JOSEPH N. AKROTIRIANAKIS (Bar No. 197971)
jakro@kslaw.com
AARON S. CRAIG (Bar No. 204741)
acraig@kslaw.com
KING & SPALDING LLP
633 West Fifth Street, Suite 1600
Los Angeles, CA 90071
Telephone: (213) 443-4355
Facsimile: (213) 443-4310

Attorneys for Defendants NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

WHATSAPP INC., a Delaware corporation, and FACEBOOK, INC., a Delaware corporation,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No. 4:19-cv-07123-PJH

DEFENDANTS NSO GROUP TECHNOLOGIES LIMITED AND Q CYBER TECHNOLOGIES LIMITED'S OPPOSITION TO MOTION FOR SANCTIONS

Date: N/A
Time: N/A
Ctrm: 3

Action Filed: 10/29/2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

I. INTRODUCTION

This was the first of five ill-conceived lawsuits filed against Defendants in the United States amidst a wave of negative press coverage. Four cases have been dismissed, three by courts finding a lack of personal jurisdiction and/or *forum non conveniens* and the fourth voluntarily by the plaintiff (who resided in this District) for reasons related to the *forum non conveniens* factors. Plaintiffs are aware that their jurisdictional allegations against Defendants were untrue and attempt through this motion to establish personal jurisdiction without proof of any purposeful direction.

There is no basis for any sanction, let alone terminating sanctions, because Defendants have not violated any order. Plaintiffs make an over the top request for terminating sanctions in the hope that the Court will take a "split the baby" approach and award a lesser issue sanction concerning the personal jurisdiction Plaintiffs know they cannot otherwise establish. The Court should see through this gamesmanship.

Defendants suspect that Plaintiffs' endgame, since the Court's 2020 denial of Defendants' Motion to Dismiss, has been to (1) seek discovery orders compelling production of export-controlled information, (2) hope that Defendants would not produce it, and (3) seek sanctions at the close of discovery. Defendants have complied with the Court's discovery orders, however, in spite of the extreme difficulty in doing so. This case has not involved the gigantic document production that has become characteristic of commercial litigation in the United States (though Defendants have produced just shy of 5,000 documents and over 46,000 pages, plus the AWS server). That is because of the export-controlled nature of the evidence at issue and the [redacted] of producing it. But it does not mean Defendants failed to meet any discovery obligations or to comply with the Court's orders. Rather, Defendants complied to the letter of this Court's discovery orders and their competing obligations under Israeli law.

Following the Court's February 23, 2024, Order (Dkt. No. 292, the "February Order"), Defendants' lead counsel traveled to Israel for a full week to work with NSO to locate documents that would satisfy Defendants' discovery obligations. Defendants then [redacted] to allow them to comply with the

Court's orders.[1] Defendants were thus able to produce, on August 23-24, 2024, nearly 14,000 documents sufficient to show the full functionality of the Accused Technologies, including 9,311 files of Pegasus code—the image of the AWS Server the Court ordered be produced.

Although Defendants have complied with the Court's orders, Plaintiffs have brought this motion, hoping to have the case determined other than on its merits. No sanctions are warranted, however, because Defendants have not violated any order. When the Court compares Defendants' discovery efforts to its discovery orders, it should easily deny this motion and impose no sanctions, including the personal jurisdiction-related issue sanction Plaintiffs hope for to save their complaint.

II. BACKGROUND

A. Plaintiffs Repeatedly Deceived the Court, Including in its *Richmark* Balancing.

In its September 5, 2024, Order relating to Plaintiffs' failure to serve a privilege log, the Court reprimanded Plaintiffs for their failure to correct a representation they made to the Court which led to unnecessary motion practice and a waste of the Court's (and Defendants') resources. (Dkt. 377.) It has become clear that such deception was not a one-off mistake; it has been a key part of Plaintiff's litigating strategy dating back to the outset of the case.

First, Plaintiffs made specific representations in the Complaint on which the Court relied in denying Defendants' motion to dismiss for lack of personal jurisdiction: "Defendants' program sought out specific [Plaintiffs'] servers—including servers located California—in order to transmit malicious code through those servers." (Dkt. No. 111 at 22:7-9.) Discovery has shown that allegation to be false: WhatsApp has two types of relevant servers, signaling servers and relay servers. No WhatsApp signaling servers were (or are) located in California. Only a small fraction of WhatsApp relay servers are located in California, and those servers are selected based not on the product of any human choice, but on computer algorithms that are part of Plaintiffs' server architecture. (McGraw Decl. ¶ 4; Gazneli Decl. ¶ 11.) In other words, Defendants' program, Pegasus, did nothing to seek out those servers. (Dkt. No 396-2 at 8-11.) There is accordingly no purposeful direction, and no personal jurisdiction. Plaintiffs have known this from the outset, but

[1] As Defendants informed the Court, [redacted], and it did.

did nothing to correct the misrepresentation they made to the Court.

Plaintiffs also omitted vital information from the Court in obtaining the Court's February Order, and in their subsequent motion to compel production of the AWS server that led to the Court's August 1, 2024 Order (Dkt. No. 358, the "August Order"). Namely, Plaintiffs did not tell the Court (or Defendants) they already had a copy of the AWS Server until *after* the Court ordered Defendants to produce their copy.[2] Plaintiffs devoted an entire section of their July 5 motion to compel to their supposed "Efforts to Obtain Information Regarding the AWS Server," which completely omitted the fact that ***Plaintiffs already had a copy of the AWS server***. (Dkt. No. 331.) This motion also included statements obviously designed to mislead the Court into affirmatively believing that Plaintiffs *did not* have a copy of the AWS server, such as: "By removing the Pegasus code from the AWS Server, NSO deprived Plaintiffs of a means of obtaining it. Given NSO's reluctance to produce responsive information from Israel, NSO's removal or deletion of copies outside Israel may deny Plaintiffs access to the relevant discovery." (Dkt. 331 at 6:28-7:2.) Because the first element of the *Richmark* analysis is "the importance to the investigation or litigation of the documents or other information requested" (Dkt. 292 at 2), and because Plaintiffs' possession of its own copy of the AWS Server would substantially decrease the importance of its request for a duplicate copy. Plaintiffs' deception misled the Court and prejudiced Defendants—especially given that Plaintiffs were asking for NSO to be ordered potentially to violate Israeli law.

B. Defendants Have Produced all Discovery Ordered (and Substantially More).

Because Plaintiffs' Motion accuses Defendants of violating two Court Orders, it is critical to review the content of those Orders closely. First, neither the February Order nor the August Order compelled any *deposition* discovery, and Plaintiffs have never sought any order compelling any deposition discovery. So it is unclear why Plaintiffs argue that four full-day depositions of Defendants' employees provides a basis for any sanction, let alone terminating sanctions.

With respect to *document* discovery, the February Order granted in part Plaintiffs' motion

[2] Plaintiffs did not divulge the fact that they had their own copy of the AWS server until the August 30, 2024, service of their expert report of David Youssef (Craig Decl. Exh. 6), or, arguably, their portion of a joint letter brief filed August 13, 2024 (Dkt. No. 359-2).

to compel (Dkt. 236). The Court analyzed the disputed issues according to the four categories by which those issues were briefed. The Court granted the motion as to categories 1 and 2 and denied the motion as to categories 3 and 4. In granting the motion as to category 1, the Court adopted Plaintiffs' definition of the Accused Technologies[3] and set the relevant time period as April 29, 2018, to May 10, 2020. The Court allowed for the possibility that Plaintiffs could seek further discovery for later time periods if they were "able to provide evidence that any attack lasted beyond that timeframe" (February Order at 4:4-7), but Plaintiffs never did so.

In granting the motion as to category 2, the Court ruled that Defendants' production should not be limited to the "installation" layer: "Defendants' proposal of producing information showing the functionality of only the installation layer of the [Accused Technologies] would not allow plaintiffs to understand how the [Accused Technologies] 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 [Accused Technologies]." (February Order at 4:28-5:4.)

The Court denied Plaintiffs' motion as to categories 3 and 4, but several months later clarified its ruling regarding part of category 4. The Court's August Order stated: "The motion is granted to the extent that plaintiffs seek production of information related to the [Accused Technologies] (including Pegasus computer code) *that was housed on the AWS web server and was subsequently preserved*." (August Order at 7:17-19 (emphasis added).) This was precisely the information Plaintiffs sought in their RFP No. 30: "A complete Image of the Device or Devices that resolve to the Internet Protocol (IP) Address 54.93.81.200." To the extent Plaintiffs' motion suggests Defendants have violated the Court's August Order by failing to produce computer code located on devices *other than* the AWS server, that is outside the scope of *both* what the Court ordered *and* what Plaintiffs requested in discovery.

Plaintiffs' motion to compel was not a model of clarity as to the document requests it put at issue, but Plaintiffs' proposed order made clear that they sought an order compelling production of the following Requests for Production, *as narrowed by Plaintiffs*: Nos. 1, 3, 5, 7, 9, 10, 14, 15,

[3] Plaintiffs have used the pejorative term "Relevant Spyware" throughout this litigation. Defendants respectfully request that the Court use the more neutral term "Accused Technologies."

16, 17, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 30, 72, 73, 75, 76, 78 and 79. (Dkt. 236-1 ¶¶ 2-3).[4] Category No. 3 (denied) requested an order for RFP No. 25, seeking interactions between Defendants and their customers. Category No. 4 (also denied) sought an order as to RFP Nos. 22, 23, 30, 72, 73, 75, 76 and 78. In the clarifying August Order, the Court granted Plaintiffs motion as to RFP No. 30 and required Defendants to produce the AWS server prior to September 13, 2024.

Giving the Court's orders their broadest possible interpretation, the Court therefore compelled Plaintiffs to produce documents responsive to RFP Nos. 1, 3, 5, 7, 9, 10, 14, 15, 16, 17, 19, 20, 21, 24, 26, 27, 28 and 30, *as narrowed by Plaintiffs* (the "Motion RFPs").[5] (Plaintiffs' narrowed production requests were set forth in a November 30, 2023 letter from Plaintiffs' counsel, Craig Decl. Exh. 3.)

With the exception of RFP Nos, 5, 17, 26, 28 and 30, all of the Motion RFPs sought documents "sufficient to show," "sufficient to describe," or "sufficient to identify" certain information. On August 23-24, 2024, [redacted] Defendants made a very substantial document production. This included (1) 9,311 native computer code files comprising Defendants' copy of the AWS server; and (2) 4,444 documents (totaling 45,304 pages). (Craig Decl. ¶ 7.) Production of the computer code files was made to Plaintiffs' counsel of record in Israel, who acknowledged his receipt of them. (Craig Decl. Exh. 7.) Defendants' total production of documents (i.e., not computer code files) is comprised of 4,933

[4] Plaintiffs' motion also sought supplemental interrogatory responses, which Defendants produced during the discovery period. (Craig Decl. Exh. 1.) Those responses, the sufficiency of which Plaintiffs apparently acknowledge, provided an enormous amount of information about the full functionality of the Accused Technologies. This included a five-page response to Interrogatory No. 2 ("Describe how each of the NSO Spyware identified in response to Interrogatory No. 1 functioned, including how it was designed to be installed on a Device, the methods used to install it on a Device, how it was used after being installed on a Device, how it exfiltrated data from a Device on which it was installed, and how it accessed or used any WhatsApp Computers.") (*Id.*)

[5] The Court also ordered the production of what Defendants "agreed to produce" (February Order at 3:8-10), which was set forth in the second column of Dkt. No. 235-4, Exhibit P, Plaintiffs' First Set of Requests for Production. The information Defendants agreed to produce, however, is simply a subset of the information requested by Plaintiffs and ordered by the Motion RFPs, and therefore no separate analysis is required.

documents and 46,542 pages over 12 productions. (Craig Decl. ¶ 7.)

The materials Defendants produced on August 24, 2024, were sufficient to show the full functionality of the Accused Technologies, and were fully responsive to the Motion RFPs, other than of RFP Nos. 5 and 10 (identification of WhatsApp vulnerabilities), 28 (NSO communications with Westbridge) and 30 (AWS server). (Gazneli Decl. ¶ 5; Craig Decl. ¶¶ 16-28.) As to RFP Nos. 5 and 10, Defendants were unable to locate any responsive documents in spite of a diligent and good faith search. (Ganzeli Decl. ¶¶ 8-9; Craig Decl. ¶ 23-26.) As to RFP No. 28, an oversight delayed production of responsive documents—a fact of which Plaintiffs were informed prior to the filing of this Motion (Craig Decl. ¶ 20), and those documents were produced on October 7, 2024 (Craig Decl. Exh. 10). As to RFP No. 30, Defendants produced their preservation copy of the AWS Server on August 23, 2024 (Gazneli Decl. ¶ 4), three weeks prior to the discovery cutoff and before the deposition of any of Defendants' employees. That production was made to Israeli attorney Ronald Lehmann (Craig Decl. Exh. 7), who has been Plaintiffs' counsel of record since the Court granted his pro hac vice application in March 2023. (Dkt. No. 175.)

Plaintiffs' sanctions motion is vague as to which RFPs they claim Defendants failed to satisfy. It includes argument only about RFP Nos. 5, 17, 28, the AWS Server (RFP No. 30), and a price list that Defendants were never ordered to produce. Defendants focus their argument below on these issues. Due to the severity of Plaintiffs' allegations (baseless though they are), however, Defendants submit to the Court information demonstrating their compliance with *each of the Motion RFPs*. (Craig Decl. Exhs. 1, 13-18 and 21-99 and ¶¶ 19-28.) Defendants do not lightly burden the Court with the volume of materials submitted herewith, but believe this submission is appropriate to demonstrate their compliance with the Court's Order to produce documents showing the full functionality of Pegasus, as well as with each of the Motion RFPs.

C. Plaintiffs' Attempted Mudslinging About the [redacted] Has Nothing to Do with This Discovery Dispute.

Plaintiffs devote nearly five pages (pages 3-4 and most of pages 16-18) to irrelevancies [redacted] (Dkt. No. 195 Exhs. A-B). Because the [redacted]

[redacted]

Defendants properly objected to discovery and 30(b)(6) deposition topics about it.[6] Plaintiffs never moved to compel discovery about [redacted], and this Court never ordered any such discovery. [redacted] thus has no place in a motion for sanctions.

The declarations of Defendants' Israeli counsel, Defendants' statements to the Court, and Defendants' RFA responses were truthful (and in any event not inconsistent with the error-riddled "public reporting"[7] upon which Plaintiffs rely), despite Plaintiffs' innuendo to the contrary. Defendants told the Court that [redacted] Both of those statements are true. [redacted]

[redacted] is not surprising and does not contradict Defendants' statements. It takes little imagination to see that there is no contradiction: [redacted]

To the extent Plaintiffs are seeking sanctions because they think Defendants' responses to Plaintiffs' requests for admissions (Block Decl. Exh. A) are different from what has been reported in the press, Defendants stand by the accuracy of those responses—even though these RFAs were

---

[6] [redacted]

[7] The basis for this reporting, according to the *Guardian* article, is a "hack of data from Israel's Ministry of Justice," as to which the "authenticity of the emails" is not "verif[ied]."

[8] [redacted]

served as to improper subject matter having nothing to do with the issues to be tried.[9] Moreover, no Rule 36(a)(6) motion has been brought regarding the sufficiency of Defendants' responses to Plaintiffs' RFAs about [redacted], and there is no basis for sanctions. If Plaintiffs believe Defendants' denials of their RFAs were improper, their sole remedy would be to file a post-trial Rule 37(c)(2) request for expenses incurred proving matters not admitted.

III. ARGUMENT

Plaintiffs rely exclusively on Rule 37(b) (as opposed to any other authority), as the basis for their motion, and Defendants respond accordingly. Rule 37(b), entitled "Failure to Comply with a Court Order," authorizes sanctions only "if [a] party fails to comply with a court's order to provide or permit discovery." *Unigard Sec. Ins. Co. v. Lakewood Eng'g & Mfg. Corp.*, 982 F.2d 363, 367-68 (9th Cir. 1992). "This court . . . has foreclosed the application of Rule 37 sanctions . . . where a party's alleged discovery-related misconduct is not encompassed by the language of the rule." *Id.*at 368. "Rule 37(b)(2) has never been read to authorize sanctions for more general discovery abuse." *Id.* "To impose sanctions pursuant to Rule 37(b) . . . a party must have violated a discovery order." *Nida v. Allcom*, 2020 WL 2405251, at *6 (C.D. Cal. Mar. 11, 2020).

A. Plaintiffs' Motion Does Not Comply with the Civil Local Rules.

The Court should strike Plaintiffs' motion for not complying with Civil Local Rules 7-2(b), 7-2(c), and 7-8. Plaintiffs' sanctions motion exceeds the Court's 25-page limit (Dkt. No. 405-2), does not include notice of the motion within the 25 pages, and lacks a statement of relief sought.

B. Production of the AWS Server Code In Israel Is Not Sanctionable.

There are numerous reasons why producing the AWS server in Israel is not sanctionable.

To begin with, Defendants complied with the Court's order compelling production of the AWS server. The Court ordered: "the motion is granted to the extent that plaintiffs seek production of information related to the [Accused Technologies] (including Pegasus computer code) that was housed on the AWS web server and was subsequently preserved." To comply, Defendants

[9] RFAs are intended to streamline trials, not to inquire about discovery disputes. RFAs "serve[] two vital purposes, both of which are designed *to reduce trial time*." Fed. R. Civ. P. 36, Notes of Advisory Committee on Rules—1970 Amendment (emphasis added).

produced 9,311 files of Pegasus code—a complete copy of their preservation copy of the AWS server to Plaintiffs' counsel of record in Israel. (Gazneli Decl. ¶ 4.) The Protective Order allows for a party to comply with its discovery obligations by making source code merely *available for review*, and Defendants could have followed that procedure, but that is not what Defendants did. Because Defendants produced all the information related to the Accused Technologies (including computer code) from the AWS server files, there is no daylight between what the Court ordered and what Defendants did, and therefore there is no sanctionable conduct.

Moreover, Plaintiffs Second Set of Requests for Production, including RFP No. 30 seeking the AWS server, did not specify a place for production. Rather, Plaintiffs simply asked Defendants to "produce and permit the inspection and copying of the Documents and things described below, within thirty (30) days after the date of service." (Craig Decl. Exh. 5.) The Court's August Order likewise did not specify any place of compliance. Production of source code in Israel (the only lawful place Defendants could produce this export-controlled material) (Gelfand Decl. ¶ 9; Gazneli Decl. ¶ 10) did not violate any order.

Defendants produced the AWS server files in the format in which NSO ordinarily maintains them. (Gazneli Decl. ¶ 4.) Plaintiffs argue that Defendants violated the requirement of Rule 34(b)(2)(E)(ii) that electronically stored information be produced "in a form . . . in which it is ordinarily maintained or in a reasonably usable form." They argue that Defendants produced the files in Israel where they cannot be used. The "usability" requirement plainly relates to the *file format* in which ESI is produced, not the location. Moreover, this requirement is plainly disjunctive. A producing party can produce ESI *either* in the form in which it is ordinarily maintained *or* in some other reasonably usable form—"a party need not produce the same electronically stored information in more than one form." Fed. R. Civ. P. 34(b)(iii). Defendants produced the AWS server as it was ordinarily maintained. There are no cases holding that production of ESI in the form it was ordinarily maintained violates Rule 34(b)(2)(E)(ii).

And, Plaintiffs have not submitted any evidence to support their foundational claim that they cannot use in this litigation the AWS server produced by Defendants. Notably, Plaintiffs have produced no declaration from their Israeli counsel of record, or anyone else, showing what efforts

Plaintiffs have made to obtain an export license from DECA. The Court should make no assumptions about Plaintiffs' efforts to obtain an export license. Particularly considering Plaintiffs' litigation conduct, it is entirely possible Plaintiffs received an export license and are concealing it until an opportune time—just as they did with the copy of the AWS server they have had for a year or more.

Plaintiffs *can* use the AWS server, even if they do not receive an export license. Even if Plaintiffs have been unable to obtain an export license from DECA, it does not follow that the AWS server is unusable in this litigation. Plaintiffs could engage a technical expert *in Israel* to review the AWS server. (Block Decl. Exhs. J, L.) That expert could analyze the AWS server and testify about it, or could compare it with Plaintiffs' own copy of the AWS server to authenticate Plaintiffs' copy, and Plaintiffs could then use their own copy.

Contrary to Plaintiffs' assertion, Defendants have never told Plaintiffs that they cannot use in litigation the AWS server produced in Israel. WhatsApp claims that "according to NSO," the Israeli production "cannot be used in the litigation or in trial." (Mot. at 11:8.) That is simply a lie. The transmittal letter accompanying production of the AWS server (and upon which Plaintiffs rely to support this false statement) is that Defendants were unaware of any license allowing for export and that counsel for Plaintiffs should "obtain any licenses that may be required before transmitting export-controlled restricted materials outside of Israel." (Block Decl. Exh. H.) That is *not remotely* the same as stating that the production cannot be used in litigation or in trial. Moreover, this admonition essentially matches the admonition *Plaintiffs* provided with each of *their* productions of technical materials, which helpfully reminded Defendants' counsel that sharing these materials with their client might violate U.S. law.[10]

---

[10] Plaintiffs' transmittal letters include the statement: "For the avoidance of doubt, by making this production and Plaintiffs' prior productions available to U.S. counsel for Defendants in the United States, Plaintiffs are under no obligation to determine, and do not take any position on, whether any of the produced documents are subject to the U.S. Department of Commerce's Bureau of Industry and Security Export Administration Regulations, 15 C.F.R. §§ 730.1, 730.6, or whether any such documents may be further transmitted to Defendants or any other party restricted from receiving such documents under those regulations. It is the obligation of King & Spalding to comply with all its legal obligations in that regard, and to obtain any licenses necessary before transmitting such documents to Defendants or any other entities." (Craig Decl. Exh. 8.)

Plaintiffs have not been prejudiced by Defendants producing the AWS server in Israel. Plaintiffs informed Defendants and the Court that the U.S. Department of Justice gave them a copy of the AWS server. Plaintiffs can use their own copy for whatever purpose they wish. Plaintiffs' copy of the AWS server includes small sections apparently redacted by FBI, but Plaintiffs have not claimed that the redacted material relates to any issue in the case. Plaintiffs also have not claimed that their copy of the AWS server is any different from the copy they received in Israel, or that if there are any differences between the two, those differences are material to any issue in the case. Plaintiffs' own version of the AWS server shows that, for the one version of Pegasus that sent messages across WhatsApp relay servers (Eden), it was the WhatsApp infrastructure, and not Pegasus, that selected which WhatsApp relay servers to use based on latency (thus proving the absence of any purposeful direction, and therefore no personal jurisdiction), although Plaintiffs withheld the files that most clearly demonstrate this important fact until the last day of fact discovery. (McGraw Decl. ¶¶ 3-4; Craig Decl. Exh. 100 and ¶ 15.)

In any event, Defendants should not be sanctioned for not doing something Plaintiffs acknowledge they are also unable to do because of foreign legal restrictions. Israel's DECL precludes exporting the Pegasus code in the AWS server files because that code is Defense Know-How. (Gelfand Decl. ¶ 9, Gazneli Decl. ¶ 10.) Plaintiffs ask the Court to sanction Defendants for not exporting the AWS server files. Plaintiffs are now equally in possession of the same files, and acknowledge they too cannot export them. Sanctions would not be appropriate in these circumstances. *Wyndham Vacation Ownership, Inc. v. Clapp Business Law, LLC*, 2020 WL 3266059, at *3 (M.D. Fla. Apr. 2, 2020) (where the non-moving party demonstrates impossibility, through more than mere assertions, the moving party must prove that compliance with order was possible in order to obtain sanctions); *cf. S.E.C. v. Custable*, 1999 WL 92260, at * (N.D. Ill. Feb. 11, 1999) (a court should not impose contempt sanctions where compliance with order is impossible); *United States v. Rylander*, 460 U.S. 752, 757 (1983) (same); Fed. R. Civ. P. 37(b)(2)(A) (sanctions orders must be "just"). If Plaintiffs' response to this is that the Court's orders apply to Defendants and not Plaintiffs, Defendants respond that the Court's orders did not

specify a place for production.[11]

Plaintiffs' cases are easily distinguishable. WhatsApp cites three cases that it claims show Defendants' noncompliance with the supposed requirement to produce ESI be in "reasonably usable form." (Mot. at 11-12.) In each of those cases, the producing party merely offered to *make available for inspection* computer code or other materials in a distant foreign location. Here, Defendants did not offer merely to make available the AWS server; Defendants gave Plaintiffs their own copy, containing the files in the same format in which they are maintained by Defendants. (Gazneli Decl. ¶ 4.) That distinction is everything. In a case not cited by Plaintiffs, *Seoul Semiconductor Co., Ltd. v. FEIT Electric Co, Inc.*, 2024 WL 1136525 (C.D. Cal. Jan. 9, 2024), the court required the defendant to travel to South Korea to review the accused products, even though plaintiff had purchased those products in the United States and then exported them to South Korea for testing, and even though there were no foreign law issues of any kind that would have prevented plaintiff from bringing them back to the United States. That court distinguished Plaintiffs' case of *Rambus Inc. v. Hynix Semiconductor Inc.*, 2007 WL 9653195 (N.D. Cal. Sept. 25, 2007), because the primary issue in *Rambus* was that the *format* of the production was not electronically searchable (and therefore not in "reasonably usable form"). That is not at issue here.

A sanction here would be unprecedented. Defendants have found no case imposing sanctions for producing materials in a particular location where no place of production was specified in either the production request or the court order.

For at least these reasons, production of the AWS server in Israel is not sanctionable.[12]

C. Plaintiffs Now Possess Information Sufficient to Show the Full Functionality of All Accused Technologies.

Plaintiffs' attempt to rewrite the Court's Orders as requiring the production of code from

[11] Principles of comity militate against the Court from sanctioning Defendants for not violating Israeli law—particularly now that Plaintiffs acknowledge that they are likewise prohibited by that same law from exporting those same materials.

[12] There is an easy and obvious solution to the inability to export the AWS server files without a license: the Court should dismiss this case for lack of personal jurisdiction and/or *forum non conveniens*, and Plaintiffs can refile it in Israel. That would not only be the correct result as a matter of law, Plaintiffs could then also use both their copies of the AWS server without restriction.

sources other than the AWS server (Mot. at 10:1-14) is unavailing. The only specific code that Plaintiffs sought in their "Motion to Compel Discovery *Regarding AWS Server*" was code housed on the AWS Server. (Dkt. No. 331, asking, on page 1, the Court to "order NSO to produce relevant *documents and information from the AWS Server*.")[13] The Court's August Order granted that request and instructed Defendants to produce information relating to the Accused Technologies "(including Pegasus computer code) that was housed on the AWS web server." (August Order 7:17-19.) Defendants have now produced that information—which Plaintiffs claim to have also acquired from the U.S. Department of Justice. In light of this, asking for sanctions because Defendants have not produced code from other sources is a massive overreach.

The Court should not compel production of any other computer code because Plaintiffs now possess information sufficient to show the full functionality of the Accused Technologies. The February 2024 Order determined that discovery into the functioning of Pegasus should not be limited to the installation layer, and thus required Defendants to "provide *information sufficient to show* the full functionality of all relevant spyware." (February Order 4:28-5:5 (emphasis added).) Defendants did not produce *other* code *not found on the AWS server* because their production is otherwise sufficient to show the full functionality of the Accused Technologies, even apart from the AWS server files. Defendants' document production, supplemental interrogatory responses, and deposition testimony of Tamir Gazneli amply set forth the full functionality of all of the Accused Technologies: the Pegasus/Phantom versions that used the installation vectors Heaven, Eden and Erised (Craig Decl. ¶ 28 and Exhs. 1-2, 24-28, 32-95; Gazneli Decl. ¶ 5). And while Plaintiffs argue that the AWS server is only "part of the Pegasus system," they fail to identify any information about the Accused Technologies for which they need any other code to discern. (*See* Mot. at 9:15-12:19.)[14] Plaintiffs clearly do not require more code to discuss how the Accused

---

[13] The only document request at issue in that motion was Plaintiffs' Request No. 30, which sought only an image of the AWS server, not any other computer code. (*Id.* at 3 ("NSO Should Be Compelled to Provide Discovery Responsive to Plaintiffs' Request for Production No. 30.")).

[14] Plaintiffs also cite a portion of Tamir Gazneli's testimony where he was uncertain whether the AWS server code included the entirety of the code for the Erised delivery vector. After his deposition, Mr. Gazneli checked the AWS server code and confirmed it did include Erised.

Technologies "target Plaintiffs' servers" (the central issue in the case) (Mot. 20:18-20), as they moved for summary judgment on that very point—which included a detailed analysis of exactly how the Accused Technologies interacted with WhatsApp's server (*see* Dkt. No. 399-2 at 11-18). In addition, Plaintiffs have opposed Defendants' motion for summary judgment on the merits and do not argue that any additional discovery is required under Rule 56(d). (*See generally* Dkt. No. 418-3.) Accordingly, it is undisputed that Defendants produced information in discovery sufficient to show the full functionality of all Accused Technologies.

Finally, Plaintiffs argue that Mr. Gazneli reviewed code prior to his deposition. (Mot. at 12:5-19.) The code Mr. Gazneli reviewed prior to his deposition *was* the AWS server code, (Gazneli Decl. ¶ 6), which has been produced. For example, Mr. Gazneli testified he reviewed the code used to "fingerprint" the target device, which is an early step in the installation process. (Block Decl. Exh. N at 12:20-13:6.) That code is on the AWS server (Gazneli Decl. ¶ 6), including, for the avoidance of doubt, the copy of the AWS server that Plaintiffs received from DOJ (Craig Decl. Exh. 100 and ¶ 15). The cases ordering production of documents reviewed by corporate representatives in preparing for Rule 30(b)(6) deposition are of no moment because Defendants produced this ESI nearly two weeks *before* Mr. Gazneli's September 4, 2024, deposition. In any event, the proper remedy for a failure to produce documents relied on by a witness to prepare for deposition would not be terminating or issue sanctions, as Plaintiffs' own cases cited on page 12 make clear. *Converse v. Vizio, Inc.*, 2019 WL 3322383 (W.D. Wash, July 23, 2019) (granting motion to compel, no mention of sanctions); *Seven Seas Cruises S. D.E.R.L. v. V. Ships Leisure Sam* 2010 WL 5187680 (S.D. Fla. Dec. 10, 2010) (granting motion to compel, denying sanctions.)

D. Defendants Have Fully Responded to the Motion RFPs, Including Documents Sufficient to Show the Accused Technologies' "Full Functionality"

The Court granted Plaintiffs' motion to compel only with respect to the Motion RFPs. Of those eighteen RFPs, thirteen require production of documents "sufficient to show," "sufficient to describe," or "sufficient to identify" certain information. These formulations were negotiated by

(Gazneli Decl. ¶ 7.) Defendants' counsel so informed Plaintiffs' counsel during a conference of counsel on September 30—a fact Plaintiffs omit from their motion. (Craig Decl. ¶ 21.)

the parties through several conferences of counsel, and they give Defendants certain latitude in determining how to comply with the Motion RFPs. Moreover, any determination that Defendants have failed to comply would require an evaluation of Defendants' production as a whole.

Here, Defendants and their counsel met for a week at Defendants' offices in Israel, and during that time, worked intensively on the project to locate and produce documents sufficient to show, describe and identify the matters that were the subject of the Motion RFPs. (Craig Decl. ¶ 3.) These materials are [redacted] Defendants produced these 4,444 documents to Plaintiffs on August 24, 2024. (Craig Decl. ¶ 7.)

Defendants have prepared a table setting forth the topics of the Motion RFPs, with examples of the documents Defendants produced that are sufficient to show, describe, or identify the material sought by the Motion RFPs. (Craig Decl. ¶ 28.) As a practical matter, Defendants cannot provide the Court with every single document produced in discovery, but Defendants have attempted to give the Court a fair cross-section of their production, which collectively demonstrates the full functionality of the Accused Technologies, *i.e.* the versions of Pegasus/Phantom at issue in this case. (Craig Decl. Exhs. 1, 24-28, 32-95.) Defendants' supplemental interrogatory responses and the deposition of Tamir Gazneli also provided Plaintiffs with an enormous amount of information about the full functionality of the Accused Technologies. (Craig Decl. Exhs. 1-2.) Plaintiffs' reply will no doubt nitpick that some aspect of the Accused Technologies is not covered by the voluminous materials Defendants are submitting in opposition. It is impossible to preempt every argument Plaintiffs might make. Defendants would happily provide the Court with all 4,933 documents prior to the November 7 hearing and, if the Court wishes, would provide the Court a non-adversarial "technology tutorial" about Pegasus.

While "full functionality" is not a subject of any of the Motion RFPs, the Court did make reference to the full functionality of Pegasus in its February Order. Accordingly, Defendants' table (Craig Decl. ¶ 28) also sets forth documents that, along with interrogatory responses and deposition

testimony, amply show the full functionality of the Accused Technologies.[15]

1. Defendants' "Communications" Are Not Necessary to Respond to the Motion RFPs Seeking "Documents Sufficient to Show…"

Plaintiffs assert that Defendants have not produced their "communications." That is untrue, and many documents produced by Defendants *are* communications; they are just not *emails*. (*See, e.g.*, Craig Decl. Exhs. 44, 62, showing technical specifications followed by comments from NSO employees.) More fundamentally, because nearly all the Motion RFPs are phrased as seeking documents and communications "sufficient to show," "sufficient to describe," or "sufficient to identify," it should not be at all surprising that Defendants, rather than sifting through countless emails and trying to make judgment calls whether or not they are collectively "sufficient to show" a particular topic, identified the *technical documents* that were in fact sufficient to show, describe, or identify, the matters about which Plaintiffs sought discovery.

After the parties' negotiations led Plaintiffs to revise their RFPs, it is telling that *only two of them*, RFP Nos. 5 and 28, require a search for communications. Those two are phrased as seeking "All Documents and Communications" about a particular subject, "as limited through the use of search terms and custodians." (Craig Decl. Exh. 3.) These two RFPs are addressed below. The remainder of the Motion RFPs do not reference "search terms and custodians."

The bulk of the Motion RFPs are the thirteen that seek documents "sufficient to show certain information, which Defendants have either satisfied without need for internal communications, or, in the case of RFP 10, have explained that no responsive documents exist (Gazneli Decl. ¶¶ 8-9). They are:

- RFP 1: "sufficient to show NSO's development, testing, deployment installation,

[15] "Functionality" means "the set of functions or capabilities associated with computer software or hardware or an electronic device." https://www.merriam-webster.com/dictionary/functionality. The full functionality of Pegasus/Phantom is data collection, monitoring and investigation, data transmission, data presentation/analysis, and certain operational security features. This functionality, and how Pegasus/Phantom performs those functions, is shown by the documents set forth in the "full functionality" row of Defendants' chart (Craig Decl. ¶ 28). Defendants do not agree that installation is a "function" of Pegasus, but for the avoidance of doubt, Defendants' document production and interrogatory responses are more than sufficient to describe the installation vectors Heaven, Eden and Erised. (Craig Decl. Exhs. 1, 24, 26-28, 32-34, 36, 38-58, 67-95.)

distribution, use, maintenance, troubleshooting, and/or operation of [the Accused Technologies];"

- RFP 3: "sufficient to show how NSO intended for or permitted third parties to use the [Accused Technologies], including but not limited to marketing materials, licensing agreements, user complaints, and training manuals or documents;"
- RFP 7: "sufficient to show how NSO developed and tested any exploit or technology used in the [Accused Technologies];"
- RFP 9: "sufficient to show the processes, methods and technology used by the [Accused Technologies] to monitor target devices and exfiltrate data, including but not limited to command and control software or payloads;"
- RFP 10: "sufficient to identify the mobile phone and device operating system vulnerabilities used to install the [Accused Technologies];"
- RFP 14: "sufficient to show the processes, methods, and technology used to install the [Accused Technologies] on the mobile phones and devices of target users, including but not limited to computer code, commands, data, or payloads transmitted or received during the installation of the [Accused Technologies];"
- RFP 15: "sufficient to show analysis, reverse engineering, disassembling, or emulating of any version of the WhatsApp application . . ."
- RFP 16: "sufficient to show the technologies used in the [Accused Technologies] to communicate with WhatsApp, including WhatsApp servers, endpoints, computers, and computer networks, other than the official WhatsApp application;"
- RFP 19: "sufficient to show the technology used to transmit any data or information from any target device containing or infected with the [Accused Technology];"
- RFP 20: "sufficient to describe the design and operation of Pegasus, including but not limited to the 'layers' described in Exhibit 10 of the Complaint: installation, data collection, data, transmission, presentation and analysis, and administration;"
- RFP 21: "sufficient to describe the design and operation of Pegasus' system architecture and technology, as described in Exhibit 10 of the Complaint;"
- RFP 24: "sufficient to describe the data and information NSO or NSO customers obtained from the target users or the target devices;"
- RFP 27: "sufficient to describe NSO's corporate structure, including all parents, subsidiaries and affiliates."

(Craig Decl. Exh. 3; *see also* Dkt. 235-4 Exh. P.)

With respect to these thirteen Motion RFPs, each of which seeks documents sufficient to show very technical matters, the documents Defendants produced as "sufficient to show" the information requested are centralized technical files, not random emails between employees. Indeed, the "substantial time, effort and cost" to collect these emails outweighs the "marginal relevance and limited potential benefit" of producing duplicative or cumulative emails at this stage

of the litigation, when Defendants have already produced technical documents that are more narrowly tailored to demonstrate the requested information. *In re Cathode Ray Tube (CRT) Antitrust Litig.*, No. 3:07-CV-05944SC, 2015 WL 13655394, at *9 (N.D. Cal. July 9, 2015). Plaintiffs include no coherent argument as to why they think it should be otherwise, but instead rally around a thoughtless "but what about the emails?" drumbeat that is better suited to Fox News *circa* 2016. The Court should reject it.

2. RFP Nos. 5 and 10, Identification of Vulnerabilities

Request No. 5 sought "all documents and communications concerning the identification of WhatsApp application or network vulnerabilities, including but not limited to any payments for bounties for WhatsApp vulnerabilities, contracts for services by vendors, or analyst work product and reports, as limited through the use of search terms and custodians." Request No. 10 sought documents sufficient to identify these vulnerabilities. After a diligent search, Defendants have not recovered no responsive documents.

Request No. 5 can be broken out into two parts, separated by an "including but not limited to" phrase. Defendants have no documents responsive to either portion. Defendants, like other companies in their industry, do not document the vulnerabilities they research and use. (Gazneli Decl. ¶¶ 8-9.) This policy is industry standard and exists for operational security reasons. (*Id.* ¶ 8.) Nevertheless, Defendants conducted an extensive keyword search of the documents of 25 custodians; those search terms hit on 6,437 documents. (Craig Decl. ¶¶ 25-26.) After a two-stage review of the "hits," Defendants located no responsive documents for RFP Nos. 5 and 10. (*Id.*) With respect to the second half of Request No. 5, Defendants did not make any payments for bounties for WhatsApp vulnerabilities, did not enter into any service contracts with vendors relating to WhatsApp vulnerabilities, and do not have any analyst work product and reports, and therefore have no responsive documents. (Gazneli Decl. ¶ 9.)

3. Request for Production No. 17, WhatsApp Accounts

Request No. 17 sought documents and communications "concerning WhatsApp Accounts used to develop, test, transmit, install, distribute or use [the Accused Technologies]." Defendants understood this request as seeking documents sufficient to identify specific WhatsApp accounts

used to develop, test, transmit, etc., the Accused Technologies. Those WhatsApp accounts are identified in hundreds of documents that Defendants produced to Plaintiffs, examples of which are attached. (Craig Decl. Exhs. 21-22.) Defendants produced all such information located after a reasonable and diligent search. Plaintiffs have now submitted a dispute to the Court seeking to share these documents about Defendants' WhatsApp accounts with certain of their "business" persons, notwithstanding Defendants' designation of such information as highly confidential—attorneys' eyes only. (Dkt. No. 408.) Based on that dispute, Plaintiffs appear to concede Defendants have produced their WhatsApp Account information to Plaintiffs.

4. RFP No. 26, Marketing Materials

Request No. 26 sought "All documents used to market, sell, or promote [Accused Technologies] that refer to WhatsApp in any way." It is unclear what relevance Defendants' marketing materials have to any issue in the litigation about the CFAA, CDAFA, WhatsApp's Terms of Service, or any affirmative defense, but Defendants nevertheless collected all responsive marketing materials and produced them to Plaintiffs. (Craig Decl. Exhs. 13-18.)

5. RFP No. 28, Defendants' Communications with Westbridge

RFP No. 28 sought all communications with Westbridge Technologies relating to WhatsApp and the surveillance of WhatsApp users, as limited through the use of search terms and custodians. During a conference on September 30, 2024, Defendants' counsel informed Plaintiffs' counsel that Defendants had collected and reviewed these documents from NSO custodians, but through an inadvertent oversight, they were not produced. (Craig Decl. ¶ 20.) Defendants subsequently produced all of NSO's communications with Westbridge relating to WhatsApp and the surveillance of WhatsApp users on October 8, 2024. (*Id.*) This production was comprised almost entirely of NSO emails. (Craig Decl. ¶ 19.)

6. RFP No. 30, the AWS server

As discussed at length above, RFP No. 30 sought a copy of the AWS server. Defendants produced it. Emails were not included because email was not stored on the AWS server.

In sum, Defendants have fully complied with ***all*** of the Motion RFPs. The fact that few internal communications were produced means only that Defendants focused on the actual

language of Plaintiffs' requests and located the documents "sufficient to show" the information requested. With respect to the two requests that sought internal communications (as limited by custodians and keyword searches), Defendants either produced those they were able to locate (RFP No. 28 re Westbridge communications), or were unable to locate any responsive documents after a good faith and diligent search (RFP No. 5 re identification of WhatsApp vulnerabilities, and the closely related RFP No. 10). (Craig Decl. ¶¶ 19-20 and 23-26.)

E. Defendants' Production of Financial Documents is More than Sufficient

Defendants are confused by Plaintiffs' discussion of financial documents in their sanctions motion because the Motion RFPs do not include any requests for financial information, and certainly do not include any request to which a price list would be responsive. Plaintiffs cite to Dkt. 176-2 (Motion at 13:21), which was Defendants' March 2023 motion for a protective order. The order denying Defendants' motion (Dkt. 233) did not *order* Defendants to produce *anything*, let alone financial information or a price list. Defendants cannot be sanctioned for failing to produce documents the production of which has not been ordered.

Defendants have produced copious financial information to Plaintiffs, including audited financial statements from 2018 through 2020 for NSO, Q Cyber (Israel), and a parent company named Triangle Holdings. (Craig Decl. Exhs. 11-12.) Defendants have also produced shareholder registries for both Defendants. (Craig Decl. Exhs. 19-20.) Further, Defendants have produced *complete* information about the amounts their customers paid for *all* of Defendants' products, including but not limited to Pegasus, for the ordered discovery period. (Craig Decl. Exh. 2045 and ¶ 16.) Every revenue stream received by Defendants during this period is reflected in the information produced to Plaintiffs, which, contrary to Plaintiffs' claim, was created by NSO employee Sarit Gil and not by Defendants' attorneys (Craig Decl. Exh. 9 at 158:19-159:3). In light of this production of information that shows the sums Defendants actually received for each contract, Plaintiffs have no need for a "price list" document that, like a car dealer's "MSRP," bears no relation to the prices customers actually paid. Moreover, the only issue that this information relates to is Plaintiffs' claim for disgorgement of Defendants' profits, which is not a jury issue. The Court can deal with any discovery disputes about Defendants' financial information after the

jury trial, if one takes place and if Plaintiffs show a right to disgorgement. The Court should neither impose sanctions nor order discovery of Defendants' price list, in light of Defendants having provided Plaintiffs with the actual amounts they have received for all sales of the Accused Technologies (and all other products besides).

F. Defendants' Refused to Answer Deposition Questions Only to Enforce the Court's Temporal Discovery Limitation and to Comply with Israeli Law.

Rule 30(c)(2) provides that a person may properly instruct a deponent not to answer when necessary to enforce a limitation ordered by the court. In the February Order, the Court ordered the time for which discovery could be had was limited to April 29, 2018, to May 20, 2020, though it advised that Plaintiffs could seek to expand that if it had cause to do so. Plaintiffs never made any such request. Accordingly, at deposition, Defendants' counsel occasionally instructed Defendants' witnesses to not answer questions that sought information about time periods other than those allowed by the Court in order to enforce the Court's limitation. This is not improper, and it is certainly not sanctionable.

Moreover, [redacted] (Gelfand Decl. ¶¶ 6, 9.) On a few occasions, Defendants' witnesses therefore asserted that they were unable to answer Plaintiffs' questions. Nevertheless, Defendants' witnesses each answered nearly all questions put to them, each over the course of a full day—or more. Plaintiffs cite to only a tiny number of instances [redacted] Plaintiffs do not and cannot explain how an answer to those questions would have been relevant to their claims in this case.

Plaintiffs point to one instance where [redacted] (Mot. at 14:20-21.) This mischaracterizes Mr. Gazneli's deposition. Immediately after the testimony cited, counsel for Defendants objected "to the form of that

question. If you want to ask him questions he can tell you whether he can testify about it or not." (Craig Decl. Exh. 2 at 142:13-16.) [redacted] Plaintiffs' complaint about the testimony of [redacted] (Mot. at 25:14-16) is similarly misleading. In the very excerpt cited by Plaintiffs, Mr. Eshkar testified about feedback he had received from customers about the loss of the Hummingbird vector. (Block Decl. Exh. O at 216:6-22.) [redacted] consistent with the Court's February Order.

Plaintiffs' cited authority provides an exception to Rule 30(c) if there is a risk of "serious harm" [redacted], and in any event those cases did not hold that sanctions were appropriate. Mot. at 15 (citing *Detoy v. City & Cnty. of San Francisco*, 196 F.R.D. 362 (N.D. Cal. 2000)). [redacted] [Dkt. 133-6 Exh. B at 2.] Additionally, Defendants and "any officer in [their] corporation[s]" face prosecution, a term of "three years' imprisonment or a fine" if they provide Defense-Know-How to a party without a defense export license. Def.'s Mot. for Protective Order at 4-5, Dkt. No. 186. These consequences no doubt constitute the "serious harm" that the exception contemplates, and excuse the few times where Defendants' witnesses could not respond to questions as phrased. Importantly, Plaintiffs do not cite cases considering Rule 30(c) violations where the requested testimony risked damaging [redacted] incurring criminal penalties, or [redacted] That is this case. And the potential consequences here preclude it from being controlled by the cases Plaintiffs cite, involving nominal objections to relevance or scope. Mot. at 15 (citing *Hernandez v. Lynch*, No. EDCV 16-620 JGB (KKX), 2019 WL 6998774 at *2 (C.D. Cal. June 18, 2019) (objections to "questions on the grounds that they were not relevant."); *Maui Jim, Inc. v. SmartBuy Guru Enterprises*, No. 16 C 9788, 2019 WL 356805, at *4 (N.D. Ill. Jan. 29, 2019) (requested testimony was not "relevant to [defendant's] trademark misuse defense"); *Vasquez v. Leprino Foods Co.*, No. 117CV00796AWIBAM, 2019 WL 1934015, at *5 (E.D. Cal. May 1,

2019) (objecting to questions "outside the scope of [deponent's] second, limited deposition.")). In those cases, the risk of providing the testimony was significantly lower than the criminal penalties [redacted] and yet the courts did not find sanctions appropriate. In fact, *Hernandez* reversed the award of sanctions as an abuse of discretion where counsel's objections were based on a "good faith misinterpretation" of the court's prior orders limiting the scope discovery. 2019 WL 6998774 at *4. Those cases provide no basis to impose sanctions for defense counsel's objections here, where an illegal disclosure of Defense-Know-How posed far graver penalties. Simply put, defense counsel's objections did not violate Rule 30(c) because the elicited testimony posed a risk of serious harm, and in any event Plaintiffs have not demonstrated sanctions are appropriate for any violation.

G. [redacted] Are Essentially Irrelevant to Plaintiffs' Motion.

[redacted] Defendants have fully complied with the Court's discovery orders, [redacted] (*see* Gelfand Decl. ¶¶ 6-9). Plaintiffs' lengthy discussion that [redacted] is incorrect. Defendants [redacted] (*see* Gelfand Decl. ¶ 9), [redacted], Defendants [redacted] and satisfy their discovery obligations, including the Motion RFPs.

Defendants' conduct does not "mirror" that of the defendant in *Richmark Corp. v. Timber Falling Consultants,* 959 F.2d 1468 (9th Cir. 1992). Unlike Defendants who have been forcibly hailed into this Court, the Beijing defendant in *Richmark* invoked federal court jurisdiction by appealing a default judgment, and then abused the discovery rules of those courts to hide its assets and frustrate the underlying judgment. *See id*. at 1478. Specifically, Beijing failed to respond to discovery requests and "refused to disclose . . . information concerning its assets" despite the court's having entered three discovery and contempt orders against it. *Id.* at 1472 n.4. Defendants

have not refused to provide any information ordered by the Court; at most Defendants produced certain information to Plaintiffs' counsel in a different location from where Plaintiffs' counsel wanted it (but had not requested it). Producing the requested information to Plaintiffs' counsel in a manner that did not violate DECL further distinguishes Defendants from Beijing, as the latter did not take "all the reasonable steps" to comply with the orders compelling disclosure. *Id*. at 1479. Finally, the threat of criminal prosecution against Beijing's was "self-imposed" as it could have posted a bond or paid the judgment without violating the blocking statute. *Id*. at 1477. Although Plaintiffs incorrectly assert (Mot. at 15) that NSO hampered its own ability to participate in discovery, Defendants have exhausted all options to comply that would not violate DECL. Defendants' good faith effort to comply with the Court's orders, and providing the information to Plaintiffs' counsel in Israel, renders Plaintiffs' 'hiding behind Israeli law' accusation and comparisons to Beijing untenable.

H. No Sanctions of Any Kind are Warranted.

Plaintiffs' request for terminating sanctions is ludicrous. Plaintiffs are trying to manipulate the Court into "splitting the baby" and awarding as an issue sanction that which Plaintiffs desperately need to avoid their case being dismissed for lack of personal jurisdiction. The last three pages of Plaintiffs' motion, setting forth the personal jurisdiction-centric issue sanctions they seek, betray Plaintiffs' actual intent.

No sanctions of any kind are warranted here because Defendants have not violated any of the Court's discovery orders. Specifically, the issue sanctions sought by Plaintiffs, the first three of which seek findings that would short-circuit the Court's personal jurisdiction analysis, are counterfactual and unwarranted.

Targeting of Plaintiffs' California-based servers. First, Plaintiffs argue that whether Defendants knowingly targeted California servers is irrelevant based on a willful misreading of the Court's Order on Defendants' Motion to Dismiss (Dkt. No. 111). In that Order, the Court credited Plaintiffs' allegations to mean that "defendants' program sought out specific servers—including servers in California—in order to transmit malicious code." (*Id.* at 22.) Those allegations have now been disproven, including by the version of the AWS server produced by

Plaintiffs in discovery. (Dkt. No. 396-2 at 9-11; Gazneli Decl. ¶ 11; McGraw Decl. ¶¶ 3-4). Plaintiffs' argument that additional discovery (presumably the AWS server produced in Israel) would prove the opposite of that which its own copy of the AWS server plainly shows is illogical.

Location of third-party servers. Plaintiffs admit the Court denied their motion to compel with respect to server architecture, which includes third-party servers. (Motion at 24:13-16.) No sanction, let alone an issue sanction, is warranted. *Unigard*, 982 F.2d at 367-68. The Court should certainly not impose the issue sanction Plaintiff requests—that Defendants knowingly used a California-based server—when the facts demonstrate that Defendants could not have known where the third-party server was located. (Dkt. No. 396-2 at 11-14.)

Relationship with Westbridge. Defendants have produced all documents responsive to Request No. 28 (Craig Decl. ¶¶ 19-20). Because Defendants are in compliance with the Court's Order, no sanction is warranted. Moreover, the fact that Defendants "routinely collud[ed]" with Westbridge, their sales agent in the United States, is not grounds for alter ego where Westbridge had its own articles of incorporation, bylaws, books and records, bank account, and employees. (Dkt. No. 396-2 at 14-16).

Use of Pegasus by NSO's customers. Plaintiffs seek issue sanctions about the roles that Defendants' customers take in using Pegsaus, without identifying any order, or even any discovery request, with which Defendants failed to comply. Yet Plaintiffs ask the Court to preclude NSO from arguing that its customers operated Pegasus. Plaintiffs' own documents show their knowledge that Defendants' customers, each a "nation state," operated Pegasus. (Dkt. No. 396-5 at Exhs. R-V.) Plaintiffs' requests for issue sanctions should be denied.

IV. CONCLUSION

For the foregoing reasons, the Court should deny Plaintiffs' motion for sanctions.

Dated: October 16, 2024

KING & SPALDING LLP

By: */s/Joseph N. Akrotirianakis*
JOSEPH N. AKROTIRIANAKIS
AARON S. CRAIG

Attorneys for Defendants NSO GROUP TECHS. LTD. and Q CYBER TECHS. LTD.