; Dkt. No. 437-2, Ex. 39 at 200:4–11. [redacted] *See* Dkt. No. 400-2, Ex. 4 at 272:7–17. On October 29, 2019, Plaintiffs filed a complaint against NSO alleging, among other things, violations of the CFAA, the CDAFA, and breach of contract for violating the WhatsApp Terms of Service. *See* Dkt. No. 1. Plaintiffs' complaint requested that the Court enter a permanent injunction against NSO. *Id*. at 14.

B. NSO Asserts That the Only Relevant Conduct Took Place in April and May 2019

In moving to dismiss Plaintiffs' request for injunctive relief on June 24, 2020, NSO argued that Plaintiffs were unlikely to face any future injury because NSO had stopped attacking Plaintiffs' servers. Dkt. No. 105 at 1–3. NSO opened its motion by stating: "For approximately 40 days in Spring 2019—from April 2019 to May 13, 2019—Plaintiffs allege that an NSO technology called Pegasus used a single vulnerability in WhatsApp's services to send messages to around 1,400 WhatsApp users. *And since May 13, 2019? Nothing.*" *Id*. at 1 (emphasis added); *see also* Dkt. No. 110 at 5 n.3 ("The alleged 'probing [of] Plaintiffs' servers and software' and 'selling products designed to exploit them' all occurred in the past and are not alleged to be ongoing.").

Later, in opposing Plaintiffs' discovery requests, NSO argued that the only conduct relevant to Plaintiffs' claims took place in April and May 2019. *See* Dkt. No. 184-2 at 17–18. Yaron Shohat, NSO's chief executive officer, declared under oath that [redacted] Dkt. No. 176-3 ¶ 8. Relying on Mr. Shohat's declaration, NSO argued that [redacted] Dkt. No. 184-2 at 20. Based

in part on these assertions, NSO was only ordered to produce documents about its conduct in the period from April 29, 2018, to May 10, 2020. Dkt. No. 292 at 4.[3]

C. Discovery Shows That NSO Attacked Plaintiffs Before April 2019, and Continued to Attack Plaintiffs After May 2019

Discovery showed that the scale and scope of NSO's illegal conduct was greater than suggested by NSO's arguments. [redacted] Dkt. No. 399-4, Ex. 6 at 76:12–22. Around this time, NSO [redacted]. *Id.*, Ex. 6 at 70:2–15, 226:17–227:14.[4] Based on this research, NSO developed [redacted] *Id.*, Ex. 6 at 155:1–164:9. NSO began [redacted] *Id.*, Ex. 6 at 76:12–22, 87:9–18.

[redacted] *See id.*, Ex. 1 at 37–38; Dkt. No. 399-2 at 4. [redacted] *See* Dkt. No. 399-4, Ex. 6 at 254:14–17, 256:23–25; *id.*, Ex. 9. All this activity took place well before the May 2019 time period that NSO had argued was exclusively at issue in the litigation.

In response to these changes, [redacted] *Id.*, Ex. 6 at 256:16–22. [redacted] *See id.*, Ex. 10 at 69:17–18.

[3] As further detailed in Plaintiffs' motion for sanctions, NSO not only refused to produce all responsive documents within that timeframe, but also improperly refused to allow its witnesses to answer questions about NSO's conduct outside of this timeframe. *See* Dkt. No. 405-2 at 14–15.

[4] The WhatsApp Terms of Service expressly prohibit "decompil[ing]" and "reverse engineer[ing]." Dkt. No. 401-2, Ex. 11 at 3.

[redacted] *Id.*, Ex. 14 at 2. [redacted] *See, e.g.*, *id.*, Ex. 15 at 2. On October 29, 2019, Plaintiffs filed this lawsuit. Dkt. No. 1. By [redacted] Dkt. No. 399-4, Ex. 6 at 266:23–267:4.

Throughout the course of discovery, NSO categorically refused to produce documents outside of the April 2018 to May 2020 timeframe and instructed its witnesses not to answer deposition questions about NSO's conduct outside this period. *See* Dkt. No. 405-2 at 14–15. For this reason, [redacted] Dkt. No. 399-4, Ex. 6 at 47:1–6. [redacted] *Id.*, Ex. 10 at 49:19–21.

D. Procedural History

On December 20, 2024, the Court granted Plaintiffs' motion for partial summary judgment and Plaintiffs' motion for evidentiary sanctions. Dkt. No. 494. In its order, the Court found NSO violated the CFAA by "sen[ding] messages through Whatsapp servers that caused Pegasus to be installed on target users' devices," and that the WIS then obtained information by "having it sent from the target users, through the What[s]app servers, and back to the WIS." *Id.* at 12–13. The Court found that this information was valuable because of "defendants' clients' willingness to pay for Pegasus," and that NSO possessed the requisite intent because it "redesigned Pegasus to evade detection after plaintiffs first fixed the security breach." *Id.* at 12. The Court rejected NSO's arguments that it was not liable because (according to NSO) its customers operated Pegasus, and the Court explained that Section 1030(b) of the CFAA assigns liability to co-conspirators. *Id.* at 13. The Court held that NSO violated the CDAFA "for the same reasons as the CFAA claim." *Id.* Finally, the Court held NSO was liable on Plaintiffs' breach of contract claim. *Id.* at 14–15. The Court scheduled a damages-only trial, which is set to begin on April 28, 2025. *See* Dkt. No. 540.

On December 24, 2024, just four days after the Court held NSO liable, Omri Lavie—NSO's co-founder, chairman, and current majority owner—publicly denounced the Court's ruling, stating, "I believe that justice was not served . . . [the Court's ruling] doesn't prove that we did anything wrong, because we really didn't." Block Decl., Ex. A at 1–2.

On January 22, 2025, the parties participated in mediation with Magistrate Judge Kim, but were unable to reach a resolution on damages or the scope of an injunction. Block Decl. ¶ 3. On February 3, 2025, Plaintiffs informed NSO that they intended to move for a permanent injunction based on the Court's summary judgment ruling. *Id.* ¶ 4. On February 7, 2025, Plaintiffs sent NSO the provisions of the proposed injunction that Plaintiffs would seek. *Id.* ¶ 5. Counsel for the parties met-and-conferred on Plaintiffs' proposal on February 10, 2025. *Id.* ¶ 6. On February 12, 2025, NSO refused to agree to these terms. *Id.* ¶ 7. Given the fundamental differences that exist between the parties on the issue of injunctive relief, and the ongoing threat Plaintiffs face from NSO, Plaintiffs now move for a permanent injunction.

LEGAL STANDARD

The CFAA allows "[a]ny person who suffers damage or loss by reason of a violation of" the CFAA to "maintain a civil action against the violator to obtain . . . injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). The CDAFA likewise allows "the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions" of the CDAFA to "bring a civil action against the violator for . . . injunctive relief or other equitable relief." Cal. Penal Code § 502(e)(1). Under California law, "a final injunction may be granted to prevent the breach of an obligation existing in favor of the applicant." Cal. Civ. Code § 3422; *see Deerpoint Grp., Inc. v. Agrigenix, LLC*, 345 F. Supp. 3d 1207, 1225–26 (E.D. Cal. 2018) (recognizing availability of injunctive relief "as part of a breach of contract/settlement claim").

Although both federal and state law authorize injunctive relief here, the Court must nonetheless "ensure that the relief comports with 'the traditional principles governing equitable remedies in federal courts.'" *Epic Games, Inc. v. Apple, Inc.*, 67 F.4th 946, 1002 (9th Cir. 2023) (quoting *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020)), *cert. denied*, 144 S. Ct. 681 (2024),

and cert. denied, 144 S. Ct. 682 (2024). Under these principles, a prevailing plaintiff is entitled to a permanent injunction if it can show that: (1) it has suffered an irreparable injury; (2) remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction. *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006). In evaluating irreparable injury, the Court should consider the risk of future harm. *See Y.Y.G.M. SA v. Redbubble, Inc.*, 75 F.4th 995, 1007 (9th Cir. 2023) ("The district court abused its discretion by discounting the relevance of future harm."), *cert. denied*, 144 S. Ct. 824 (2024). Because the "irreparable injury requirement for a permanent injunction overlaps with lack of an adequate remedy at law," *Rocawear Licensing, LLC v. Branco Enters., Inc.*, 2009 WL 10703523, at *9 (C.D. Cal. July 22, 2009) (citation omitted), courts often discuss them together, *see, e.g.*, *City & Cnty. of S.F. v. Trump*, 897 F.3d 1225, 1243 (9th Cir. 2018).

ARGUMENT

I. Plaintiffs Are Entitled to Injunctive Relief

Plaintiffs satisfy all four factors for awarding permanent injunctive relief. The Court has already found that there is no genuine dispute of material fact that NSO violated the CFAA, the CDAFA, and the WhatsApp Terms of Service. *See* Dkt. No. 494. The undisputed facts likewise show that Plaintiffs face irreparable harm that monetary damages cannot redress based on the threat of NSO's ongoing and future attacks against Plaintiffs' computers, client applications, and users. The hardship that Plaintiffs face from NSO's illegal behavior outweighs any interest that NSO has in continuing to violate the law. An evaluation of the public interest also warrants enjoining NSO from violating the law, as the record lacks any evidence that NSO's attacks on Plaintiffs' computers benefited the public in any way.

A. Plaintiffs Suffered Irreparable Injury for Which Monetary Damages Are Insufficient

Plaintiffs have established irreparable injury for which monetary damages are inadequate. As other courts in this district have concluded, violations of federal and state computer hacking laws give rise to irreparable harm. Moreover, NSO poses an ongoing and prospective threat to Plaintiffs'

security and the privacy of Plaintiffs' users. Not only did NSO refuse to stop its illegal conduct after Plaintiffs filed this lawsuit, but it also affirmatively invested in solutions to circumvent Plaintiffs' security measures, thus heightening the risk to Plaintiffs. NSO still possesses all the computer code that enabled it to attack Plaintiffs' servers and collect data from Plaintiffs' users, and NSO therefore remains capable of launching a new attack. Without an injunction, Plaintiffs will have to expend resources investigating and mitigating NSO's conduct, including by bringing additional cases—one of the harms that an injunction would prevent.

1. NSO's Violations of the CFAA and the CDAFA Establish Irreparable Harm

The Court's findings about NSO's past conduct alone establish that Plaintiffs have suffered irreparable harm. As described above, the Court's decision holding NSO liable for violating the CFAA and the CDAFA found that NSO hacked into WhatsApp servers so that NSO's Pegasus spyware could be covertly installed on the mobile devices of WhatsApp users. Dkt. No. 494 at 12–13. It is well-established that "some qualitative feature" about certain *past* illegal conduct can "elevate its status into the realm of 'irreparable harm.'" *Elohim EPF USA, Inc. v. Aceplus, Inc.*, 2015 WL 13753299, at *9 (C.D. Cal. Jan. 2, 2015) (citing *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 518 F. Supp. 2d 1197, 1215 (C.D. Cal. 2007)).

Computer hacking falls within this category, and "[n]umerous courts have found that unauthorized access of computers and the acquisition of data . . . constitute irreparable harm." *Facebook, Inc. v. Power Ventures, Inc.*, 252 F. Supp. 3d 765, 782 (N.D. Cal. 2017), *aff'd*, 749 F. App'x 557 (9th Cir. 2019). In *Power Ventures*, the court found that Facebook was irreparably harmed by the defendant's past violations of the CFAA and the CDAFA, which "interfered with Facebook's right to control access to its own computers." 252 F. Supp. 3d at 782; *see also, e.g.*, *Meta Platforms, Inc. v. Nguyen*, 2023 WL 8686924, at *10 (N.D. Cal. Nov. 21, 2023) (finding that defendant's violations of CDAFA gave rise to irreparable injury even where defendant's "account takeover scheme" was stopped more than two years earlier); *Meta Platforms, Inc. v. Ates*, 2023 WL 4035611, at *2, 8 (N.D. Cal. May 1, 2023) (finding that defendant's violations of CDAFA gave rise to irreparable injury, even when defendant "represented that he had stopped all activity"), *report and recommendation adopted*, 2023 WL 4995717 (N.D. Cal. June 27, 2023); *Enargy Power Co. v. Wang*, 2013 WL

6234625, at *10 (D. Mass. Dec. 3, 2013) (finding irreparable harm for CFAA violation that "has prevented [plaintiff] from enjoying the uninterrupted use of its property"). Even without examining the undisputed facts about NSO's likelihood of ongoing and future violations, the findings of fact as to NSO's past violations suffice to establish that Plaintiffs have suffered irreparable harm.

2. Without an Injunction, Plaintiffs Face a Risk of Future Harm

There is no evidence that NSO will stop its illegal conduct without a court ordering it to do so. To the contrary, [redacted] *See* Dkt. No. 399-4, Ex. 6 at 271:3–8. Though NSO has refused to provide discovery about its actions post-dating May 2020, the undisputed evidence leaves little doubt that NSO would continue its misconduct without an injunction. Just days after being found liable on all of Plaintiffs' claims, NSO confirmed its total lack of remorse, publicly stating that it did not "d[o] anything wrong" and maintaining that its illegal conduct was "important and essential." *See* Block Decl., Ex. A at 2–3. This current and future threat gives rise to irreparable harm that cannot be redressed with monetary damages.

"Generally, 'absent a great public injury, a permanent injunction will be granted when liability has been established and there is a threat of a continuing violations.'" *Michael Grecco Prods., Inc. v. 8 Decimal Cap. Mgmt., LLC*, 2021 WL 2534567, at *6 (N.D. Cal. June 1, 2021) (quoting *Michael Grecco Prods., Inc. v. WrapMarket, LLC*, 2017 WL 10434020, at *4 (C.D. Cal. Nov. 8, 2017)), *report and recommendation adopted*, 2021 WL 2531093 (N.D. Cal. June 21, 2021); *Adobe Sys., Inc. v. Taveira*, 2009 WL 506861, at *7 (N.D. Cal. Feb. 27, 2009) ("[I]f plaintiff has demonstrated a significant threat of future violations this Court will recommend that the injunction issue."). Here, at least four independent bases demonstrate a significant threat of ongoing and future violations.

The nature of NSO's business. All the facts in the record suggest that NSO will continue to look for ways to install Pegasus on target devices, without regard that such conduct violates the CFAA, the CDAFA, and the WhatsApp Terms of Service. [redacted] *See, e.g.*, Dkt. No. 396-3 ¶ 3; Dkt. No. 396-5, Ex. H at 233:5–7. Though NSO refused to provide any computer code for use in this litigation, let alone to show how Pegasus operates

today, Mr. Gazneli confirmed that [redacted] Dkt. No. 399-4, Ex. 6 at 109:3–110:22.

NSO also maintains a research-and-development team that searches for new covert installation vectors. NSO's research-and-development team [redacted] *Id.*, Ex. 6 at 266:3–7. As Mr. Gazneli puts it, [redacted] *Id.*, Ex. 6 at 266:10. Mr. Shohat even went as far as [redacted] *Id.*, Ex. 10 at 49:19–21.

NSO's rapid response to Plaintiffs' own security fixes demonstrate just how quickly NSO will attempt to circumvent any technical restriction that it faces. [redacted] *Id.*, Ex. 9 at 1. [redacted] *Id.*, Ex. 6 at 257:6–21. NSO's ability to quickly circumvent sophisticated technical obstacles exemplifies what one of NSO's own employees saw as the company's greatest strength: [redacted] *Id.*, Ex. 14 at 2.

NSO's post-complaint conduct. The filing of this lawsuit did not deter NSO from continuing to access Plaintiffs' servers in violation of federal and state law, confirming that NSO will continue its misconduct without a stronger sanction. Plaintiffs closed the [redacted] installation vector on May 12, 2019, and filed their complaint against NSO on October 29, 2019. *See* Dkt. No. 1. Unbeknownst to Plaintiffs, [redacted] *See* Dkt. No. 399-4, Ex. 6 at 266:11–22. NSO admitted that "[redacted] *Id.*, Ex.

6 at 271:3–8. [redacted] [redacted] *Id.*, Ex. 6 at 267:5–268:16.

In the specific context of unlawful computer access, "courts in this district . . . have granted injunctive relief upon a showing that a defendant continued to access a plaintiff's computers, in an unauthorized manner, regardless of [a victim's] attempts to halt the access." *Chegg, Inc. v. Doe*, 2023 WL 7392290, at *8 (N.D. Cal. Nov. 7, 2023). The plaintiff in *Chegg* demonstrated that there was a likelihood of irreparable harm from defendants who responded to cease-and-desist letters by conducting another cyberattack against the plaintiff. *Id.* Similarly, in *Power Ventures*, the defendant's historical conduct made it "very likely" that they would "they w[ould] not easily be deterred" and would "again attempt to access Facebook's servers without authorization . . . unless they [we]re strongly deterred," making it "very likely that in the absence of a permanent injunction, Facebook will suffer irreparable harm again in the future." 252 F. Supp. 3d at 782–83. The "high probability that Defendants will repeat their illegal conduct" also establishes that "money damages are inadequate to compensate for [Plaintiffs'] injury." *Id.* at 783–84; *see also Craigslist, Inc. v. Kerbel*, 2012 WL 3166798, at *16 (N.D. Cal. Aug. 2, 2012) (finding that an award of damages would not prevent future harm based on defendant's refusal to respond to cease-and-desist letters and existing website); *Facebook, Inc. v. Grunin*, 77 F. Supp. 3d 965, 973 (N.D. Cal. 2015) ("Even after two cease-and-desist letters, Grunin continued to fraudulently obtain Facebook accounts and to access Facebook's services."). Here, NSO not only refused to change its conduct after being named in Plaintiffs' lawsuit, but also affirmatively invested in new ways to access Plaintiffs' servers while litigating this case. And now, after being found liable, NSO publicly denounced this Court's ruling and essentially committed to continue its unlawful conduct. *See* Block Decl., Ex. A at 2 ("Certainly, it doesn't prove that we did anything wrong, because we really didn't.").

NSO's inability to show that it halted its misconduct. Nothing in the limited evidence NSO produced or the deposition questions it answered suggests that it no longer accesses or uses WhatsApp and Plaintiffs' other technologies today. NSO generally refused to provide discovery post-dating May 2020. In particular, NSO's executives refused to answer deposition questions about the company's current operations. For example, Mr. Gazneli refused to disclose [redacted]

[redacted] Dkt. No. 399-4, Ex. 6 at 63:4–7. Mr. Shohat similarly refused to answer whether NSO "[redacted] *Id.*, Ex. 10 at 49:25–50:5. The Court has already ruled that NSO should face "evidentiary sanctions when appropriate," Dkt. No. 494 at 9, and NSO should not be entitled to favorable inferences about its current conduct—especially without producing any supporting evidence—now that it has flouted its discovery obligations.

The widespread use of Plaintiffs' products. Plaintiffs' products remain an appealing target for NSO's spyware. WhatsApp's popularity means that it is downloaded on billions of mobile devices around the world, [redacted]. *See* Dkt. No. 399-4, Ex. 24 at 1 ([redacted] Even putting aside potential targets' use of the WhatsApp application, and NSO's misuse of WhatsApp as an installation vector, NSO will likely continue to test and demonstrate its products to its clients vis-à-vis Plaintiffs' Platforms, all in violation of the CFAA, the CDAFA, and the WhatsApp Terms of Service. *See id.*, Ex. 8 at 270:1–7 ([redacted]).[5] For these reasons, Plaintiffs face a particularized risk that their infrastructure and users will again be targeted by NSO's illegal conduct.

3. NSO Still Possesses the Technologies Used to Access Plaintiffs' Servers and Install Spyware on Target Devices

In addition to the likelihood of ongoing or future attacks, Plaintiffs are likely to suffer irrep-

[5] Even accepting NSO's unsubstantiated position that its customers are responsible for its misconduct, NSO's "brazen plans to continue trafficking in" products that violate the law provides "evidence of irreparable harm," as "such trafficking has induced and would continue to induce third parties—namely, [NSO] customers" to violate the law, which "would result in the same harms" to Plaintiffs. *Apple Inc. v. Psystar Corp.*, 673 F. Supp. 2d 943, 949 (N.D. Cal. 2009) (finding "this factor tilts heavily towards granting injunctive relief"), *aff'd*, 658 F.3d 1150 (9th Cir. 2011). The murky relationship between NSO and its customers, which NSO has pointedly blocked from discovery, therefore provides no reason to withhold a permanent injunction.

arable harm that cannot be addressed by monetary damages because NSO still retains all the technology, infrastructure, and spyware that led to the current litigation. For example, NSO has [redacted] *See* Dkt. No. 399-4, Ex. 6 at 226:12–24 ([redacted]); *id.*, Ex. 6 at 143:7–13 ([redacted]"); *id.*, Ex. 6 at 161:22–23 ("[redacted]"); *id.*, Ex. 6 at 189:23–24 ("[redacted]"). There is no evidence that NSO has deleted the WIS, despite the fact that it was created in violation of the WhatsApp Terms of Service and used to violate the CFAA and the CDAFA. Similarly, NSO maintains control over Pegasus and the installation vectors it uses to install Pegasus on target devices. *See* Dkt. No. 419-2 at 18–19 (describing NSO's purported oversight of Pegasus's use).

Courts have found a defendant's retention of the software used to illegally collect data established irreparable harm and formed the basis to issue an injunction. In *Facebook, Inc. v. Sluchevsky*, a court in this district entered a permanent injunction against defendants who developed software that obtained data from users in violation of the CFAA, the CDAFA, and their contract with Facebook. 2020 WL 5823277, at *1 (N.D. Cal. Aug. 28, 2020), *report and recommendation adopted*, 2020 WL 5816578 (N.D. Cal. Sept. 30, 2020). The *Sluchevsky* court found that the irreparable harm requirement was met because, among other things, "defendants retain the software, tools or means at issue to continue their harmful behavior." *Id*. at *9. Similarly, in *Power Ventures*, the court noted that the defendants "may still possess the software at issue in this litigation and the data illegally acquired from Facebook," which demonstrated the inadequacy of monetary damages, especially given the defendants' history of illegal conduct. 252 F. Supp. 3d at 783. Without forcing NSO to delete the WIS, which it made by violating the WhatsApp Terms of Service, and enjoining NSO from recreating such a technology, NSO can continue to identify new ways to attack Plaintiffs' computers.

4. Plaintiffs Will Likely Be Forced to File Multiple Lawsuits to Stop NSO's Misconduct

The overwhelming evidence of NSO's past misconduct, its likelihood of ongoing and future misconduct, and its retention of its spyware tools all signal that Plaintiffs will be forced to file future lawsuits against NSO if the Court does not enter an injunction now, which provides another basis for finding irreparable harm that cannot be addressed with monetary damages. Courts have found that monetary damages for past misconduct are insufficient to compensate plaintiffs for ongoing and future costs to prosecute such violations. *See United Nat'l Maint., Inc. v. San Diego Convention Ctr. Corp.,* 2012 WL 3861946, at *7 (S.D. Cal. Sept. 5, 2012) ("Where the plaintiff will have to litigate multiple suits in the future, monetary damages are deemed to be insufficient and thus, an injunction may issue."); *Metro-Goldwyn-Mayer Studios*, 518 F. Supp. 2d at 1219 (holding that "the very need to file multiple lawsuits as a consequence of [defendant's misconduct] is itself supporting of an irreparable harm finding").

Here, NSO's business, its conduct after Plaintiffs brought suit, and its statements about its ongoing activities—paired with the widespread use of Plaintiffs' applications—show the likelihood of ongoing and future harm. Forcing Plaintiffs to bring new legal actions every time they discover one of NSO's violations, and forcing Plaintiffs to surmount the obstacles that NSO has constructed in this litigation, would be an inadequate alternative to entering a permanent injunction. Without an injunction, Plaintiffs will be forced to sue NSO again and again to stop NSO's illegal activity. This provides yet another reason to enter the proposed injunction.

5. NSO's Evasive Tactics Would Force Plaintiffs to Spend Additional Resources Detecting Future Unauthorized Activity by NSO

Plaintiffs face additional irreparable injury because NSO has demonstrated a history of attempting to evade detection, creating a serious risk that Plaintiffs will be forced to expend resources monitoring, discovering, and remediating NSO's constant efforts to identify and use exploits on Plaintiffs' services. This too provides a reason to enjoin NSO from future misconduct.

Other courts have concluded that a defendant's breach of online terms of use justifies a permanent injunction where the defendant has demonstrated an ability to evade detection. *See Google,*

Inc. v. Jackman, 2011 WL 3267907, at *5–6 (N.D. Cal. July 28, 2011). In *Jackman*, the defendants had violated Google's advertising terms, and the court held that a permanent injunction was necessary in light of the defendants' prior attempts to "evade detection," including by "using different names and false contact information, even after their original accounts were suspended." *Id.* at *1. The court explained that, without an injunction, "Google will need to expend further resources to discover and eliminate Defendants' improper advertising," and that "Defendants' violations of the Ad Terms will persist unless they are prohibited from" evading Google's automatic monitoring systems. *Id.* at *5; *see also Power Ventures*, 252 F. Supp. 3d at 783 (granting injunction where defendants showed propensity to use "tactics to circumvent plaintiff's security measures") (citation omitted); *Disney Enters., Inc. v. Delane*, 446 F. Supp. 2d 402, 408 (D. Md. 2006) ("[T]here is no way to know how many times this content has been accessed and downloaded. . . . [B]ecause of the nature of [defendant's] Web site and trackers, further infringements are a continuing threat, making remedies at law insufficient to compensate for Plaintiffs' injuries.").

NSO's use of detection-evading strategies is undisputed. [redacted]. *See, e.g.*, Dkt. No. 399-4, Ex. 24 at 2 ([redacted]). As described in Plaintiffs' motion for summary judgment, [redacted] *See id.*, Ex. 6 at 298:12–21. [redacted] *See id.*, Ex. 25 at 8–10 ([redacted]). [redacted], *see, e.g.*, *id.*, Ex. 24 at 4 ([redacted], *id.*, Ex. 6 at 236:8–237:1; *see, e.g.*, Dkt. No. 436-4, Ex. 41 at 1 [redacted]

Similarly, NSO took steps to avoid having its exploits linked back to NSO or its customers. [redacted]

[redacted] Dkt. No. 399-4, Ex. 8 at 17:13–23; *see id.*, Ex. 17 ([redacted]). In addition, NSO would [redacted]. *Id.*, Ex. 8 at 18:15–17 [redacted]

The secretive nature of NSO's conduct heightens the risk that Plaintiffs will have to devote significant resources to monitoring and investigating NSO. Mr. Shohat admitted that [redacted] *Id.*, Ex. 10 at 49:13–18. Mr. Shohat further admitted that NSO [redacted] Dkt. No. 436-4, Ex. 38 at 189:15–16.

In addition to its refusal to disclose details about its installation vectors, NSO affirmatively maintains an [redacted] Dkt. No. 399-4, Ex. 6 at 232:7–12. To NSO, [redacted]. *Id.*, Ex. 24 at 1. Despite having advanced knowledge of WhatsApp's technical defenses, [redacted] *See id.*, Ex. 6 at 223:24–224:3. Presented with all this evidence, the Court found that NSO possessed an intent to defraud by continuing to attempt to evade WhatsApp's technical restrictions, Dkt. No. 494 at 12, and courts may consider "the degree of scienter involved" in determining whether there is a "cognizable danger of recurrent violations." *United States v. Laerdal Mfg. Corp.*, 73 F.3d 852, 855 (9th Cir. 1995). NSO's intentional and considered deception makes it likely it will continue to violate the law in the absence of an injunction.

Just as it tried to evade Plaintiffs' technical barriers, NSO tried to hide its ongoing misconduct from the Court. For instance, NSO moved to dismiss Plaintiffs' claims for injunctive relief in 2020,

disingenuously suggesting its access to Plaintiffs' servers was limited to a two-week period. Dkt. No. 105 at 2 ("And since May 13, 2019? Nothing."). Based on this assertion, NSO later argued that the Court should impose a narrow discovery window. *See* Dkt. No. 176-2 at 13. What's more, NSO improperly instructed its witnesses to refuse to answer questions about its current conduct, in order to conceal its ongoing activities from Plaintiffs and from the Court. *See* Dkt. No. 405-2 at 14–15. All the while, [redacted] *See* Dkt. No. 399-4, Ex. 6 at 271:3–8 ("[redacted]").

NSO is the paradigmatic defendant that, having "frequently exhibited bad faith conduct that indicates that they will not easily be deterred from attempting to access Facebook's servers without authorization in violation of the CFAA and § 502," should be subject to a permanent injunction. *Power Ventures*, 252 F. Supp. 3d at 782; *see also Bd. of Trs. of Bay Area Roofers Health & Welfare Tr. Fund v. Westech Roofing*, 2014 WL 4383062, at *4 (N.D. Cal. Sept. 4, 2014) (entering permanent injunction, noting that "long history of non-compliance in the face of multiple court orders . . . reflects bad faith . . . and makes clear that legal remedies are not adequate as to this Defendant."). Because NSO employs tactics that make it difficult to detect its behavior, and has not been forthcoming about the extent of its activity, it would be especially inequitable to require Plaintiffs to file a new lawsuit each time NSO violates the CFAA, the CDAFA, or the WhatsApp Terms of Service.

B. The Balance of Hardships Weighs in Favor of Injunctive Relief

The balance of hardships weighs in favor of granting Plaintiffs injunctive relief. The substantial and irreparable harm Plaintiffs will continue to suffer far outweighs any potential harm to NSO, which has willfully and repeatedly violated the CFAA, the CDAFA, and the WhatsApp Terms of Service for years. Plaintiffs face the real threat of ongoing harm given the "probability that [NSO] will engage in similar conduct in the future" and NSO's continued refusal to accept the Court's finding of liability. *See Power Ventures*, 252 F. Supp. 3d at 784 (finding that balance of hardships favored plaintiff).

In contrast, NSO "will suffer no harm from being unable to develop software to engage in illegal conduct." *Id*. at 785; *see also Deckers Outdoor Corp. v. Ozwear Connection Pty Ltd.*, 2014 WL 4679001, at *13 (C.D. Cal. Sept. 18, 2014) ("There is no hardship to a defendant when a permanent injunction would merely require the defendant to comply with law."). As described below, the proposed injunction targets NSO's access to Plaintiffs' computers and client applications, and NSO's schemes to find potential vulnerabilities in Plaintiffs' code—all of which violates federal and state law and/or the WhatsApp Terms of Service.

C. An Injunction Is in the Public Interest

Public interest is served by ensuring compliance with the law. In passing the CFAA and the CDAFA, Congress and the California State Legislature responded to the problem of "hackers hatch[ing] ways to coopt computers for illegal ends." *Van Buren v. United States*, 593 U.S. 374, 378 (2021); *see Golden Gate Rest. Ass'n v. City & Cnty. of S.F.*, 512 F.3d 1112, 1127 (9th Cir. 2008) ("The public interest may be declared in the form of a statute" (quoting Charles Alan Wright et al., *Federal Practice and Procedure* § 2948.4, at 207 (2d ed. 1995)). The public has an interest in ensuring these laws are followed, and that those who violate them are stopped.

In addition, the Ninth Circuit has recognized that "Internet companies and the public do have a substantial interest in thwarting denial-of-service attacks and blocking abusive users, identity thieves, and other ill-intentioned actors." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1202 (9th Cir. 2022). Along the same lines, this Court has recognized that "Facebook's ability to decisively police the integrity of its platforms is without question a pressing public interest. In particular, the public has a strong interest in the integrity of Facebook's platforms, Facebook's policing of those platforms for abuses, and Facebook's protection of its users' privacy." *Stackla, Inc. v. Facebook Inc.*, 2019 WL 4738288, at *6 (N.D. Cal. Sept. 27, 2019). NSO's attack not only violated the law, but undermined the integrity of WhatsApp and the security and privacy that its users rely upon.

Courts have also recognized the public interest in "the enforcement of a valid and binding contract" that supports entry of an injunction. *Gen. Motors LLC v. Santa Monica Grp., Inc.*, 2010 WL 2740166, at *3 (C.D. Cal. July 9, 2010); *see also Allen v. Campbell*, 2021 WL 737123, at *11

(D. Idaho Feb. 25, 2021) ("The public interest of the enforcement of contracts . . . supports the issuance of the permanent injunction as well."). NSO agreed to the WhatsApp Terms of Service many times over, while having no intention of following it. Such conduct flouts the public's interest. Because the public interest favors permanently enjoining NSO's conduct, and Plaintiffs satisfy the other factors for obtaining injunctive relief, an injunction is therefore warranted and appropriate.

II. The Court Should Enjoin NSO from Future Violations of the Law and the WhatsApp Terms of Service

"A district court has considerable discretion in fashioning suitable relief and defining the terms of an injunction." *Hecox v. Little*, 104 F.4th 1061, 1089 (9th Cir. 2024), *as amended* (June 14, 2024) (quoting *Lamb-Weston, Inc. v. McCain Foods, Ltd.*, 941 F.2d 970, 974 (9th Cir. 1991)). In order to ensure that NSO no longer violates the law, the Court should prohibit NSO and its affiliates from: (a) using Plaintiffs' Platforms in any way, including as an installation vector; (b) emulating Plaintiffs' Platforms, including by using the WIS; (c) collecting data from Plaintiffs' Platforms; (d) reverse-engineering or decompiling Plaintiffs' Platforms; (e) sending harmful code through Plaintiffs' Platforms; (f) using Plaintiffs' Platforms for illegal purposes; and (g) creating accounts on Plaintiffs' Platforms. The Court should also require NSO to destroy all computer code that uses Plaintiffs' Platforms (including the WIS), to disable customer access to such code, and to delete all the data it obtained from Plaintiffs' Platforms (including any data it obtained from WhatsApp users). Finally, the Court should order NSO to certify that it provided notice of the injunction and complied with the injunction's requirements. These provisions are tailored to remedy the irreparable harm caused by NSO's illegal conduct and prohibit NSO from engaging in misconduct and from using the ill-gotten data that it obtained from Plaintiffs or derived from Plaintiffs' source code.

A. Prohibition on Using Plaintiffs' Platforms

The Court should prohibit NSO and its related entities from "[d]eveloping, using, selling, offering for sale, distributing, transferring, or licensing, whether directly or through a third party, intermediary, or proxy, any technology that uses Plaintiffs' Platforms in any way, including as a method or approach used to install and deploy the technology (an 'installation vector'), without first

requesting and obtaining Plaintiffs' express written permission." Proposed Order § 3(a). The undisputed facts establish that NSO created a modified version of the WhatsApp application that enabled "'cipher' files with 'installation vectors'" to be "sent through plaintiffs' California-based servers." Dkt. No. 494 at 2, 6. Though NSO claimed that its code accessed WhatsApp servers "just like any other message," *id*. at 11, the Court rejected this argument and ruled that NSO exceeded its authorized access under federal and state law, *id*. at 12. Having proven that it cannot be trusted to use Plaintiffs' Platforms within the scope of the law or contractual limitations, NSO should no longer be able to use Plaintiffs' servers or send code through Plaintiffs' computers at all.

Courts in this district frequently include similar prohibitions in permanent injunctions for violations of the CFAA and the CDAFA. For example, in *Power Ventures*, the court granted summary judgment for Facebook on its CFAA and CDAFA claims, and enjoined the defendant from "[a]ccessing or using . . . the Facebook website or servers." 252 F. Supp. 3d at 786; *see also Nguyen*, 2023 WL 8686924, at *11 (enjoining defendants from "[a]ccessing or attempting to access Meta's platforms and computer systems"); *Ates*, 2023 WL 4035611, at *9 (enjoining defendant from "[a]ccessing or attempting to access Meta's platforms . . . and Meta's computer systems"). Given NSO's course of conduct here, an outright prohibition on NSO's access or use of Plaintiffs' Platforms is warranted.

Moreover, even if NSO were to claim that it no longer uses installation vectors that exploit vulnerabilities in Plaintiffs' systems, it should nonetheless be prohibited from accessing or using Plaintiffs' Platforms in any way. Even when exploiting other vulnerabilities, NSO has targeted WhatsApp as part of its installation process. For instance, [redacted] *See* Dkt. No. 399-4, Ex. 6 at 269:13–18 ([redacted]). Thus, NSO's unsupported claim that it currently uses a different installation vector does not exclude the possibility that it continues to access Plaintiffs' Platforms.

B. Prohibition on Emulating Plaintiffs' Technologies

The Court should enjoin NSO and its related entities from "[d]eveloping, using, selling, offering for sale, distributing, transferring, or licensing, whether directly or through a third party, intermediary, or proxy, any technology that emulates Plaintiffs' Platforms in any way, including but not limited to the [WIS], without first requesting and obtaining Plaintiffs' express written permission." Proposed Order § 3(b). The Court's order finding NSO liable recognized that the WIS—which NSO developed in violation of the WhatsApp Terms of Service—enabled NSO to attack Plaintiffs' servers. *See* Dkt. No. 494 at 2 ("The WIS, among other things, allows defendants' clients to send "cipher" files with "installation vectors" that ultimately allow the clients to surveil target users."). NSO should be prohibited from using the WIS, or building a replacement version that would enable NSO to send malicious code through Plaintiffs' servers to Plaintiffs' users.

Prohibitions on using or developing violative technology are regularly found appropriate in connection with violations of computer hacking laws. In *Power Ventures*, the court enjoined defendants from "[d]eveloping, using, selling, offering for sale, or distributing, or directing, aiding, or conspiring with others to develop, sell, offer for sale, or distribute, any software that allows the user to engage in the conduct found to be unlawful." 252 F. Supp. at 786; *see also Nguyen*, 2023 WL 8686924, at *11 (enjoining defendant from "developing malware that targets Facebook"); *Ates*, 2023 WL 4035611, at *9 (enjoining defendant from "[d]eveloping, offering, and marketing software, computer code, or other products or services intended to automate the collection of data from Meta's platforms or circumvent Meta's enforcement measures"). NSO could not have attacked Plaintiffs' infrastructure and Plaintiffs' users without emulating Plaintiffs' Platforms and should be prohibited from doing so again.

C. Prohibition on Collecting Data from Plaintiffs' Platforms

The Court should prohibit NSO and its related entities from "[c]ollecting, or assisting others in collecting, data or information from Plaintiffs' Platforms, whether directly or through a third-party, intermediary, or proxy, without first requesting and obtaining Plaintiffs' express written permission." Proposed Order § 3(c). Even if NSO does not currently send code through Plaintiffs' computers, it should not be permitted to collect private information from Plaintiffs' users. In granting Plaintiffs'

motion for summary judgment, the Court held that NSO "obtain[ed] information directly from the target users' devices" and "also obtain[ed] information about the target users' device via the Whatsapp servers." Dkt. No. 494 at 12. The Court likewise found that NSO breached the WhatsApp Terms of Service by "collecting user information." *Id*. at 13. Indeed, the overarching purpose of NSO's technology is to allow the collection of user information, and NSO should be banned from continuing towards this illegal end.

Courts routinely enjoin defendants who have improperly obtained data from continuing their actions. *See, e.g.*, *Sluchevsky*, 2020 WL 5823277, at *10 (enjoining defendant from "soliciting, storing, and/or using Facebook login information from any current, past, or future Facebook user"); *Facebook, Inc. v. Solonchenko*, 2022 WL 18491616, at *7 (N.D. Cal. Dec. 29, 2022) (enjoining defendant from "selling or distributing data of any kind obtained from Meta and its products"), *report and recommendation adopted*, 2023 WL 420677 (N.D. Cal. Jan. 26, 2023). In addition, the Ninth Circuit has upheld a permanent injunction that included "prohibitions against . . . copying or storing . . . source code" and "using information related to or based on . . . source code." *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 937 (9th Cir. 2004). Such a remedy is warranted here, especially because NSO's data collection conduct was found to have violated the CFAA, the CDAFA, and the WhatsApp Terms of Service.

D. Prohibition Against Conduct That Violates the WhatsApp Terms of Service

The Court should prohibit NSO and its related entities from engaging in conduct that violates the WhatsApp Terms of Service. Specifically, NSO should be enjoined from reverse-engineering or decompiling Plaintiffs' computer systems, platforms, client applications, or other technologies; sending harmful code through Plaintiffs' computer systems, platforms, client applications, or other technologies; and using Plaintiffs' computer systems, platforms, client applications, or other technologies for illegal purposes. Proposed Order §§ 3(d)–3(f). These prohibitions mirror the Court's findings on NSO's breaches, as the Court held that NSO violated the WhatsApp Terms of Service, "specifically the provisions prohibiting users from 'reverse engineering' or 'decompiling' Whatsapp products, from sending 'harmful code' through Whatsapp, and . . . from using Whatsapp for illegal purposes." Dkt. No. 494 at 13. NSO should be prohibited from continuing its violations in the future.

In similar cases, courts—including in this district—have enjoined defendants from violating terms of service. *See, e.g.*, *Nguyen*, 2023 WL 8686924, at *11 (enjoining defendant from "[e]ngaging in any activity, or facilitating others to do the same, that violates Meta's Terms"); *Facebook, Inc. v. ILikeAd Media Int'l Co.*, 2022 WL 2289058, at *1 (N.D. Cal. Mar. 15, 2022) (enjoining defendant from "[e]ngaging in any activity, or facilitating others to do the same, that violates Facebook's Terms of Service and Advertising Policies, including the use of cloaking software to circumvent Facebook's ad review process"); *Sluchevsky*, 2020 WL 5823277, at *10 (enjoining defendant from "engaging in any activity, or facilitating others to do the same, that violates Facebook's TOS, Community Standards, Platform Policy, or other related policy referenced"). Plaintiffs' proposal targets the specific actions that the Court found violated the WhatsApp Terms of Service.

E. Prohibition on New Account Creation

The Court should prohibit NSO and its related entities from "[c]reating accounts, whether directly or through a third party, intermediary, or proxy, on Plaintiffs' Platforms, without first requesting and obtaining Plaintiffs' express written permission." Proposed Order § 3(g). In finding NSO liable for violating the CFAA and the CDAFA, and for breaching the WhatsApp Terms of Service, the Court held that NSO obtained authentic WhatsApp credentials by creating legitimate WhatsApp accounts. *See* Dkt. No. 494 at 14; *see also* Dkt. No. 399-4, Ex. 6 at 80:2–81:7, 83:12–21, 86:23–87:18, 223:4–224:14 ([redacted]). [redacted] *See* Dkt. No. 399-4, Ex. 8 at 17:13–23, 21:13–24; *id.*, Ex. 6 at 188:12–25. Creating WhatsApp accounts for these purposes constitutes a *prima facie* violation of the WhatsApp Terms of Service, including the prohibitions on using or assisting others in using WhatsApp to "collect the information of or about [WhatsApp] users in any impermissible or unauthorized manner." Dkt. No. 401-2, Ex. 11 at 3.

Because NSO's creation of accounts for illicit purposes violated the WhatsApp Terms of Service, Plaintiffs' proposed injunction properly enjoins NSO from creating any accounts at all. *See Power Ventures*, 252 F. Supp. 3d at 784 (finding that restriction on defendants using Facebook for

commercial purposes was "warranted to prevent future violations of the law"); *see also Sluchevsky*, 2020 WL 5823277, at *10 (enjoining defendants from "creating or maintaining any Facebook accounts in violation of Facebook's TOS"). In a similar context, the Ninth Circuit upheld an injunction prohibiting the defendant from accessing plaintiff's website for any reason, reasoning that the defendant was "in a position analogous to one who has repeatedly shoplifted from a particular store, so the judge prohibits him from entering it again, saving the store's security guards from the burden of having to follow him around whenever he is there." *Creative Computing*, 386 F.3d at 937–38. Barring NSO from creating new accounts would save Plaintiffs from this same burden.

F. Requirement to Delete Computer Code and Improperly Obtained Data

The Court should also order NSO and its related entities to "delete and destroy any and all computer code or technologies that use, access, or depend on Plaintiffs' Platforms, including the WhatsApp Installation Server ('WIS'), to delete all data obtained or derived from Plaintiffs' Platforms, and to disable customer access to any and all computer code or technologies that use, access, or depend on Plaintiffs' Platforms." Proposed Order § 4. As detailed above, the WIS—which NSO built by violating the WhatsApp Terms of Service—played a crucial role in allowing NSO to send malicious code to Plaintiffs' servers. An injunction that does not require NSO to delete the WIS, or any related technologies, would leave NSO able to target Plaintiffs' servers with malicious code at a moment's notice. NSO should similarly delete all data it obtained from Plaintiffs' Platforms in violation of the law. If NSO is to be believed that its "government customers alone operate Pegasus and make all decisions about how to do so," Dkt. No. 469 at 10, then allowing NSO to give its customers the tools to access Plaintiffs' servers (or continue to profit from its customers' use of those tools) would not remedy the underlying harm. The Court should therefore order NSO to cut off its customers' access to installation vectors or technologies that attack Plaintiffs' infrastructure.[6]

Deletion of computer code and unjustly obtained data forms a central aspect of similar injunctions. The *Power Ventures* court entered an injunction obligating the defendant to "destroy any

[6] For the avoidance of doubt, the proposed injunction prohibits NSO from "transferring" any technologies that use or emulate Plaintiffs' Platforms in any way, *see* Proposed Order §§ 3(a), 3(b), and requires any transferee to "delete and destroy" any such technologies, *id.* § 4; *see id.* § 1 (defining "Prohibited Parties" to include "persons who are in active concert or participation with Defendants").

software, script(s) or code designed to access or interact with the Facebook website, Facebook users, or the Facebook service" and "destroy Facebook data and/or information obtained from Facebook or Facebook's users, or anything derived from such data and/or information." *Power Ventures*, 252 F. Supp. 3d at 786; *see also Priority Payment Sys., LLC v. Intrend Software Sols.*, 2016 WL 8809877, at *9 (N.D. Ga. Nov. 28, 2016) (entering injunction requiring defendants to "destroy all copies of the . . . Source Code that are currently in their possession"); *ClearOne Advantage, LLC v. Kersen*, 2024 WL 4754051, at *11 (D. Md. Nov. 12, 2024) ("[T]he proposed injunction's requirement for Defendants to search for and return to [plaintiff's] counsel any [of plaintiff's] confidential information in their possession is a reasonable one.").

G. Notice and Certification Requirements

Finally, to ensure NSO's compliance with an injunction, the Court should require NSO to "affirm in writing that [it] notified all Prohibited Parties of the existence of this Permanent Injunction and provide a copy of this Order to each of them" and "certify in writing that [it is] in compliance with the provisions of this Order" 30 days after entry of the permanent injunction. *See* Proposed Order §§ 5, 6. Courts in this district routinely require enjoined parties to certify their compliance with injunctions. *See, e.g.*, *OpenAI, Inc. v. Open A.I., Inc.*, 719 F. Supp. 3d 1033, 1052 (N.D. Cal. 2024) (requiring defendants to file a written report detailing manner of compliance within 30 days), *aff'd*, 2024 WL 4763687 (9th Cir. Nov. 13, 2024); *Psystar*, 673 F. Supp. 2d at 956–57 (requiring defendant to file a "report in writing and under oath detailing the manner in which defendant has complied with the injunction"), *aff'd*, 658 F.3d 1150 (9th Cir. 2011); *Power Ventures*, 252 F. Supp. 3d at 786 (requiring defendants to "certify in writing, under penalty of perjury, that they have complied with the provision of this order"). Especially given NSO's history of noncompliance with this Court's orders, a similar provision is warranted here.

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court grant their motion and enter a permanent injunction.

Dated: February 24, 2025

Respectfully Submitted,

DAVIS POLK & WARDWELL LLP

By: */s/ Micah G. Block*

Greg D. Andres
Antonio J. Perez-Marques
Gina Cora
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
gina.cora@davispolk.com
craig.cagney@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.