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 MOTIONS FOR SUMMARY JUDGMENT, MOTION FOR SANCTIONS, AND DISCOVERY LETTER BRIEFS** Re: Dkt. 381, 383, 387, 397, 401, 406, 408, 409, 411

Plaintiffs' motion for summary judgment, defendants' motion for summary judgment/motion to dismiss, and plaintiffs' motion for sanctions came on for hearing on November 7, 2024. Plaintiffs appeared through their counsel, Antonio Perez-Marques, Craig Cagney, Micah Block, Greg Andres, Gina Cora, and Luca Marzorati. Defendants appeared through their counsel, Joseph Akrotirianakis, Matthew Dawson, and Matthew Noller. 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

On October 29, 2019, plaintiffs filed this lawsuit, alleging that defendants sent malware, using WhatsApp's system, to approximately 1,400 mobile phones and devices designed to infect those devices for the purpose of surveilling the users of those phones and devices. Dkt. 1, ¶ 1. The complaint alleges four causes of action: (1) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; (2) violation of the California

Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; (3) breach of contract; and (4) trespass to chattels.

The court dismissed plaintiffs' fourth cause of action under Rule 12(b)(6), and no amended complaint was filed. See Dkt. 111. That leaves only the first three causes of action as operative claims in this case. The allegations underlying the complaint are set forth in detail in the court's previous order on defendants' motion to dismiss. See Dkt. 111. As relevant to this order, the parties' briefs further explain some technical details regarding the parties' respective technologies. To summarize, when users communicate via plaintiffs' software, plaintiffs use a "signaling server" to create an initial connection between two users, and then use a "relay server" to send the communication data between the parties.

Defendants' relevant software products, collectively referred to as "Pegasus," allow defendants' clients to use a modified version of the Whatsapp application – referred to as the "Whatsapp Installation Server," or "WIS. The WIS, among other things, allows defendants' clients to send "cipher" files with "installation vectors" that ultimately allow the clients to surveil target users. As mentioned above, plaintiffs allege that defendants' conduct was a violation of the CFAA, the CDAFA, and a breach of contract.

Plaintiffs now move for partial summary judgment seeking a finding of liability on all claims, leaving only the issue of damages for trial. Defendants move to dismiss or for summary judgment based on lack of personal jurisdiction and for partial summary judgment on the merits of the asserted claims. Plaintiffs also seek sanctions based on defendants' discovery conduct.

DISCUSSION

A. Legal standard

1. Motion for summary judgment

Summary judgment is proper where the pleadings, discovery, and affidavits show that there is "no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). Material facts are those which may affect the outcome of the case. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). A dispute as to a material fact is genuine if there is sufficient evidence for a reasonable jury to return a verdict for the nonmoving party. Id. "A 'scintilla of evidence,' or evidence that is 'merely colorable' or 'not significantly probative,' is not sufficient to present a genuine issue as to a material fact." United Steelworkers of Am. v. Phelps Dodge Corp., 865 F.2d 1539, 1542 (9th Cir. 1989) (citation omitted).

Courts recognize two ways for a moving defendant to show the absence of genuine dispute of material fact: (1) proffer evidence affirmatively negating any element of the challenged claim and (2) identify the absence of evidence necessary for plaintiff to substantiate such claim. Nissan Fire & Marine Ins. Co. v. Fritz Cos., 210 F.3d 1099, 1102 (9th Cir. 2000) ("In order to carry its burden of production, the moving party must either produce evidence negating an essential element of the nonmoving party's claim or defense or show that the nonmoving party does not have enough evidence of an essential element to carry its ultimate burden of persuasion at trial.")

"Once the moving party meets its initial burden, the nonmoving party must go beyond the pleadings and, by its own affidavits or by the depositions, answers to interrogatories, and admissions on file, come forth with specific facts to show that a genuine issue of material fact exists." Hansen v. United States, 7 F.3d 137, 138 (9th Cir. 1993) (per curiam). "When the nonmoving party relies only on its own affidavits to oppose summary judgment, it cannot rely on conclusory allegations unsupported by factual data to create an issue of material fact." Id.

The court must view the evidence in the light most favorable to the nonmoving party: if evidence produced by the moving party conflicts with evidence produced by the nonmoving party, the judge must assume the truth of the evidence set forth by the nonmoving party with respect to that fact. See Tolan v. Cotton, 134 S. Ct. 1861, 1865 (2014); Leslie v. Grupo ICA, 198 F.3d 1152, 1158 (9th Cir. 1999). However, when a non-moving party fails to produce evidence rebutting defendants' showing, then an order for summary adjudication is proper. Nissan Fire, 210 F.3d at 1103 ("If the nonmoving party fails to produce enough evidence to create a genuine issue of material fact, the moving party wins the motion for summary judgment."

2. Motion for sanctions

Federal Rule of Civil Procedure 37(b)(2)(A) provides for sanctions for not obeying a discovery order, specifically providing that "if a party . . . fails to obey an order to provide or permit discovery . . . the court where the action is pending may issue further just orders," including "directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims," or "rendering a default judgment against the disobedient party."

B. Legal analysis

The court will first address the threshold jurisdictional issue raised by defendants' motion, and will then address the merits of the three claims asserted by plaintiffs.

1. Personal jurisdiction

Defendants' summary judgment motion and their opposition to plaintiffs' motion both argue that the court lacks personal jurisdiction. As an initial matter, defendants' opposition to the sanctions motion also contains a single sentence (without elaboration or citation) stating that five cases were filed against defendants, four of which have been dismissed, three of which were for lack of personal jurisdiction and/or forum non conveniens. At the hearing, the court asked defendants for clarification as to which cases they were referring. Defendants identified a case in this district that was voluntarily dismissed by Apple (case no. 21-9078), as well as three other cases:

- Corallo v. NSO, N.D. Cal. (Seeborg, J.), case no. 22-5229, dismissed on September 30, 2024 based on lack of personal jurisdiction and/or forum non conveniens, as plaintiff was a native of Italy and citizen of the Netherlands who resided in St Maarten in the Caribbean at the time of the alleged attacks. ("Corallo is a foreign citizen suing other foreign citizens for conduct initiated from foreign locations. The litigation does not belong in the courts of this state.")
- Dada v. NSO, N.D. Cal. (Donato, J.), case no. 22-7513, dismissed on March 8,

2024 based on forum non conveniens, as plaintiffs were journalists for a newspaper based in El Salvador. ("The nub of this case is entirely foreign, and concerns the use of software produced in Israel to hack devices owned by a Salvadoran news service and used by journalists in El Salvador. Every incident described in the complaint involved Salvadoran journalists covering Salvadoran news stories while working primarily in El Salvador.")

- Elatr Khashoggi v. NSO, E.D. Va., case no. 23-0779, dismissed on October 26, 2023 based on lack of personal jurisdiction, as plaintiff was a citizen of Egypt and had not adequately alleged that she was in Virginia during the alleged attacks.

The key distinction in all of those cases appears to be the citizenship/residency of the plaintiffs. In this case, defendants do not dispute that plaintiffs are citizens of the United States and residents of this district, making the cited cases inapposite.

Turning to the merits of defendants' jurisdictional argument, as was laid out in the court's previous order at the pleadings stage, personal jurisdiction can be established through consent, or by either showing that defendants purposefully directed conduct at the forum state, or that they purposefully availed themselves of the state's laws. See Dkt. 111 at 15-32. The court's previous order concluded that plaintiffs had adequately alleged purposeful direction, see Dkt. 111 at 28, but defendants now argue that the allegations are not supported by the evidence.

As to purposeful direction, the court's previous order went through the relevant analysis, explaining that the test has three elements (1) defendants committed an intentional act, (2) expressly aimed at the forum state, and (3) caused harm that the defendant knew was likely to be suffered in the forum state. Dkt. 111 at 18 (citing Calder v. Jones, 465 U.S. 783, 789-90 (1984)).

The key arguments – both then and now – go to the second element, express aiming. Plaintiffs allege that defendants expressly aimed their conduct at plaintiffs' servers, a significant number of which are in California. Defendants now argue that, while the court was obligated to accept that allegation as true at the pleadings stage, discovery has shown that none of plaintiffs' signaling servers are in California and only some of their relay servers are in California, and more importantly, the choice of which server to use was made by plaintiffs, and thus defendants could not have engaged in any express aiming of servers.

Plaintiffs argue that, because defendants did not produce Pegasus code, there is no way of confirming exactly how the WIS chose which server to use. Defendants self-servingly claim that the WIS functioned in the same way as the official Whatsapp client, but there is no evidence to support that claim. Plaintiffs also argue that, even if the WIS did indeed function in the same way, that was still an intentional choice made by defendants. See Dkt. 418-3 at 15-16.

The limited evidentiary record before the court does show that defendants' Pegasus code was sent through plaintiffs' California-based servers 43 times during the relevant time period in May 2019. See, e.g., Dkt. 418-3 at 13. The evidence before the court is consistent with the court's earlier conclusion, at the pleading stage, that defendants "caused a digital transmission to enter California, which then effectuated a breaking and entering of a server in California." See Dkt. 111 at 23. Accordingly, the court finds that the evidentiary record supports the conclusion that defendants are subject to personal jurisdiction in this district.

Because plaintiffs' argument also implicates defendants' discovery conduct, the court will now address plaintiffs' motion for sanctions.

2. Motion for sanctions

The crux of plaintiffs' sanctions motion is that defendants have failed to produce Pegasus source code in a manner that can be used in this litigation, failed to produce internal communications (i.e., email), and wrongfully imposed temporal limitations on their production/testimony. Plaintiffs ask for terminating sanctions, or in the alternative, evidentiary sanctions.

With regard to the Pegasus source code, plaintiffs point out the history of the court's orders regarding defendants' discovery obligations. In November 2023, the court issued an order balancing (under Richmark) defendants' discovery obligations with its need to comply with Israeli government restrictions, and concluded that defendants would not be entirely excused from discovery, and instead would be required to produce information that was "sufficiently specific and important to the asserted claims in this case." Dkt. 233 at 9.

In February 2024, the court considered specific discovery disputes between the parties, one of which involved defendants' argument that they were required to produce only the "installation layer" of the source code, showing how Pegasus was installed on the target users' devices. The court rejected that argument, because "the complaint contains numerous instances alleging not only that spyware was installed on users' devices, but also that information was accessed and/or extracted from those devices." Dkt. 292 at 4 (emphasis added). Accordingly, the court held that defendants "must produce information concerning the full functionality of the relevant spyware." Id. The court went on to say:

> Defendants' proposal of producing information showing the functionality of only the installation layer of the relevant spyware would not allow plaintiffs to understand how the relevant spyware performs the functions of accessing and extracting data, and thus, the court directs defendants to provide information sufficient to show the full functionality of all relevant spyware. Under Richmark, that information is sufficiently important and specific such that compliance with discovery obligations may not be excused.

Id. at 4-5.

Then, a few months later, plaintiffs moved to compel production of one of defendants' computer servers containing Pegasus source code (referred to as the "AWS" (Amazon web services) server). Defendants claimed that production was not warranted, arguing that the court never technically used the word "granted" in its previous order with respect to the Pegasus code. Defendants argued that they were prepared to file a motion for reconsideration/clarification to pursue their argument that production of source code was not actually required. The court instead issued an order granting plaintiffs' motion to compel the AWS server and "clarify[ing] that the previous order's reference to 'full functionality' was indeed intended to require NSO to produce Pegasus computer code." Dkt. 358 at 5-6. The court then further clarified:

> Accordingly, the court now clarifies that its previous order, dated February 23, 2024, should be read to encompass Pegasus computer code, as well as code that shows the full functionality of any other "relevant spyware." To the extent that information on the AWS server as of November 2020, and which has since been moved to a different server, reflects such computer code, the court orders production of that code under Richmark, as the information is sufficiently important and specific to require production despite the existence of foreign legal restrictions. To be clear, the court is not rebalancing the Richmark factors on this motion, it is simply reiterating the balance that was struck in the previous order. The information showing the full picture of how Pegasus functions – which squarely includes Pegasus computer code – is discoverable under Richmark despite the various restrictions that have been cited.

Id. at 6.

Plaintiffs now argue that defendants have produced Pegasus code in a manner that is unusable in this litigation, as it is viewable only by Israeli citizens while in Israel. And even that production is limited to Pegasus code that was on the one specific AWS server mentioned above, rather than the full set of Pegasus code that would show its full functionality. Plaintiffs cite cases from this district and C.D. Cal. holding that production of source code in a foreign country or "distant" or "relatively inaccessible" location was not compliant with the federal rules. See Dkt. 405 at 19-20 (citing Rambus v. Hynix, 2007 WL 9653194 (N.D. Cal. 2007); Satya v. Martin, 2019 WL 666722 (N.D. Cal. 2019); InTouch Techs. v. VGO, 2012 WL 7783405 (C.D. Cal. 2012)).

Beyond source code, plaintiffs also argue that defendants refused to produce internal communications, including communications about Whatsapp vulnerabilities and about NSO's interactions with the US company Westbridge. Plaintiffs also argue that defendants refused to produce key financial information and refused to answer certain deposition questions.

As mentioned above, plaintiffs ask for terminating sanctions, and alternatively ask for evidentiary sanctions on the following topics: (1) targeting of plaintiffs' California-based servers, (2) location of third-party servers, (3) relationship with Westbridge, (4) use

United States District Court
Northern District of California

of Pegasus by NSO's customers, as well as "additional issues to be determined."

Defendants' opposition makes a number of different arguments, including an argument that the court never ordered them to produce any Pegasus source code beyond what was on the AWS server. See, e.g., Dkt. 429-2 at 8, 17-18.

Defendants also argue that production of the AWS server in Israel is fully compliant with discovery obligations, as plaintiffs could either use Israeli counsel to view the code, or they could seek an export license from the Israeli government to use the code in the US.

Overall, the court concludes that defendants have repeatedly failed to produce relevant discovery and failed to obey court orders regarding such discovery. Most significant is the Pegasus source code, and defendants' position that their production obligations were limited to only the code on the AWS server is a position that the court cannot see as reasonable given the history and context of the case. Moreover, defendants' limitation of its production such that it is viewable only by Israeli citizens present in Israel is simply impracticable for a lawsuit that is to be litigated in this district.

Accordingly, the court concludes that plaintiffs' motion for sanctions must be GRANTED. And while the court concludes that terminating sanctions may be reasonably warranted given that defendants' discovery non-compliance goes to the key facts at issue in this case, the court prefers not to issue such a harsh sanction where lesser ones are available. Thus, the court will impose evidentiary sanctions when appropriate, but will only address the issue of terminating sanctions if plaintiffs are unable to establish their claims in their absence.

The first topic of possible evidentiary sanctions, mentioned above, is defendants' alleged targeting of plaintiffs' California-based servers. The court concludes that, 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 WIS chose which server(s) to use, and thus, an evidentiary sanction is warranted such that the court will conclude that the use of plaintiffs' California-based servers was a purposeful choice made by defendants. Accordingly, the court reiterates its previous conclusion that the record supports a finding that defendants are subject to personal jurisdiction in this district.

3. Merits of the asserted claims

As mentioned above, plaintiffs assert claims for violation of the CFAA, for violation of the CDAFA, and for breach of contract.

a. CFAA

As to the CFAA, plaintiffs allege that defendants violated sections (a)(2) and (a)(4), and also conspired with their clients in violation of section (b). The relevant provisions are as follows:

> (a) Whoever—
>
> …
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer;
>
> …
>
> (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.
>
> …
>
> (b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030.

Plaintiffs' motion also argues that defendants have violated section (a)(6), which prohibits trafficking in password-like information, but they acknowledge that they did not plead section (a)(6). See Dkt. 399-2 at 30, n. 10. Because any claim under section (a)(6) was not pled in the complaint, the court will not consider it now.

The first big dispute on the CFAA, briefly alluded to above, is that plaintiffs now seek to proceed under either a "without authorization" or "exceeds authorization" theory, even though the court's previous order limited them to the "exceeds authorization" theory. See Dkt. 111 at 35-39. The court reasoned that, because all Whatsapp users are authorized to send messages, defendants did not act without authorization by sending their messages, even though the messages contained spyware. Instead, the court held that the complaint's allegations supported only an "exceeds authorization" theory.

The nub of the fight here is semantic. Essentially, the issue is whether sending the Pegasus installation vector actually did exceed authorized access. Defendants argue that it passed through the Whatsapp servers just like any other message would, and that any information that was 'obtained' was obtained from the target users' devices (i.e., their cell phones), rather than from the Whatsapp servers themselves. (Defendants also argue that any 'obtaining' was done by their government clients, rather than by defendants, but that's a separate argument – and in the court's view, fully addressed by section (b) which assigns liability to co-conspirators).

Defendants point to the statutory definitions set forth in § 1030(e)(6), specifically the definition of "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." Defendants argue that the definition shows that the alleged violator must "obtain or alter" information from the same computer that he "access[es]," as shown by the language "the computer."

For their part, plaintiffs point to section (a)(2) itself, which imposes liability on whoever "accesses a computer" in excess of authorized access, and "thereby obtains information from any protected computer," pointing to the word "any."

Neither party cites any case law, either controlling or even persuasive, with a definitive answer to this statutory interpretation question. Plaintiffs, relying on section (a)(2)(C), argue that liability is present if defendants obtain information from any computer, i.e., either from Whatsapp servers or from the target users' devices directly. Defendants, pointing to section (e)(6), argue that any information was obtained from the target users, not from Whatsapp's servers, and thus the CFAA does not apply.

However, the court need not resolve this statutory interpretation question in order to rule on the summary judgment motions. As the parties clarified at the hearing, while the WIS does obtain information directly from the target users' devices, it also obtains information about the target users' device via the Whatsapp servers. See Dkt. 464 at 44 ("before Pegasus is on the device, in the process of getting the Pegasus agent installed on the target device, there is a whole lot of signaling that goes on. . . . They had to fingerprint the device which used a pretty sophisticated set of messaging to get information back to the WIS via the Whatsapp servers about the precise operating system and memory structure of the [target] phone."); see also Dkt. 399-2 at 27 ("NSO also obtained information via the Whatsapp servers from the target device, such as the structure of its operating system and the location of crucial memory files, which a regular Whatsapp user using the Whatsapp client app cannot obtain.").

The analysis for section (a)(4) is largely the same, as it uses the same statutory definition found in section (e)(6). Plaintiffs argue that the information's value is established by defendants' clients' willingness to pay for Pegasus. Defendants challenge the mens rea showing for the 'intent to defraud' (as well as the 'intent' requirement of section (a)(2)), but the fact that defendants redesigned Pegasus to evade detection after plaintiffs first fixed the security breach is enough to prove intent.

Thus, the court GRANTS summary judgment in plaintiffs' favor on the CFAA claim under both section (a)(2) and (a)(4), on the theory that defendants exceeded their authorization. Defendants appear to fully acknowledge that the WIS sent messages through Whatsapp servers that caused Pegasus to be installed on target users' devices, and that the WIS was then able to obtain protected information by having it sent from the target users, through the Whatapp servers, and back to the WIS. Defendants' only arguments go to statutory interpretation (addressed above), and their delegation of Pegasus operation to their clients (addressed by § 1030(b)). The court need not address plaintiffs' alternative argument, that defendants acted without authorization.

b. CDAFA

The CDAFA is the state-law equivalent of the CFAA, with the additional requirement that a computer be unlawfully accessed in California. See, e.g., Meta Platforms, Inc. v. BrandTotal Ltd., 605 F.Supp.3d 1218, 1260 (N.D. Cal. 2022). In the court's view, plaintiffs' evidence regarding California relay servers is sufficient, even without more, and to the extent the statute requires an intent to target a California server, the outcome is the same as it was with respect to the jurisdictional analysis – because defendants' failure to produce Pegasus source code is at least one reason why there is no evidence of exactly how the WIS chose servers, an evidentiary sanction is appropriate to conclude that the WIS did indeed target California servers. Thus, the court concludes that summary judgment must be GRANTED on the CDAFA claim for the same reasons as the CFAA claim.

c. Breach of contract

The elements of a breach of contract claim are (1) the existence of a contract, (2) plaintiff's performance or excused non-performance, (3) defendant's breach, and (4) resulting damages. See, e.g., EDC Techs. v. Seidel, 216 F.Supp.3d 1012, 1015 (N.D. Cal. 2016).

As mentioned above, the breach of contract claim is based on violation of the terms of service, specifically the provisions prohibiting users from "reverse engineering" or "decompiling" Whatsapp products, from sending "harmful code" through Whatsapp, and from collecting user information, from accessing or attempting to access Whatsapp without authorization, and from using Whatsapp for illegal purposes.

Defendants argue that no contract exists because there is no evidence that they agreed to the terms of service. However, defendants cannot meaningfully dispute that agreeing to the terms of service was necessary to create a Whatsapp account and to use Whatsapp, and moreover, defendants have refused to produce information about the phones that were used to create Whatsapp accounts on defendants' behalf. See Dkt. 408. Based on controlling Ninth Circuit case law regarding agreement to terms of service, the court concludes that a contract was indeed formed between plaintiffs and defendants. See, e.g., Laatz v. Zazzle, Inc., 2024 WL 377970 at *7 (N.D. Cal. Jan. 9, 2024); Sellers v. JustAnswer LLC, 73 Cal.App.5th 444, 472 (2021).

Defendants do not dispute that plaintiffs performed their obligations under the contract. That leaves the last two elements, breach and damages.

NSO offers only about two pages of opposition regarding breach. First, they argue that plaintiffs cannot prove when they reverse-engineered or decompiled the Whatsapp program, and therefore it could have been done before any agreement to the terms of service. But as plaintiffs point out, they offer no evidence as to when they did such reverse-engineering or decompiling.

Next, defendants argue that Pegasus was operated by their clients, and thus defendants did not collect any information. Defendants further argue that terms such as 'illegal,' 'unauthorized,' and 'harmful' as used in the terms of service are vague and ambiguous. Finally, defendants argue that plaintiffs waived those contractual provisions by failing to enforce them against any other users. See Dkt. 419-2 at 15-17.

The court finds no merit in the arguments raised by defendants. Defendants do not dispute that they must have reverse-engineered and/or decompiled the Whatsapp software in order to develop the WIS, but simply raise the possibility that they did so before agreeing to the terms of service. However, as discussed above, defendants have withheld evidence regarding their agreement to the terms of service. Moreover, common sense dictates that defendants must have first gained access to the Whatsapp software before reverse-engineering and/or decompiling it, and they offer no plausible explanation for how they could have gained access to the software without agreeing to the terms of service. Accordingly, the court concludes that plaintiffs have sufficiently established breach.

Finally, as to damages, defendants do not dispute that plaintiffs incurred costs investigating and remediating defendants' breaches, which are sufficient to establish the fourth and final element of a breach of contract claim. Accordingly, the court GRANTS summary judgment on plaintiffs' claim for breach of contract.

4. Discovery letter briefs

For the reasons set forth above, the court concludes that summary judgment is warranted even without resolving the disputes raised by the parties' various discovery letter briefs. Thus, the discovery letter briefs (Dkt. 381, 383, 387, 408, 409, 411) are all DENIED as moot, as is the related motion for clarification (Dkt. 404).

5. Motions to seal

At the hearing, the court stated to the parties that it would not seal the material in the parties' briefs, and directed the parties to file unredacted versions of the briefs on the public docket. See Dkt. 464 at 5-6, 94. The parties have since filed unredacted versions of the summary judgment briefs, and have filed briefs on the sanctions motion with limited redactions, with plaintiffs having filed a narrowed motion to seal based on defendants' confidentiality designations. See Dkt. 471.

In light of the court's decision not to seal the summary judgment briefs, the parties are now directed to meet and confer with the purpose of filing an omnibus motion to seal that would cover all material sought to be sealed in the exhibits and declarations in connection with the summary judgment motions. The parties shall have until **January 17, 2025** to file the omnibus sealing motion. Any opposition shall be filed by **January 24, 2025**.

The motion to seal the limited material in the briefing on the motion for sanctions (Dkt. 471) is GRANTED. For the exhibits and declarations filed in connection with the sanctions motion, the parties are similarly directed to meet and confer and to file an omnibus motion with the same briefing schedule as above.

CONCLUSION

For the foregoing reasons, plaintiffs' motion for partial summary judgment is GRANTED, defendants' motion for summary judgment is DENIED, and plaintiffs' motion for sanctions is GRANTED in part and DENIED in part.

Because this order resolves all issues regarding liability, a trial will proceed only on the issue of damages. The parties have already filed motions related to their experts – specifically, a motion to substitute and a motion to strike – the parties are directed to meet and confer to determine if any expert-related motions are mooted by this order, and to notify the court by **January 17, 2025** which, if any, expert-related motions need to be resolved by the court prior to the trial on damages.

IT IS SO ORDERED.

Dated: December 20, 2024

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