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 RE MOTION FOR PERMANENT INJUNCTION, MOTION FOR REMITTITUR OR NEW TRIAL, AND MOTION TO SEAL

Re: Dkt. 558, 747, 790, 791, 797

Plaintiffs' motion for permanent injunction and defendants' motion for a remittitur or a new trial came on for hearing on August 28, 2025. Plaintiffs appeared through their counsel, Greg Andres, Antonio Perez-Marques, Luca Marzorati, and Micah Block. Defendants appeared through their counsel, Joseph Akrotirianakis, Aaron Craig, Matthew Noller, and Matthew Dawson. 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.

BACKGROUND

The facts underlying this lawsuit have been presented in numerous previous orders, including this court's order granting partial summary judgment on the issue of liability. See Dkt. 494. In short, the court granted partial summary judgment in favor of plaintiffs under the Computer Fraud and Abuse Act ("CFAA") and the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), as well as for breach of contract. The evidence showed that defendants reverse-engineered Whatsapp's code to create a modified version of the Whatsapp client application, which they then used to install their software on target users' devices via WhatsApp's servers. The evidence

further showed that defendants repeatedly re-designed their software to avoid detection and circumvent plaintiffs' security fixes. See id.

After summary judgment, the court conducted a damages-only trial, in which a jury unanimously awarded plaintiffs the full amount of $444,719 they sought in compensatory damages. The jury also found that defendants acted with malice, oppression, or fraud, and awarded plaintiffs $167,254,000 in punitive damages. See Dkt. 736.

After trial, the court scheduled an evidentiary hearing on plaintiffs' motion for permanent injunction. Defendants filed a motion for new trial on the issue of punitive damages, which the court set for hearing on the same day as the evidentiary hearing regarding the injunction motion.

Before the hearing, defendants also filed a motion to strike to preclude plaintiffs' witnesses from testifying, on the basis that they had not been properly disclosed. See Dkt. 770. After allowing both parties to file briefs on the issue, the court denied the motion, concluding that any imperfect disclosure could be remedied by cross-examination at the hearing and, if necessary, by allowing defendants to depose the challenged witnesses either before or after the hearing. See Dkt. 781. At the hearing defendants advised that they had not taken the witnesses' depositions beforehand, but would depose them after the hearing and file supplemental briefing. They also declined to cross-examine the witnesses at the hearing because they needed document discovery before meaningful depositions could be conducted. Accordingly, the court heard only direct testimony from plaintiffs' challenged witnesses at the hearing, who testified that defendants continue to collect users' messages through Whatsapp and have been observed using Whatsapp as part of their research and development activities as recently as April 2025. Notwithstanding this testimony, plaintiffs argued, as they had in the past, that this additional testimony was really unnecessary to support their request for an injunction, as the record contained ample justification for injunctive relief.

After hearing much of the evidence, the court expressed surprise at how "most of the factual matters that have been brought forth today are matters about which I read

over and over about in this case," and that "there's really nothing new, nothing that's materially new, that will affect the outcome of this case." See Dkt. 795 at 132. In that sense, the court agrees with the argument made by plaintiffs and by defendants' counsel in their reply brief, that "Pegasus's collection of WhatsApp messages is not a new fact, because all the documentary information produced by Defendants about the functionality of Pegasus touts this as a key feature, and Defendants have never stated or suggested that Pegasus ever stopped collecting WhatsApp messages." Dkt. 779 at 4. Indeed, as will be discussed in further detail below, many of the material facts in this case are undisputed – it is the legal significance of those facts that the parties dispute.

Thus, having determined that the testimony presented by plaintiffs' witnesses (namely, Andrew Blaich and Lander Brandt) at the evidentiary hearing was cumulative in nature, and in order to avoid reopening discovery to permit defendants to effectively depose witnesses not previously deposed, the court hereby STRIKES their testimony from the record. Defendants' counsel confirmed at the hearing that, if the court were to disregard the testimony of plaintiffs' witnesses, there would be no need for further discovery from the witnesses. See Dkt. 795 at 138-39.

Accordingly, the court will now address plaintiffs' motion for permanent injunction on the basis of the factual record presented up to and including trial, as well as defendants' expert witness Joshua Minkler, who testified at the evidentiary hearing. The court will then address defendants' motion for a new trial on the issue of punitive damages.

DISCUSSION

Motion for Permanent Injunction

A. Legal Standard

The CFAA provides that "any person who suffers damage or loss" under the statute can obtain "injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). The CDAFA also provides for injunctive or other equitable relief. See Cal. Penal Code § 502(e)(1).

A plaintiff seeking a permanent injunction must satisfy a four-factor test before a court may grant such relief, and is required to show the following: (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction. eBay v. MercExchange, 547 U.S. 388 (2006).

B. Analysis

1. Irreparable Injury

Plaintiffs argue that their "most important" purpose in this litigation is "protecting WhatsApp's platforms, servers, and users." Dkt. 795 at 143:4-5. Plaintiffs assert that "NSO admits that to this day they continue collecting WhatsApp messages, that that is something that cannot be accomplished without accessing parts of the devices and parts of the WhatsApp software that are not accessible to normal users." Id. at 14:6-10.

As a general matter, "[n]umerous courts have found that unauthorized access of computers and the acquisition of data in violation of the CFAA constitute irreparable harm." See Facebook, Inc. v. Power Ventures, Inc., 252 F.Supp.2d 765, 782 (N.D. Cal. 2017) (internal citations omitted).

The Power Ventures case involved a claim that the defendant had used Facebook's proprietary data without permission by "inducing Facebook users to provide their login information and then using that information to 'scrape' Facebook's proprietary material" and display it on Power Ventures' own website. See 252 F.Supp.2d at 768-69.

The district court concluded that Facebook had shown irreparable harm because "in accessing Facebook's computers without authorization, defendants have interfered with and acquired data to which the defendants have no lawful right" in violation of the CFAA and CDAFA. See Power Ventures at 782.

The district court further concluded that "unless the court issues a permanent injunction, it is very likely that Facebook will suffer irreparable harm again," because

defendants' "bad faith conduct" indicated that "they will not easily be deterred from attempting to access Facebook's servers without authorization in violation of the CFAA" and CDAFA. Power Ventures at 782.

The Power Ventures injunction was affirmed by the Ninth Circuit; though, as defendants point out, the Ninth Circuit did not issue a detailed opinion on the case. 844 F.3d 1058 (9th Cir. 2016). However, the Ninth Circuit did cite and discuss Power Ventures with approval in a subsequent case in which it distinguished the "user data that was protected by Facebook's username and password authentication system" in Power Ventures from data that "was available to anyone with a web browser." See hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1199 (9th Cir. 2022).

The unlawfully-accessed data in this case was not only protected with a username and password authentication system, but further protected by Whatsapp's end-to-end encryption. See Dkt. 795 at 86:16-19. Thus, in that sense, the injury in this case is even greater than in Power Ventures – because in addition to accessing plaintiffs' proprietary data and servers, defendants' access also prevents plaintiffs from delivering privacy and security to its users. As plaintiffs' counsel argued, "the expectation of privacy of users of the service is frustrated by bad actors like NSO who seek to collect messages that they're not entitled to." Dkt. 795 at 156:11-13.

Plaintiffs further argue that, as in Power Ventures, 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." See 252 F.Supp.3d at 782. As plaintiffs argue, the "central issue here and the reason that an injunction is so important is because the risk of future harm is so clear," as defendants "have already demonstrated and admitted a pattern of conduct whereby, when they were stopped from engaging in this conduct, they sought to resume it." Dkt. 795 at 143:7-12.

Plaintiffs argue that, absent an injunction, defendants would be "like a safecracker who still has all his tools. And they still have every economic and commercial incentive to target WhatsApp again." Dkt. 795 at 153:2-6. Plaintiffs point out that "[b]y their own

estimation, they engaged in these violations tens of -- up to tens of thousands of times," and "three different vectors [] were used, and each time one was stopped, either because we detected it or just because we changed our software in a way that frustrated it, they came back and they did it again." Id. at 148:11-17. "They were undeterred by our security measures. They were undeterred by their knowledge that WhatsApp did not want this conduct and would stop it if it was detected, and they were undeterred even by the filing of this lawsuit." Id. at 148:10-21.

Finally, plaintiffs argue that "the nature of their violations, including through the reverse engineering of this software, subjects us to an ongoing risk." Dkt. 795 at 155:14-16. Specifically, plaintiffs argue that defendants "have learned something that they weren't entitled to know, and it's information that they continue to possess that puts us at a risk of continued attacks." Id. at 155:17-19.

Indeed, the prospect of future harm is directly relevant to the irreparable injury inquiry. See, e.g., Y.Y.G.M. SA v. Redbubble, Inc., 75 F.4th 995, 1007 (9th Cir. 2023). And plaintiffs point to defendants' own testimony as evidence that the harm is ongoing.

In August 2024, NSO's CEO Yaron Shohat testified that defendants "have installation vectors for Pegasus today." Dkt. 399-4, Ex. 10 at 49.

In September 2024, NSO's vice-president of research and development Tamir Gazneli testified that Pegasus was still capable of obtaining "unlimited access to targets' mobile devices" and "remotely and covertly collect[ing] information about a target's relationships, locations, phone calls, plans and activities," and could also "activate the microphone to listen in on a target's environment" and "turn on the camera to take snapshots and take screenshots." Dkt. 399-4, Ex. 6 at 109. When asked to clarify whether defendants still invested efforts in circumventing Whatsapp's security measures, Gazneli answered "this is our business." Id. at 266.

The latter statement is similar to that of the Power Ventures defendants, who responded to the plaintiffs' cease-and-desist letter with a statement that it had "made the business decision to not prevent the interruption of service to our millions of users." 252

F.Supp.3d at 782.

Defendants' own statements in their opposition brief lead to the same conclusion that plaintiffs face the risk of ongoing harm. Defendants argue that the requested injunction "would put NSO's entire enterprise at risk" and "force NSO out of business," as "Pegasus is NSO's flagship product." See Dkt. 759-2 at 21. And as quoted above, defendants' counsel expressly acknowledged that "Pegasus's collection of WhatsApp messages is not a new fact, because all the documentary information produced by Defendants about the functionality of Pegasus touts this as a key feature, and Defendants have never stated or suggested that Pegasus ever stopped collecting WhatsApp messages." Dkt. 779 at 4.

In other words, while the parties dispute whether plaintiffs have actually been harmed, they do not dispute that any such harm is ongoing. In defendants' view, because their software purportedly no longer uses Whatsapp servers as an installation vector, their conduct – though ongoing – is legal and not harmful. As an initial matter, the court agrees with plaintiffs that, "by not telling us how they're collecting WhatsApp messages - the burden is improperly put on the plaintiffs to try to figure out how they're doing it and whether they're accessing our servers, something that they've admitted they tried to conceal when they did it in the past." See Dkt. 795 at 168:9-13. But in addition, plaintiffs are harmed not only when their servers are improperly accessed, but also when they are not able to offer the end-to-end encryption that they have promised their users. See id. at 156:11-13 ("the expectation of privacy of users of the service is frustrated by bad actors like NSO who seek to collect messages that they're not entitled to.").

Defendants argue that plaintiffs are improperly seeking to establish irreparable injury by pointing to harms suffered by the users, rather than to harms suffered by plaintiffs themselves. Defendants argue that the court previously held that any harm to users was outside the scope of this case. See, e.g., Dkt. 747 at 11 ("This court held before trial . . . that the only relevant conduct was NSO's use of Whatsapp servers, not the downstream use of Pegasus on target user devices."). However, defendants'

argument reaches too far. While the court did indeed exclude "evidence of the identities and occupations of the ~1,400 targets" from the trial (see Dkt. 686 at 9), that ruling simply prevented the jury from considering targets' status as journalists, activists, etc. when deciding the issue of damages – it was not a ruling that the existence of the users and their data are completely irrelevant for all purposes. See also Dkt. 358 at 3 ("Because NSO has not made even an initial showing that the [law enforcement] exception [to the CFAA] applies to any of the alleged victims in this case, the court concludes that the discovery sought in relation to those alleged victims would be disproportionate to the needs of the case.").

Consistent with its earlier rulings, the court is not considering the evidence that certain targets were members of 'civil society' – to the contrary, the court approaches this analysis as if the targets were ~1,400 individuals about whom nothing is known. And in this scenario, where ~1,400 individuals' data was unlawfully accessed, and where Whatsapp has over 3 billion users to whom privacy and security were promised in the form of end-to-end encryption, the court concludes that such unlawful access does indeed constitute an irreparable injury to Whatsapp.

The idea of a business offering technological privacy as a service is a relatively new one, as evidenced by defendants' expert's discussion of the recent proliferation in end-to-end encryption technology. Plaintiffs appear to have made such encryption, and the privacy and security that it entails, a significant part of its pitch to users, making it reasonable to conclude that users would be dissuaded from using Whatsapp if its encryption were ineffective.

And while it is true that the court's consideration of liability and damages was based on NSO's accessing of Whatsapp's servers, the ultimate purpose of defendants' actions was to obtain data from the target users. Accordingly, when considering the issue of a forward-looking injunction, the court may consider the nature of any prospective harm, and how/whether that harm would affect plaintiffs. In other words, when deciding whether to issue an injunction, the court may consider ways in which

plaintiffs have been harmed in the past or will be harmed in the future, which is a different standard than was applicable when considering the issue of compensatory and punitive damages.

In the court's view, any business that deals with users' personal information, and that invests resources into ways to encrypt that personal information, is harmed by the unauthorized access of that personal information – and it is more than just a reputational harm, it's a business harm. Essentially, part of what companies such as Whatsapp are 'selling' is informational privacy, and any unauthorized access is an interference with that sale. Defendants' conduct serves to defeat one of the purposes of the service being offered by plaintiffs, which constitutes direct harm.

Defendants argue that any finding of irreparable injury must be "grounded in [] evidence" specific to each case, rather than "cursory and conclusory." Herb Reed Enters., LLC v. Florida Ent. Mgmt., 736 F.3d 1239, 1250 (9th Cir. 2013). The court agrees, and places emphasis on the covert, undetectable nature of defendants' technology, as well as the repeated efforts to circumvent plaintiffs' security measures, as described above.

Plaintiffs have presented evidence regarding the "zero-click" nature of Pegasus, as well as the specific steps that defendants took to evade detection. See, e.g., Dkt. 557-3 at 21-22. Given the multiple design-arounds, the covert nature of NSO's work, and the designed undetectability of Pegasus itself, plaintiffs are unable to anticipate all the ways that defendants can access their platform, which is why they seek a broad injunction. As plaintiffs argue, "reverse engineering[1] is how they developed the exploit that was able to attack our servers," and that "the reason that they were hacking the servers was to get access to the messages." See Dkt. 795 at 165:2-8. In the court's view, this is the evidence that grounds the finding of irreparable injury in this case, and keeps any

[1] While reverse engineering is not expressly covered by the CFAA, the fact that defendants breached Whatsapp's terms of service by doing so is a fact that informs the court's understanding of the risk of ongoing harm and the scope of any injunction needed to prevent such harm.

findings from being "cursory and conclusory." Defendants reverse engineered plaintiffs' code to evade detection and to defeat encryption, and infected the target users' devices with spyware that no one wanted or expected. Defendants' arguments seem to presume the "right" to use Whatsapp for their intended purposes, notwithstanding the fact that neither Whatsapp nor the users invited or wanted NSO's software on their devices

This specific evidence regarding the undetectable nature of defendants' technology also shows the difficulty of preventing or mitigating such harm. See also Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 518 F.Supp.2d 1197, 1219 (C.D. Cal. 2007) ("the very need to file multiple lawsuits as a consequence of [defendants' conduct] is itself supportive of an irreparable harm finding."). In short, the court agrees with plaintiffs' argument that the evidence "establishes that NSO maintains the technical expertise and commercial incentives not only to access plaintiffs' servers, but also to hide any access from plaintiffs." See Dkt. 782 at 9.

Accordingly, having concluded that defendants' conduct causes irreparable harm, and there being no dispute that the conduct is ongoing, the court concludes that the first factor weighs strongly in favor of granting an injunction.

2. Adequacy of Monetary Damages

Many courts have found that this factor overlaps with the 'irreparable harm' factor. See, e.g., Rocawear Licensing, LLC v. Branco Enterprises, Inc., 2009 WL 10703523, at *9 (C.D. Cal. July 22, 2009) ("the irreparable injury requirement for a permanent injunction overlaps with lack of an adequate remedy at law") (internal citations omitted).

And in this specific case, the same rationale applies – the irreparable nature of the injury also suggests that the injury cannot be remedied by monetary damages alone. Separate from any reputational damages, which are not properly part of this case, Whatsapp would suffer harm in the form of having its proprietary code and its users' data compromised, along with the loss of any users who migrate to a platform with better protection against unauthorized access. Technology companies are commonly sued based on allegations that their privacy protections are not strong enough. In short, as

mentioned above, a breach of plaintiffs' encryption serves to defeat one of the purposes of the service that they offer to users.

Moreover, as set forth above, defendants freely acknowledge that they continue to use Whatsapp to collect users' messages. In concluding that monetary damages were inadequate, the Power Ventures court noted that "defendants may still possess the software at issue in this litigation and the data illegally acquired from Facebook." See 252 F.Supp.3d at 783. The argument for an injunction is even stronger in this case, because there is no dispute that defendants still possess the software at issue in this litigation, as well as the source code and other data illegally acquired from Whatsapp. "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." United Nat'l Maint., Inc. v. San Diego Convention Ctr. Corp., 2012 WL 3861946 at *7 (S.D. Cal. Sept. 5, 2012); see also Metro-Goldwyn-Mayer, 518 F. Supp. 2d at 1220 ("A legal remedy is inadequate if it would require a multiplicity of suits."). Although defendants do dispute that they use plaintiffs' servers to access users' data, the court has previously concluded that plaintiffs themselves are harmed when its users' data is unlawfully accessed.

Accordingly, the court concludes that the second factor weighs strongly in favor of granting an injunction.

3. Balance of Hardships

The Power Ventures court held that "defendants will suffer no harm from being unable to develop software to engage in illegal conduct." Power Ventures, 252 F.Supp.3d at 785. Defendants argue that the court must consider the business hardships that they would suffer if an injunction were to issue, "even if the conduct at issue is unlawful." See Dkt. 759-2 at 21 (citing Softketeers, Inc. v. Regal W. Corp., 2023 WL 2024701, at *11 (C.D. Cal. Feb. 7, 2023)). As stated above, defendants argue that the requested injunction "would put NSO's entire enterprise at risk" and "force NSO out of business." See Dkt. 759-2 at 21.

Even if the court were to accept defendants' position and consider the hardship

they would suffer if an injunction were to issue, the court must also consider the harm to plaintiffs' business if an injunction were not to issue. As noted above, plaintiffs tout end-to-end encryption as a feature for users to protect their privacy and security, and their business would be significantly harmed if that feature was rendered ineffective.

Moreover, defendants' argument overlooks the fact that plaintiffs are free to revoke authorization from any user, let alone a user that has already been found liable for wrongdoing. In the previously-mentioned hiQ Labs case, the Ninth Circuit recognized that "Facebook has tried to limit and control access to its website" by requiring "its users to register with a unique username and password," in contrast to the LinkedIn website, which made data "available to anyone with a web browser." 31 F.4th at 1199. If, as in hiQ Labs, defendants were simply seeking to access the type of information that was "available to anyone with a web browser," they would have a stronger argument that they would suffer hardship as a result of an injunction. Instead, defendants are seeking to access data that plaintiffs have protected not only with a username-and-password requirement, but also with end-to-end encryption.

Accordingly, the court concludes that the third factor weighs in favor of granting an injunction.

4. Public Interest

"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, 31 F.4th at 1202. Defendants argue that they do not fall into the category of "ill-intentioned actors" because their software is used only for law enforcement purposes such as surveilling criminals and terrorists.

To support their argument, defendants presented testimony from their expert, Joshua Minkler. At the hearing, defendants' counsel made clear that "the issue for which he's been tendered as an expert is the challenges posed to law enforcement by end to end encryption," which is "directly related to one of the factors that they need to prove, which is that the injunction . . . would not disserve the public interest." Dkt. 795 at 105.

Minkler testified about his experience with state and federal law enforcement investigations in Indiana, with a focus on the undesirability of end-to-end encryption as it pertains to law enforcement investigations. Minkler conceded that he had not interviewed anyone at NSO, had not operated Pegasus or seen it in use, and had no knowledge of NSO's clients or the targets against whom Pegasus has been used. Dkt. 795 at 93.

During cross-examination, Minkler also conceded that his knowledge of Pegasus's use to combat crime and/or terrorism was based solely on publicly-available information, such as newspaper articles. See Dkt. 795 at 119-120. This exchange highlighted one of the unique aspects of this case – because of the sealed nature of much of defendants' evidence, defendants have sought to establish their law-enforcement defense with citations to newspaper articles and similar types of publicly-available, unverified evidence. See, e.g. Dkt. 759-2 at 11. However, when plaintiffs seek to undermine the law-enforcement defense by citing articles reporting that Pegasus has been misused for non-law-enforcement purposes, such as surveilling journalists, human rights activists, political dissidents, etc., defendants argue that the court should ignore such unverified evidence. It would violate basic principles of equity and fairness to allow defendants to rely on such evidence, but to prohibit plaintiffs from doing so. Accordingly, the court will not consider any such evidence from either party, consistent with the court's rejection of this material at trial.

Nor will the court consider evidence or argument about the use of Pegasus by foreign governments in foreign countries, because as will be further discussed in the next section (regarding the scope of the injunction), the court has already concluded that any foreign sovereign governments should be excluded or carved out from any injunctive relief. See Dkt. 111 at 34. Thus, even assuming that foreign governments do use Pegasus for legitimate law enforcement purposes, those uses are not relevant to the court's current analysis. In contrast, there is no evidence that Pegasus has been used for law enforcement purposes within the United States, and indeed, NSO remains on the U.S. Department of Commerce's Entity List after it was "determined by the U.S.

Government to be acting contrary to the foreign policy and national security interests of the United States." See 86 Fed. Reg. 60759 (Nov. 4, 2021) ("Specifically, investigative information has shown that the Israeli companies NSO Group and Candiru developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers.").

Accordingly, the court concludes that the public interest in the United States weighs in favor of an injunction.

5. Scope of Injunction

"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 an initial matter, defendants argue that the "proposed injunction improperly applies to NSO's government customers," and would "arrogate to this court the power to dictate permissible law-enforcement, counterterrorism, and military surveillance techniques for every country in the world." See Dkt. 759-2 at 9, 27.

In their reply, plaintiffs cite to the court's previous order stating that "the plaintiffs are not seeking injunctive relief against defendants' foreign sovereign customers." See Dkt. 782 at 19 (citing Dkt. 111 at 34).

Indeed, the court's previous order concluded that defendants' customers "are not required parties because the court can craft injunctive relief that excludes or carves out any sovereign nation." See Dkt. 111 at 34. Such a carve-out would allay defendants' concern about foreign countries' law-enforcement techniques.

Because defendants' foreign sovereign customers are not before the court and have not been named as defendants, and because the court expressly ruled that they are not necessary parties, of course an injunction in this case cannot apply to them. To the extent that defendants believe that an injunction would indeed cover their foreign sovereign customers, the injunction will be revised to specifically exclude them.

Accordingly, plaintiffs shall revise the proposed injunction to exclude defendants'

foreign sovereign customers. As stated in the proposed injunction, the court shall retain jurisdiction over any allegations that defendants have failed to comply with their obligations as set forth in the injunction, and the parties shall submit to the court's jurisdiction for those purposes. See 18 U.S.C. § 1030(e)(2) (defining "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States"); see also In re Apple Inc. Device Performance Litig., 347 F.Supp.3d 434, 448 (N.D. Cal. 2018) ("the text of the CFAA provides a clear indication of extraterritorial application."); Alhathloul v. DarkMatter Group, -- F.Supp.3d ---, 2025 WL 2320474 (D. Or. 2025) ("Every court to consider the question has concluded that the CFAA applies extraterritorially.") (internal citations omitted).

Paragraph 2 of the proposed injunction defines its scope to include "all of plaintiffs' platforms." See Dkt. 558-3, ¶ 2. Defendants argue that any injunction should be limited to the Whatsapp platform. Plaintiffs argue that the complaint included Facebook as a plaintiff and included allegations regarding Facebook Messenger. See Dkt. 782 at 18.

While plaintiffs' description of the complaint is correct, the evidence throughout the course of the litigation has been focused solely on Whatsapp, and the court has no information about the other platforms and whether they have been or are in danger of being harmed in the same way by Pegasus.

Moreover, plaintiffs' inclusion of the language "but not limited to Whatsapp, Facebook, Instagram, Messenger, Meta AI, Threads, and Meta Horizon platforms" is unclear as to what unnamed platforms would also be covered by an injunction. See Dkt. 558-3, ¶ 2 (emphasis added). Accordingly, the injunction shall be limited to the Whatsapp platform.

Paragraph 3 of the proposed injunction sets forth the conduct from which defendants are enjoined: (a) developing, using, selling, offering for sale, distributing, transferring, or licensing any technology that uses plaintiffs' platforms in any way, (b)

developing, using, selling, offering for sale, distributing, transferring, or licensing any technology that emulates plaintiffs' platforms in any way, (c) collecting data from plaintiffs' platforms, (d) reverse engineering or decompiling code from plaintiffs' platforms, (e) sending viruses or harmful code through plaintiffs' platforms, (f) using plaintiffs' platforms for illegal purposes, and (g) creating new accounts on plaintiffs' platforms. See Dkt. 558-3, ¶ 3.

Defendants argue that the proposed provisions against "using" Whatsapp or creating new accounts are impermissible because they seek to enjoin lawful activity. However, the Power Ventures court and others have observed that "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." See Power Ventures, 252 F.Supp.3d at 784 (internal citations and quotations omitted); see also Oracle USA, Inc. v. Rimini St., Inc., 81 F.4th 843, 857 (9th Cir. 2023) ("an injunction is proper if it restrains acts which are of the same type or class as unlawful acts which the court has found to have been committed."). Moreover, while the court relies only on the CFAA and CDAFA in issuing this injunction, the court notes that some courts have issued injunctions to enforce contractual terms, on the basis that it was preferable to having the plaintiff file "lawsuit after lawsuit" to enforce their rights. See Deerpoint Group, Inc. v. Agrigenix, LLC, 345 F.Supp.3d 1207, 1225-26 (E.D. Cal. 2018); Densmore v. Manzarek, 2008 WL 2209993 at *47 (2008); see also Cal. Civ. Code § 3422, subd. 3 (injunction may be granted when "necessary to prevent a multiplicity of judicial proceedings.").

Turning to specific provisions of paragraph 3, the court is unclear how provisions (a) and (b) are different from each other in practice, and also finds the phrasing of (a) to be confusing to the extent it contains the word "uses" multiple times (e.g., "using . . . any technology that uses plaintiffs' platforms . . . including as a method or approach used to install the technology"). Accordingly, the court directs plaintiffs to rephrase provision (a),

and to consider combining it with provision (b).

Turning to provision (c), the court agrees that "collecting data" goes to the conduct at the heart of this lawsuit, but the court finds this provision to be vague to the extent that it enjoins "collecting . . . data or information from plaintiffs' platforms, whether directly or through a third party, intermediary, or proxy." Given that the parties have made arguments about whether defendants collect data from plaintiffs' servers or directly from the target users' devices, the court would prefer more clarity as to whether or not this provision is intended to cover the collection of data from users' devices.

As to provision (d), covering reverse engineering and decompiling, while the court acknowledges that "the CFAA is best understood as an anti-intrusion statute and not as an anti-misappropriation statute," the court nevertheless concludes that the activities such as reverse engineering or decompiling are sufficiently related to defendants' unlawful access of plaintiffs' and their users' data as to warrant injunctive relief on that basis. See, e.g., Dkt. 795 at 147:21-23 ("it was through reverse engineering that they developed these vectors. It's part and parcel of the CFAA and CDAFA violations."); 165:4-5 ("Reverse engineering is how they developed the exploit that was able to attack our servers."). Accordingly, provision (d) is approved.

Provision (e) covers the sending of harmful code, and provision (f) covers the use of plaintiffs' platforms for "illegal purposes." The court finds that provision (e) is vague and possibly overbroad, and that provision (f) is essentially circular in that it simply requires compliance with all relevant laws. Accordingly, provisions (e) and (f) shall be removed from any revised proposed injunction.

Finally, as to provision (g), 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, the court, in its discretion, concludes that such activity must be enjoined.

Paragraph 4 of the proposed injunction requires defendants to delete and destroy computer code related to plaintiffs' platforms. The court concludes that this provision is

necessary to prevent future violations, especially given the undetectable nature of defendants' technology.

Paragraph 5 requires defendants to affirm that it provided notice of the injunction to all affected parties, and paragraph 6 requires defendants to certify compliance with the injunction. The court has not required defendants to provide such notice and certification in other cases, and will not do so in this case. Additionally, any deadline the court imposes will undoubtedly necessitate further motion practice once the inevitable appeals process begins. Accordingly, paragraphs 5 and 6 are to be removed from any revised proposed injunction.

Finally, defendants argue that the injunction would place an unreasonable burden on its outside counsel, to the extent it prevents them from using Whatapp, and plaintiffs' reply offers to "clarify the proposed permanent injunction to exclude NSO's outside counsel." Dkt. 782 at 14. Plaintiffs shall thus revise paragraph 1 to exclude defendants' outside counsel.

Accordingly, the court directs plaintiffs to file a revised proposed injunction order, making the changes specified above, namely: (1) exclude defendants' sovereign government customers from the scope of the injunction, and (2) narrow the scope of the injunction to apply only to the Whatsapp platform, (3) clarify paragraphs 3(a), 3(b), and 3(c), (4) remove paragraphs 3(e) and 3(f), (5) remove paragraphs 5 and 6, and (6) add language excluding defendants' outside counsel from the injunction. Plaintiffs shall file the revised proposed injunction order within 14 days of the date of this order.

Motion for Remittitur or a New Trial

As stated above, the jury in this case awarded plaintiffs compensatory damages in the amount of $444,719, and punitive damages in the amount of $167,254,000, a ratio of over 376/1. Defendants have filed this motion under Rule 59, asking the court to order a new trial or alter/amend the judgment to reduce the punitive damages award.

A. Legal Standard

The first question presented by defendants' motion is whether the $167.25M

punitive damages award is excessive; and if so, the second question is by how much to reduce the award.

The seminal Supreme Court cases are BMW v. Gore (1996) and State Farm v. Campbell (2003), which prohibit the imposition of "grossly excessive or arbitrary punishments on a tortfeasor" as inconsistent with the due process requirements of the Fifth and Fourteenth Amendments. BMW, 517 U.S. 559 (1996); State Farm, 538 U.S. 408 (2003).

A 2022 opinion from the Ninth Circuit provides a helpful distillation of the due process principles:

> The Supreme Court in BMW of North America, Inc. v. Gore established three guidelines governing whether punitive damage awards comply with due process: (1) the reprehensibility of the defendant's conduct; (2) the disparity between the harm or potential harm suffered by the claimant and his punitive damages; and (3) the difference between the punitive damages and any civil penalties authorized or imposed in comparable cases.

Riley v. Volkswagen Group of America, 51 F.4th 896, 900 (2022).

Those three prongs will guide the analysis.

B. Analysis

1. Reprehensibility

The Supreme Court has said that the degree of reprehensibility is "the most important indicium of the reasonableness of a punitive damages award." State Farm, 538 U.S. at 419 (citing BMW at 575). The Supreme Court went on to articulate how to conduct the reprehensibility analysis:

> We have instructed courts to determine the reprehensibility of a defendant by considering whether: the harm caused was physical as opposed to economic; the tortious conduct evinced an indifference to or a reckless disregard of the health or safety of others; the target of the conduct had financial vulnerability; the conduct involved repeated actions or was an isolated incident; and the harm was the result of intentional malice, trickery, or deceit, or mere accident.

State Farm at 419.

NSO argues that the only factors that possibly favor plaintiffs are the repeated nature of the conduct, and the fact that the jury found malice, oppression, or fraud. NSO

argues that the other factors cut against reprehensibility, as all the harm was economic and caused no lasting damage.

Plaintiffs argue that (1) NSO repeatedly targeted plaintiffs, (2) NSO acted deliberately, (3) NSO sought to conceal its activity, and (4) NSO repeatedly acted with a knowing disregard of plaintiffs' rights.

Defendants cite to cases involving racial discrimination and threats to abortion providers, arguing that the conduct in this case is less reprehensible and thus worthy of a lower punitive damages ratio. See Zhang v. Am. Gem. Seafoods, Inc., 339 F.3d 1020 (9th Cir. 2003); Bains LLC v. Arco Prods. Co., 405 F.3d 764 (9th Cir. 2005); Planned Parenthood of Columbia/Willamette Inc. v. Am. Coal. of Life Activists, 422 F.3d 949 (9th Cir. 2005). However, these cases are far too different from the present case to support any sort of 'apples to apples' comparison. Therefore, rather than trying to compare the reprehensibility of 'unlawful surveillance' vs. 'racial discrimination,' the court simply concludes that some of the reprehensibility factors support plaintiffs' argument, while some support defendants' argument, and then moves on to the next factor, which provides more guidance regarding the proper size of any punitive damages award in this case.

2. Disparity

Courts have rejected any bright-line rule on this factor, but the Ninth Circuit in Riley articulated the relevant precedent regarding proportionality, and set forth three groups: (1) punitive damages are limited to 4/1 where there are significant economic damages and the behavior is not particularly egregious, (2) punitive damages can range from 4/1 to 9/1 where there are significant economic damages and the behavior is more egregious, and (3) punitive damages can exceed 10/1 only if there are insignificant economic damages and the behavior was particularly egregious.

The threshold argument between the parties is whether the $444,719

compensatory damage award in this case is significant[2] or insignificant. Plaintiffs argue that the figure should be considered in the context of the size of the companies involved in the litigation – for both of which, $444,719 is a small amount, when compared to their overall capitalization. Defendants argue that the case law does not allow for such consideration of context, and that the test for whether economic damages are "significant" must be the same in all cases. Specifically, defendants cite cases in which individuals were awarded amounts such as $15,000, $50,000, and $88,000, and argue that, because those amounts were considered "significant" or "substantial" in those cases, then the award in this case must necessarily be "significant." See Bains, 405 F.3d at 776; Planned Parenthood, 422 F.3d at 963-64; Mitri v. Walgreen Co., 60 Fed App'x 528, 530 (9th Cir. 2016). Defendants then argue that, because economic damages were substantial, any punitive damages award ratio is limited to 4/1 under Riley. See Dkt. 747 at 9.

Having reviewed the authority cited by the parties, the court concurs with defendants that the Ninth Circuit has not held that courts may consider context, such as the financial conditions of the parties, when determining whether a compensatory damages award is "significant" or "substantial." However, in this court's view, an amount that would be "significant" to an individual plaintiff in a specific case may be very insignificant to a plaintiff such as Whatsapp or its parent company, Meta. Thus, to best apply the principles articulated in Riley, a "one size fits all" approach to determining significance should be avoided. And under that rationale, a compensatory damage award of $444,719 to a company the size of Whatsapp and/or Meta strikes the court as relatively insignificant.

However, the court is of course cognizant of stepping beyond Ninth Circuit precedent, and moreover, as will be discussed in further detail below, the court's result

[2] Some of the case law uses 'substantial' rather than 'significant' – the Riley case actually uses both at various times. See 51 F.4th at 902. The understanding of the court and the parties, as confirmed at hearing, is that the terms are effectively interchangeable in this context. See Dkt. 795 at 202-03.

on this motion would be the same regardless of whether the compensatory damage award is considered "significant" or insignificant." In short, under Riley, the "significant" vs. "insignificant" distinction comes into play only if a court seeks to approve a punitive damages ratio above 9/1 – in which case, economic damages must be insignificant and the behavior must be "particularly egregious." See 51 F.4th at 902. In this case, the court does not have a sufficient basis for determining that defendants' behavior is "particularly egregious," which means the punitive damages ratio is capped at 9/1, which means it does not matter whether the court concludes that the economic damages are "significant" or "insignificant" – under either conclusion, the ratio is limited to 9/1. Within that range, the court must determine whether defendants' behavior is either (1) "not particularly egregious" (in which case the ratio is capped at 4/1), or (2) "more egregious" (in which case the ratio can be extended up to 9/1). See id.

To be clear, other courts may later determine that behavior such as defendants' is indeed "particularly egregious" and capable of supporting a ratio of even higher than 9/1. In this court's view, at this time, there have simply not yet been enough cases involving unlawful electronic surveillance in the smartphone era for the court to be able to conclude that defendants' conduct was "particularly egregious." As time goes on, more of a shared societal consensus may emerge about the acceptability of defendants' conduct. For now, the court concludes only that defendants' conduct is not so innocuous as to fall in the category of "not particularly egregious," which means that "more egregious" is the most fitting category. Thus, the court concludes that this case falls within category (2) under the Riley framework, which means that the punitive damages ratio cannot exceed 9/1 – in other words, the punitive damages award cannot exceed a maximum of $4,002,471.

Accordingly, based on Riley, the court must conclude that the jury's award was excessive, as it vastly exceeds the $4,002,471, the maximum permissible under Riley. That leaves one question for the court – to what number should the damages award be reduced?

3. Comparable Civil Penalties

The parties appear to agree that this factor is "less important than the other two" in this case, and the court also believes that the lack of any similar cases involving civil penalties limits this factor's usefulness here.

Accordingly, the court's determination must be based on the reprehensibility of defendants' behavior and the disparity between the compensatory damages award and punitive damages award. And as stated above, based on the latter, the constitutional upper limit of any punitive damages award in this case is 9/1.

Within those constitutional guidelines, the court believes that a high-end award is justified. In particular, the repeated, deliberate, and covert nature of defendants' intrusions, and the fact that defendants specifically designed around plaintiffs' attempted fixes, persuade the court that the punitive damages award should not be further reduced.

Moreover, contrary to defendants' arguments, the court finds no basis to conclude that the jury relied on improper factors. To the contrary, in the court's view, the jury displayed an uncommonly high level of attention and engagement, and the court sees no reason to discredit the jurors' reasoning. In addition, the jury was instructed not to "be influenced by any personal likes or dislikes, opinions, prejudices, or sympathy," and to "decide the case solely on the evidence before you," and the jury is presumed to follow the court's instructions. See Dkt. 737 at 2.

Accordingly, defendants' motion is GRANTED, and the jury's punitive damages award is remitted to the amount of **$4,002,471**. Plaintiffs may accept a remittitur to $4,002,471, or the court will order a new trial as to the amount of punitive damages, though the court will be bound by the same constitutional limit on the amount of punitive damages that are set forth in this order, i.e., the 9/1 ratio under Riley.

Remaining motions

Following the court's previous order on the parties' various motions to seal, the parties filed a narrowed joint omnibus motion to seal. See Dkt. 784, 797.

There is a general principle in favor of public access to federal court records.

Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 602 (1978). "[T]he proponent of sealing bears the burden with respect to sealing. A failure to meet that burden means that the default posture of public access prevails." Kamakana v. City & Cnty. of Honolulu, 447 F.3d 1172, 1182 (9th Cir. 2006).

When a request to seal documents is made in connection with a motion, the court must determine whether the parties are required to overcome that presumption with "compelling reasons" or with "good cause." A party seeking to seal materials submitted with a motion that is "more than tangentially related to the merits of the case"—regardless of whether that motion is "technically 'dispositive'"—must demonstrate that there are compelling reasons to keep the documents under seal. Ctr. for Auto Safety v. Chrysler Grp., LLC, 809 F.3d 1092, 1101–02 (9th Cir. 2016). "That the records are connected to a Daubert motion does not, on its own, conclusively resolve the issue." In re Midland Nat. Life Ins. Co. Annuity Sales Pracs. Litig., 686 F.3d 1115, 1119 (9th Cir. 2012). For example, the "compelling reasons" standard applies where the "judicial records at issue were filed 'in connection' with pending summary judgment motions." Id. at 1120 (citing San Jose Mercury News, Inc. v. U.S. Dist. Ct., 187 F.3d 1096, 1102 (9th Cir. 1999)).

"Under this stringent standard, a court may seal records only when it finds a compelling reason and articulates the factual basis for its ruling, without relying on hypothesis or conjecture. The court must then conscientiously balance the competing interests of the public and the party who seeks to keep certain judicial records secret. What constitutes a 'compelling reason' is best left to the sound discretion of the trial court. Examples include when a court record might be used to gratify private spite or promote public scandal, to circulate libelous statements, or as sources of business information that might harm a litigant's competitive standing." Ctr. for Auto Safety, 809 F.3d at 1096–97 (internal quotation marks and citations omitted).

The parties' joint omnibus motion to seal complies with the court's previous order regarding sealing, and has been sufficiently narrowed to cover only truly sealable material. Therefore, the parties' joint omnibus motion to seal (Dkt. 797) is GRANTED.

There are two remaining motions, both filed by defendants. The first is listed on the docket as a motion to seal (Dkt. 790), but that appears to be an error, because the filed document contains no sealed or redacted material, and is in fact a duplicate of the document filed at Dkt. 791, which is properly listed as a motion for leave to file a supplemental reply brief.

Accordingly, the erroneously-filed "motion to seal" at Dkt. 790 is denied as moot, and the motion for leave to file a supplemental reply brief (Dkt. 791) is granted.

CONCLUSION

For the foregoing reasons, plaintiffs' motion for permanent injunction is GRANTED, and defendants' motion for remittitur is GRANTED. The punitive damages award is remitted to the amount of $4,002,471, and plaintiffs shall have 14 days from the date of this order to file a notice stating whether it accepts or rejects the remittitur.

And as stated above, plaintiffs shall have 14 days from the date of this order to file a revised proposed injunction order. Finally, plaintiffs shall file a proposed form of final judgment, to be filed no later than 14 days from the date of this order.

IT IS SO ORDERED.

Dated: October 17, 2025

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

United States District Court
Northern District of California