KING & SPALDING

King & Spalding LLP
633 West Fifth Street
Suite 1600
Los Angeles, CA 90071
Tel: +1 213 443 4355
Fax: +1 213 443 4310
www.kslaw.com

CONFIDENTIAL AND ATTORNEY-CLIENT PRIVILEGED MEMORANDUM

TO: NSO Group Technology Limited

FROM: King & Spalding LLP

DATE: April 17, 2020

RE: WhatsApp v. NSO Group – Blocking Orders

This memorandum analyzes the effect a "blocking order" from Israel—an order prohibiting NSO from producing certain information to Plaintiffs—would have on discovery. Our conclusion is that NSO cannot be confident that a blocking order will excuse NSO from its obligation under U.S. law to produce relevant information. If Israel issues a blocking order, it will have to carefully tailor the order under Ninth Circuit law to maximize the chances of success.

Conflicts Between U.S. and Foreign Discovery Laws

The permissible scope of discovery in federal courts in the United States is broad. A party may "obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1). Many countries have much more restrictive discovery systems than the United States. Some of those countries have laws that prohibit the disclosure of information that would otherwise have to be produced in the United States. Countries may also issue orders prohibiting disclosure.

As a general matter, foreign laws prohibiting disclosure do "not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [law]." *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct.*, 482 U.S. 522, 543 n.29 (1987). Instead, whether a foreign person must produce the information depends on a multi-factor balancing test, which considers:

> [i] the importance to the investigation or litigation of the documents or other information requested; [ii] the degree of specificity of the request; [iii] whether the information originated in the United States; [iv] the availability of alternative means of securing the information; [v] and the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.

Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992). The Ninth Circuit also considers "the extent and the nature of the hardship that inconsistent enforcement would impose upon the person" and "the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state." *Id.* (cleaned up).[1]

Richmark is the leading Ninth Circuit case addressing the effect of a foreign blocking law on U.S. discovery. The plaintiff in *Richmark* sought discovery of a Chinese corporation's assets to satisfy a judgment the corporation had refused to pay. 959 F.2d at 1471. The corporation argued that Chinese "secrecy laws prevent[ed] it from complying with the discovery order and that it would be subject to prosecution in [China] were it to comply." *Id.* China issued an order to the corporation forbidding it from producing most of the requested information and informing the corporation that it "shall bear any or all legal consequences should you not comply with th[e] order." *Id.* at 1476.

The Ninth Circuit accepted that the corporation could face criminal prosecution in China if it disclosed the requested information. *Id.* at 1474, 1477. But it still ordered the corporation to provide the discovery. Weighing the applicable factors, the court found that (1) the requested information was relevant, favoring disclosure; (2) the plaintiff's requests were specific, favoring disclosure; (3) the information and corporation were located in China, favoring nondisclosure; (4) there was no substantially equivalent alternative source for the information, favoring disclosure; (5) the United States' interest in disclosure outweighed China's expressed interest in protecting the corporation's information because China had not expressed the interest prior to the litigation and had not explained how the corporation or China would be negatively affected by disclosure; (6) although the corporation could face criminal prosecution, it could avoid discovery by paying the plaintiff's judgment or posting a bond; and (7) although the corporation was not likely to comply with a discovery order, sanctions for noncompliance could still be effective by making it harder for the corporation to do business in the United States in the future. *Id.* at 1475-78. Balancing these factors, the court ordered disclosure.

Richmark suggests that courts within the Ninth Circuit—including the Northern District of California, where Facebook filed its lawsuit against NSO—will be reluctant to excuse discovery based on a foreign prohibition/blocking order, even when the foreign country has expressly ordered the party not to comply and has threatened criminal prosecution. For example,

[1] As an alternative to excusing production outright, a court may require the party seeking discovery to do so through the Hague Convention on the Taking of Evidence Abroad. *Aerospatiale*, 482 U.S. at 541. The Hague Convention "prescribes certain procedures by which a judicial authority in one contracting state may request evidence located in another contracting state." *Id.* at 524. The Hague Convention procedures can be "time consuming and expensive," and result in less discovery than the U.S. rules. *Id.* at 542. The factors for deciding whether to apply the Hague Convention are the same as those for deciding whether to excuse production outright. *Sun Grp. U.S.A. Harmony City, Inc. v. CRRC Corp. Ltd.*, 2019 WL 6134958, at *2–3 (N.D. Cal. Nov. 19, 2019). Accordingly, we would expect the court to analyze the issue in the same way. *See id.* at *3–5.

the court in *In re Air Crash* ordered the defendant to produce information despite a letter from the Attorney General of Singapore prohibiting the defendant from doing so under Singapore's privacy laws. 211 F.R.D. 374, 377-79 (C.D. Cal. June 19, 2002). And in *Fenerjian v. Nong Shim Co.*, the court ordered a company to produce information about its employees despite a Korean statute criminalizing disclosure. 2016 WL 245263, at *2-6 (N.D. Cal. Jan. 21, 2016).[2]

Application to NSO

In this case, we think it is likely that Facebook may request documents or other discovery that Israel or NSO's other customers prohibit NSO from providing. For example, Facebook may request NSO's contracts with its customers or all documents relating to each Pegasus license to any of its customers. Facebook will doubtlessly seek discovery related to how the Pegasus technology operates.[3] If NSO refuses to provide the discovery, the Court will apply the factors from *Richmark*. It will, therefore, be important that any blocking order from Israel adhere closely to *Richmark*'s requirements.

1. Importance of Documents

This factor favors discovery when "the evidence is directly relevant." *Id.* at 1475. On the other hand, "[w]here the outcome of litigation does not stand or fall on the present discovery order, or where the evidence sought is cumulative of existing evidence, courts have generally been unwilling to override foreign secrecy laws." *Id.* Whether the evidence sought by Facebook is relevant will, of course, depend on Facebook's specific requests, but we would expect that much of the discovery to which Israel would object would be relevant to Facebook's claims.

2. Specificity of Request

Whether the discovery request is specific bears on "how burdensome it will be to respond to that request." *Id.* If the request is a "[g]eneralized search[] for information," courts are more likely to deny the request. *Id.* Again, it is not possible to say whether Facebook's requests will be sufficiently specific until Facebook makes the requests.

3. Location of Information and Parties

When "all the information to be disclosed (and the people who will be deposed or who will produce the documents) are located in a foreign country," that "weighs against disclosure." *Id.* This factor will favor NSO. *See id.* (finding "[t]his factor weighs against requiring disclosure" when party "ha[d] no United States office" and "[a]ll of its employees, and all of the documents . . . requested" were located in China).

[2] Other Circuits take a similar approach. *See, e.g.*, *In re Sealed Case*, 932 F.3d 915, 933 (D.C. Cir. 2019) (ordering discovery from Chinese bank despite threat of criminal penalties by Chinese government); *Linde v. Arab Bank, PLC*, 706 F.3d 92, 114 (2d Cir. 2013) (ordering discovery from Jordanian bank despite letters from Jordan, Lebanon, and Palestinian Monetary Authority threatening legal sanctions).

[3] A preliminary list of anticipated discovery topics is included in an appendix to this memorandum.

4. Alternative Means

For an alternative means of discovery to weigh against disclosure, it "must be 'substantially equivalent' to the requested discovery." *Id.* If an alternative means would cost more "time and money" or is unlikely to be effective, it is not an adequate alternative. *United States v. Vetco Inc.*, 691 F.2d 1281, 1290 (9th Cir. 1981).

Here, we expect that the only alternative source for the information Facebook will seek would be NSO's customers. If those customers are objecting to discovery, they will not be an adequate alternative means of discovery. This factor is likely to favor disclosure. *See id.* at 1476 ("The absence of other sources for the information . . . is a factor which weights strongly in favor of compelling disclosure.").

5. Interests of the United States and of the State Where the Information is Located

"This is the most important factor." *Id.* To analyze the foreign country's interest in preventing disclosure, courts "will consider expressions of interest by the foreign state, the significance of disclosure in the regulation of the activity in question, and indications of the foreign state's concern for confidentiality prior to the controversy." *Id.* (cleaned up).

Even if the foreign country has an interest in prohibiting disclosure, that interest "must be weighed against the United States' interests in vindicating the rights of American plaintiffs and in enforcing the judgments of its courts." *Id.* at 1477. Those interests are "substantial" in every case. *Id.*

To overcome the United States' substantial interests, if Israel objects to discovery, they would need to create a writing—either to the court or to NSO—that expresses an interest in this specific case and explains with particularity why discovery would impair its interests. The writing will have to identify the specific discovery to which it objects and provide a clear explanation for why that discovery would endanger an important governmental interest. It will not be enough to simply object to discovery in general or to make a broad assertion of an interest in confidentiality. *See In re Air*, 211 F.R.D. at 379 (discounting Singapore's interest when government's letter did "not mention any of the specific document requests at issue").

There is no question that Israel's national security would be a weighty interest, and a court would likely understand that. *See In re CRT Antitrust Litig.*, 2014 WL 1247770, at *3 (N.D. Cal. Mar. 26, 2014) (finding significant foreign interest in antitrust enforcement); *cf. Richmark*, 959 F.2d at 1477. But the court may discount Israel's statement if it has "not express[ed] interest in the confidentiality of th[e] information prior to the litigation." *In re CRT*, 2014 WL 1247770, at *3. Israel will, therefore, need to be able to identify other times when it has asserted a confidentiality interest in the kind of information requested. In this case, that may be partially accomplished through an explanation of Israel's export control regime, including instances in which it has prohibited other companies from disclosing the details of sensitive regulated products.

Finally, a court may also discount the foreign government's interest in confidentiality if "the court has entered a protective order preventing disclosure of the secret information." *Finjan, Inc. v. Zscaler, Inc.*, 2019 WL 618554, at *3 (N.D. Cal. Feb. 14, 2019). If the court issues a protective order prohibiting the parties from disclosing NSO's information to anyone outside of the lawsuit, the court may consider that order sufficient to protect Israel's interests. To be most persuasive, Israel's blocking order should explain why disclosing the information only to Facebook and the court would still damage its interests.

6. Hardship

"The party relying on foreign law has the burden of showing that such law bars production." *Vetco*, 691 F.2d at 1289. If the foreign law does not actually bar production, then there is no hardship on the producing party. *Id.* at 1289–90. Therefore, any blocking order from Israel must identify the law barring disclosure and explain why the specific discovery falls within that law.

If the law does forbid production, then the court will consider the severity of the punishment for violating the law. The possibility of "criminal prosecution," for example, is "a weighty excuse for nonproduction." *Richmark*, 959 F.2d at 1477. To be effective, a blocking order from Israel should spell out the punishment NSO would face if it provided the information to Facebook.

Even the possibility of criminal sanctions, however, does not guarantee that a court will excuse discovery. *See id.* (ordering discovery despite possibility of criminal prosecution in China); *Vetco*, 691 F.2d at 1287 (finding possibility of criminal prosecution did not automatically excuse discovery where party had not "made good faith efforts to comply" with discovery). In particular, courts will not credit a foreign prohibition on disclosure if it has not been enforced in the past. *See Fenerjian*, 2016 WL 245263, at *6 (discounting foreign criminal prohibition because defendant could not cite an instance in which the prohibition had been enforced). The strongest argument for hardship would be established if Israel provides examples of other parties that have been punished for disclosing similar information.

7. Likelihood of Compliance

"If a discovery order is likely to be unenforceable, and therefore have no practical effect, that factor counsels against requiring compliance with the order." *Richmark*. 959 F.2d at 1478. If NSO refused to comply with a discovery order even in the face of sanctions, that could be "a factor counseling against compelling discovery." *Id.* However, the *Richmark* court ruled that an order may "be effective" even if it is unlikely to result in compliance. If the party does business in the United States or might "wish to do business in the [United States] in the future," that possibility can support a discovery order. *Id.*

8. Summary

Although any multi-factor test involves uncertainty as to how it would be applied by a particular judge, our research indicates that U.S. courts overwhelmingly require disclosure despite a foreign prohibition.[4] Thus, while the effectiveness of a blocking order from Israel will depend on the contents of the order and the discovery requests at issue, there is no guarantee that the blocking order would prevent NSO from being ordered to produce the same discovery the blocking order prohibits it from producing. To maximize the chance of success, the blocking order should be a targeted objection to specific discovery requests, explain clearly how that discovery will impair Israel's interests, explain the sanctions for production, and make a persuasive case that the threat of punishment is real.

Even with a strong blocking order, however, a court may still order discovery, which could leave NSO no way to avoid disclosure without being held in contempt of court. As we have previously discussed with you, a proper invocation of the state secrets privilege would present a much stronger basis to deny discovery to Facebook. The state secrets privilege would require the Government of Israel (or another government) to assert that disclosure of the information would cause harm to its national security. But if Israel or another government is concerned about avoiding production of information about NSO's customers and technology, asserting the state secrets privilege is the most reliable —and likely the only—way to do so.

[4] There are cases within the Ninth Circuit in which a court has excused production, but they involved factors that strongly opposed production on top of the foreign country's significant interests. *See Campbell v. Facebook Inc.*, 2015 WL 4463809, at *3–5 (N.D. Cal. July 21, 2015) (excusing production because discovery was irrelevant and available through other sources); *In re CRT Antitrust Litig.*, 2014 WL 6602711, at *3 (N.D. Cal. Nov. 20, 2014) (excusing production based on comity, the location of discovery abroad, and the possibility of obtaining the same discovery from a different source); *In re TFT-LCD Antitrust Litig.*, 2011 WL 13147214, at *4–6 (N.D. Cal. Apr. 26, 2011) (excusing production because discovery was irrelevant, cumulative, based overseas, and available elsewhere, and foreign governments has expressed strong interest in nondisclosure); *In re Rubber Chemicals Antitrust Litig.*, 486 F. Supp. 2d 1078, 1082–84 (N.D. Cal. May 9, 2007) (same). Many of those factors—such as the relevance, specificity, and availability of the discovery—cannot be analyzed until Facebook actually serves its discovery requests.

Appendix of Possible Discovery Requests

Documents and Witness Testimony

1. **Information relating to NSO's Clients**
    a. *Full customer list*
        i. U.S. customers (goes to personal jurisdiction)
    b. *All customer contracts*
        i. Terms of "appropriate use" in contracts (Hulio Declaration ¶ 12)
        ii. Pricing terms and records of contracts / licensing
    c. *All end use certificates* (Hulio Decl. ¶ 8)
    d. *Due Diligence Materials* (Hulio Decl. ¶ 11)
        i. Questionnaires to customers
        ii. Records / testimony on any reports of "abuses" or investigations into abuses (Hulio Decl. ¶ 17)
    e. *MoD Registrations* (Hulio Decl. ¶ 5)
    f. *Correspondence with the Israeli Ministry of Defense* regarding Pegasus and/or export control licenses
    g. *Marketing materials to customers*
        i. U.S. customer requests (may argue is relevant to personal jurisdiction argument)
    h. *Westbridge*—relationship with NSO and operations in the U.S.
        i. Relationship between Westbridge and NSO
        ii. Correspondence with existing or potential U.S. clients
    i. *Financing*—did NSO have sources of U.S. financing during the period of the allegations? (may argue is relevant to personal jurisdiction argument)
2. **Information Relating to NSO Operations Generally**
    a. Employee lists—where are employees located geographically (will argue it goes to personal jurisdiction)
3. **Information Relating to NSO Pegasus Technology**
    a. *Whether NSO employees ever created WhatsApp accounts*
        i. Details of how those accounts were created

1. Identities Used
2. Agreement to ToS

b. **Details on the NSO Hardware and Software Deployed** to the Customer (Compl. ¶¶ 58, 61; Hulio Decl. ¶ 14)

c. NSO "Hacking" Techniques and Support

i. Any information or *use of NSO "zero days" or OS system exploits* that would be applicable to a wide range of targets (Compl. ¶ 25)

ii. NSO *use of spearphishing or other malware delivery methods* (Comp. ¶ 25)

iii. *Platforms against which Pegasus* could be used (iMessage, Skype, Telegram, WeChat, Facebook) (Comp. ¶ 27)

iv. *What information can Pegasus extract from a target* (Comp. ¶ 27)

v. *How does Pegasus otherwise work*?

vi. Does NSO provide training for its users

1. Documents of the same

vii. Whether and how NSO updated Pegasus on users' phones

viii. Does NSO have remote support capabilities for its customers

1. Any specific details of technical support?

d. **How does NSO "set up" technology**?

e. **Aside from Pegasus software, what other technology does NSO create / maintain for customers after the setup**?

i. How do NSO's network of "remote servers" work? (Compl. ¶ 32)

1. Do they have a role in deploying Pegasus
2. How do they conceal the identities of NSO Group or its customers so Pegasus is not discovered

f. What ongoing access does NSO have to its technology once its installed at a customer location

g. **How does Pegasus change after its installed** (Compl. ¶ 27 "modular software")

h. Information on limitations on use of Pegasus

i. Audit trail

ii. Any Other Technical Safeguards

iii. *Limitation on US phones* (Hulio Decl. ¶ 13)

1. Can NSO's customers modify/evade this limitation
2. Known instances of failure (e.g. was a US person or phone ever surveilled)
3. How does it work for a U.S. person/phone overseas

iv. Extraterritorial Limitations

1. Can a government customer use Pegasus extraterritorially, outside of their own nation? (Goes to derivative sovereign immunity; Bezos scenario)

4. Information Relating to NSO / MoD Interactions

a. Whether MoD has ever conducted an investigation into NSO technology or customer use of the technology

b. Whether MoD has ever revoked an export control license

5. NSO Specific Operations

a. Any information about the 1,400 targets identified by Facebook

b. Information about the Jeff Bezos hack or Khashoggi killing

6. NSO's Relationship to Facebook

a. Documents and emails regarding the Facebook's attempt to purchase NSO services in 2017