UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC., et al.,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED, et al.,

Defendants.

Case No. 19-cv-07123-PJH

ORDER DENYING MOTION TO STAY PERMANENT INJUNCTION; EXTENDING ADMINISTRATIVE STAY FOR 45 DAYS

Re: Dkt. 813

Before the court is defendants' motion to stay the court's permanent injunction order pending appeal. See Dkt. 813. Having read the papers filed by the parties and carefully considered their arguments and relevant authority, and good cause appearing, the court hereby rules as follows.

A. Legal standard

Federal Rule of Civil Procedure 62(d) provides that, "[w]hile an appeal is pending from an interlocutory order or final judgment that grants, continues, modifies, refuses, dissolves, or refuses to dissolve or modify an injunction, the court may suspend, modify, restore, or grant an injunction on terms for bond or other terms that secure the opposing party's rights."

In evaluating a motion for a stay pending appeal, the court considers "whether the applicant has made a strong showing of likelihood of success on the merits, whether the applicant will be irreparably injured without a stay, whether a stay will substantially injure the other parties, and where the public interest lies." See Arizona Democratic Party v. Hobbs, 976 F.3d 1081, 1086 (9th Cir. 2020); Al Otro Lado v. Wolf, 952 F.3d 999, 1006-07

(9th Cir. 2020) (citing Nken v. Holder, 556 U.S. 418, 434 (2009)). The first two factors "are the most critical"; the last two are reached only after "an applicant satisfies the first two factors." Al Otro Lado, 952 F.3d at 1007 (citing Nken at 434-35).

The standard for granting a stay is a "sliding scale," i.e., the elements of the test are "balanced, so that a stronger showing of one element may offset a weaker showing of another." Arizona Democratic Party, 976 F.3d at 1086 (citing Al Otro Lado, 952 F.3d at 1007). "A stay is not a matter of right, even if irreparable injury might otherwise result." Al Otro Lado, 952 F.3d at 1006 (citing Virginian Ry. Co. v. United States, 272 U.S. 658, 672 (1926)).

B. Analysis

1. Likelihood of success on the merits

Defendants argue that they are likely to succeed on the merits on the following issues: (1) the court's imposition of liability, (2) the court's finding of personal jurisdiction, (3) the court's treatment of defendants' affirmative defenses, and (4) the court's issuance of a permanent injunction. See Dkt. 813 at 8-19.

a. Liability

As to liability, defendants argue that the court "improperly found that NSO exceeded authorized access'" under the CFAA and CDAFA, that the court misapplied the "intent to defraud" standard under the CFAA, that the court had insufficient evidence that NSO had agreed to the Whatsapp terms of service, and that the court improperly held NSO liable for the alleged conduct of its clients. See Dkt. 813 at 8-12.

The court does not find that defendants have made a strong showing of likelihood of success on the merits of their arguments regarding liability. Starting with the "exceeds authorized access" issue, even based only on the limited discovery provided by defendants, the undisputed evidence showed that NSO went far beyond their authorized use of Whatsapp by reverse-engineering the application to design a spyware vector which allowed NSO's clients to surveil Whatsapp's users and obtain data from its servers. See, e.g., Dkt. 494 at 11-13. When Whatapp attempted to fix the security vulnerability,

defendants designed around the fix to continue their surreptitious access. See id.; Dkt. 802 at 5-7. Defendants could not, and do not, argue that they had actual authorization to engage in this conduct – instead, they simply argue that there is not yet a Ninth Circuit or Supreme Court case that directly contradicts their position. However, given the cutting-edge technology at issue in this case, the lack of similar past cases does not persuade the court that defendants are likely to succeed on the merits of their argument regarding the "exceeds authorized access" prong of the CFAA and CDAFA.

Next, defendants argue that they are likely to succeed on the merits of their argument that they did not have the requisite "intent to defraud." The essence of defendants' argument is that they did not intend to steal "any money or property from Whatsapp." See Dkt. 813 at 11. Defendants cite no authority applying their purported rule to violations of the CFAA or CDAFA. And on the merits, the court concludes that defendants' view does not present a strong showing that they are likely to succeed.

As to the Whatsapp terms of service, plaintiffs presented testimony regarding the necessity of agreeing to the terms of service before creation of a Whatsapp account, and the notice given to users. See Dkt. 467 at 2. Moreover, the court noted in its summary judgment order that defendants refused to produce relevant discovery regarding the phones that were used to create accounts on defendants' behalf. See Dkt. 494 at 14. Based on that evidentiary record, the court concluded that "defendants cannot meaningfully dispute that agreeing to the terms of service was necessary to create a Whatsapp account and to use Whatsapp," and defendants' arguments on this motion do not persuade the court that they are likely to succeed on the merits of this argument.

Finally, defendants argue that the court held NSO liable for its clients' conduct, namely, obtaining data from target users. As mentioned in this and previous orders, defendants withheld significant discovery in this case, and the relationship between NSO and its customers was a topic where evidence was particularly limited. As a result, conclusions about certain conduct could not be drawn. As the court stated in a previous order:

> [T]he evidentiary record did not show (at the time of summary judgment, nor now) the specific details about how exactly the relevant attacks were conducted. Based on that unclear record, the court concluded that even the limited conduct to which defendants admit (i.e., developing Pegasus and providing it to their clients, as well as providing training and ongoing support) along with evidence that appears undisputed that they updated Pegasus to circumvent plaintiffs' security updates, sufficed to establish liability even before reaching the issue of whether evidentiary sanctions were necessary.

See Dkt. 699 at 1-2.

Thus, the court held defendants liable for their own conduct, not for the conduct of its customers. As the court explained, "[w]hile the court's order left open the possibility that defendants engaged in conspiracy to violate the CFAA, as the relevant evidence may indeed support that conclusion – based on the state of the evidentiary record, the court stopped short of an express finding that defendants engaged in conspiracy to violate the CFAA." See id. at 2. Accordingly, the court is not persuaded that defendants are likely to succeed on the merits of their argument that the court improperly found NSO liable for the conduct of its customers.

b. Personal jurisdiction

Turning to the issue of personal jurisdiction, defendants argue that the court improperly held that the use of California-based servers was sufficient to support personal jurisdiction, and that the court erred by imposing a discovery sanction that defendants intended to use California-based servers. See Dkt. 813 at 12-14.

As the court noted in its previous order, the court had first addressed personal jurisdiction during the pleadings stage and found that it was supported by the complaint's allegations, but defendants argued at summary judgment that the allegations were not supported by the evidence. See Dkt. 494 at 5.

Notably, defendants do not dispute that their code was indeed sent through plaintiffs' California-based servers, defendants dispute only that they had intent to use those servers and/or any control over which servers were used. However, as the court noted in its order granting summary judgment, because "defendants did not produce Pegasus code in a way that was meaningfully accessible to plaintiffs or to the court,

plaintiffs were unable to obtain detailed evidence of how the [defendants' code] chose which server(s) to use." See Dkt. 494 at 9. Accordingly, the court imposed a narrow evidentiary sanction that "the use of plaintiffs' California-based servers was a purposeful choice made by defendants." Id. at 9-10.

Defendants appear to now challenge the premise that they should have been required to produce Pegasus code in the first place, but the court finds no basis for those arguments, which attempt to distract from the plain fact that the functionality of the Pegasus code was central to resolving this litigation, and that defendants consistently resisted producing discovery on that topic. While defendants did and still do claim that they should be excused from the applicable discovery rules, and remain free to present that argument on appeal – the court at this time does not conclude that defendants are likely to succeed on the merits of their personal jurisdiction argument.

c. Affirmative defenses

Defendants argue that the court did not resolve their affirmative defenses regarding the law enforcement exception, the unclean hands defense, and the waiver defense. See Dkt. 813 at 14-15.

Regarding the law enforcement exception, defendants have repeatedly presented their argument that Pegasus was licensed by the FBI, but have also repeatedly failed to produce any evidence that the conduct challenged in this case was part of a "lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States," as required by 18 U.S.C. § 1030(f). Defendants simultaneously argue that the court "did not address" this defense, and that the court "has made that finding" rejecting the defense but that "there are serious questions as to its correctness." See Dkt. 821 at 13. In short, the court has indeed resolved defendants' argument regarding the CFAA's law enforcement exception, and while defendants are free to challenge that resolution on appeal, they have not persuaded this court that they are likely to succeed on the merits of that argument.

As to the unclean hands defense, plaintiffs are correct that the defense is premised on an argument that was rejected at trial – that plaintiffs' investigation into defendants' spyware itself constituted an attempt to steal defendants' code. And finally, as to waiver, the court finds no basis for the argument that plaintiffs allowed defendants' conduct to continue after learning about it. To the extent that defendants complain about the lack of specific written findings on each asserted affirmative defense, the court notes that such specificity is not required. See, e.g., United States v. Dooley, 719 Fed. App'x 604, 606 (9th Cir. 2018). Overall, defendants have not persuaded the court that they are likely to succeed on the merits of their argument regarding affirmative defenses.

d. Injunction

Defendants challenge the court's imposition of a permanent injunction, arguing that the court improperly found irreparable harm, improperly enjoined activities that did not involve Whatsapp servers, failed to carve out a law enforcement exception, and improperly enjoined reverse-engineering and decompiling code from the Whatsapp platform. See Dkt. 813 at 15-19.

Regarding irreparable harm, defendants argue that the court erred in relying on reputational damages, which were expressly disclaimed by plaintiffs. However, the court explained in its previous order that it concluded that the thwarting of end-to-end encryption caused plaintiffs to suffer business harm, and that such harm was properly considered when determining whether to order an injunction. See Dkt. 802 at 7-9. Moreover, plaintiffs presented testimony regarding the primary role of privacy in Whatsapp's business. See, e.g., Dkt. 749 at 325-27. Accordingly, the court is not persuaded that defendants are likely to succeed on the merits of this argument.

The law enforcement exception was previously addressed above, and was also addressed in an order resolving defendants' objections to the proposed injunction. See Dkt. 808 at 1. In short, the court concluded that there was "no evidence that the United States has ever used Pegasus for law enforcement activities," and thus, there was no basis for the "sweeping carveout" proposed by plaintiffs, which went further than the

exception as codified in 18 U.S.C. § 1030(f). Accordingly, the court is not persuaded that defendants are likely to succeed on the merits of this argument.

Finally, the court will address both arguments about the scope of the injunction together. As stated above, defendants object to the injunction's inclusion of activity that does not access Whatsapp's servers, as well as reverse-engineering and decompiling. The court addressed both arguments in its order granting plaintiffs' motion for permanent injunction, and concluded that both inclusions were warranted as "sufficiently related to defendants' unlawful access of plaintiffs' and their users' data." See Dkt. 802 at 11, 17; see also Facebook, Inc. v. Power Ventures, Inc., 252 F.Supp.2d 765, 784 (N.D. Cal. 2017) ("it is well established that federal courts have the equitable power to enjoin otherwise lawful activity if they have jurisdiction over the general subject matter and if the injunction is necessary and appropriate in the public interest to correct or dissipate the evil effects of past unlawful conduct or to prevent continued violations of the law."). Accordingly, the court is not persuaded that defendants are likely to succeed on the merits of these arguments.

Thus, overall, the court concludes that defendants have not made a strong showing of likelihood of success on the merits of the arguments presented.

2. Irreparable injury to applicant

Defendants argue that they will be irreparably injured in the absence of a stay, first because the destruction of any code is permanent, and second because an injunction "will put NSO's entire enterprise at risk." See Dkt. 813 at 19-21. The court recognizes that the illegal nature of the enjoined conduct does not automatically prevent consideration of the harm that an injunction would impose, but the court also finds persuasive the "long-settled principle that harm caused by illegal conduct does not merit significant equitable protection." See Disney Enters., Inc. v. VidAngel, Inc., 869 F.3d 848, 867 (9th Cir. 2017); Softketeers, Inc. v. Regal W. Corp., 2023 WL 2024701 at *11 (C.D. Cal. Feb. 7, 2023).

Moreover, plaintiffs point to defendants' own evidence on this motion, showing that

Whatsapp is just one of many sources from which defendants' software can extract data. See, e.g., Dkt. 813-6 at 8 ("Monitor a multitude of applications including Skype, Whatsapp, Viber, WeChat, Line, Facebook Messenger, Telegram, and Blackberry Messenger (BBM).")

As a result, the court gives only slight weight to any injury caused by the absence of a stay.

3. Substantial injury to other parties

Defendants argue that plaintiffs will not be irreparably harmed in the absence of a stay. Plaintiffs argue that this factor is due less weight than the first two factors, and further argue that the court's order granting the injunction set forth the ways in which plaintiffs continue to be harmed by defendants' conduct. Overall, the court agrees that its previous order set forth the basis for concluding that plaintiffs face at least the same risk of ongoing harm as did the plaintiff in Power Ventures, because, as in that case, the defendants in this case have exhibited "bad faith conduct" indicating that "they will not easily be deterred from attempting to access [plaintiffs'] servers without authorization in violation of the CFAA." See Dkt. 802 at 4-5 (citing Power Ventures, 844 F.3d at 782).

Accordingly, the court concludes that plaintiffs would indeed be substantially injured by a stay.

4. Public interest

Defendants argue that the public interest favors a stay, first because "the FBI purchased a license for Pegasus in December 2018," and second because "the U.S. public would also be harmed by depriving foreign governments of access to Pegasus." See Dkt. 813 at 22-24. Defendants' first argument has been addressed in this order's discussion of the asserted law enforcement exception, and is further undermined by NSO's presence on the U.S. Department of Commerce's Entity List. As to defendants' second argument, the injunction specifically does not apply to foreign governments. See Dkt. 802 at 13, 14-15.

Instead, the court notes that the Ninth Circuit has held that the public has

"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). Accordingly, the court concludes that the public interest weighs against a stay.

Thus, having considered the four factors applicable to defendants' motion for a stay pending appeal, the court concludes that defendants have not met their burden on this motion. In particular, the court is not persuaded that defendants have shown that they are likely to succeed on the merits of their appeal. Moreover, as quoted above, the Ninth Circuit has held that "[a] stay is not a matter of right, even if irreparable injury might otherwise result." See Al Otro Lado, 952 F.3d at 1006 (internal citation omitted). Accordingly, defendants' motion to stay the permanent injunction pending appeal is DENIED.

The only remaining issue is whether to extend the administrative stay to allow defendants to seek a stay from the Ninth Circuit. The court agrees that a final, limited administrative stay for that purpose is warranted, and thus temporarily stays the permanent injunction order (Dkt. 809) for a period of up to 45 days from the date of this order to allow defendants to seek a stay pending appeal from the Ninth Circuit Court of Appeals in accordance with Federal Rule of Appellate Procedure 8(a)(2). Within five (5) days of the Ninth Circuit's decision on the anticipated motion to stay, defendants shall file a notice of the decision in this court.

IT IS SO ORDERED.

Dated: December 19, 2025

/s/ Phyllis J. Hamilton
PHYLLIS J. HAMILTON
United States District Judge

United States District Court
Northern District of California