No. 21-1338

IN THE

Supreme Court of the United States

NSO GROUP TECHNOLOGIES LIMITED AND Q CYBER TECHNOLOGIES LIMITED,

Petitioners,

v.

WHATSAPP INC. AND META PLATFORMS, INC.

Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

BRIEF IN OPPOSITION TO CERTIORARI

Anton Metlitsky
O'MELVENY & MYERS LLP
Times Square Tower
7 Times Square
New York, NY 10036
(212) 326-2000

Michael R. Dreeben
Counsel of Record
Ephraim McDowell
O'MELVENY & MYERS LLP
1625 Eye St., NW
Washington, DC 20006
(202) 383-5300
mdreeben@omm.com

QUESTION PRESENTED

The Foreign Sovereign Immunities Act (FSIA) establishes a comprehensive scheme governing foreign sovereign immunity for entities and grants no immunity to private entities like respondents under any circumstances. The question presented is:

Whether private entities like respondents—which are categorically ineligible for foreign sovereign immunity under the FSIA—may nonetheless obtain foreign sovereign immunity under the common law.

CORPORATE DISCLOSURE STATEMENT

Respondent Meta Platforms, Inc. (previously known as Facebook, Inc.) is a publicly traded company and has no parent corporation. No publicly held company owns 10% or more of its stock. Respondent WhatsApp LLC (previously known as WhatsApp Inc.) is a wholly owned subsidiary of Meta Platforms, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

STATUTES

REGULATIONS

TABLE OF AUTHORITIES (continued)

Page(s)

OTHER AUTHORITIES

INTRODUCTION

The Ninth Circuit correctly held that foreign sovereign immunity does not protect private foreign companies against liability in this Nation's courts. The court of appeals explained that because Congress comprehensively addressed foreign sovereign immunity claims by entities in the Foreign Sovereign Immunities Act (FSIA), and allowed only foreign-state-owned entities to assert such claims, private entities cannot obtain foreign sovereign immunity under the FSIA, the common law, or any other source.

NSO seeks certiorari, arguing that the Ninth Circuit's holding conflicts with the decisions of two other courts of appeals and with this Court's decision in *Samantar v. Yousuf*, 560 U.S. 305 (2010). NSO is incorrect. Neither appellate decision embraced a claim of common-law foreign sovereign immunity for private entities or suggested that such immunity could be available. And *Samantar*—like the judicial decisions before it, and consistent Executive Branch practice—recognized common-law foreign sovereign immunity claims only for individuals. *Samantar*'s logic precludes a similar recognition for private entities.

NSO asserts that the petition presents "an important question with significant foreign-policy implications." Pet. 14. But that speculation enjoys no support from Executive Branch practice. And a foreign company's foreign-policy conjectures do not take precedence over our political branches' consistent judgments. Nor is the question presented recurring or significant, as demonstrated by the paucity of precedent and absence of a single instance in which the State

Department has suggested common-law immunity for a foreign private entity.

Not only is the question presented unworthy of review, but this interlocutory petition presents a singularly inapt vehicle. The United States has determined that NSO's spyware activities—the very type of activities for which NSO seeks immunity—are contrary to U.S. national-security and foreign-policy interests, and has therefore added NSO to its Entity List restricting the export, reexport, and transfer of covered entities' items. Even if private entities were eligible for common-law foreign sovereign immunity (they are not), a company on the Entity List would have no plausible claim to such immunity. And this case's interlocutory posture further undermines the petition's suitability for review. The purported factual basis for NSO's immunity claim has never been tested in discovery because of NSO's threshold immunity assertion, which two courts below rejected. No foreign government has ever stepped forward to support NSO's immunity claim. And an antecedent question of appellate jurisdiction—whether the collateral-order doctrine applies to denials of common-law foreign sovereign immunity—would complicate this Court's review at this juncture.

Finally, there is no basis for prolonging this case by calling for the Solicitor General's views. Even though NSO has had ample time and opportunity, nothing in the record indicates that it invoked the usual channels for seeking the government's support for a suggestion of immunity—a request to the State Department. Nor has the United States *ever* suggested immunity for a foreign private company like

NSO, let alone one it has added to the Entity List for engaging in activities contrary to U.S. national-security or foreign-policy interests. Nothing justifies NSO's effort to draw the government into a case that it has shown no interest in supporting. The petition should be denied.

STATEMENT

A. Factual Background

1. a. WhatsApp LLC provides an end-to-end encrypted communication service available on mobile devices and computers. Court of Appeals Excerpts of Record, Dkt. 25-1, No. 20-16408 (9th Cir.) ("C.A. E.R.") 65 ¶ 17. Approximately 1.5 billion people across 180 countries have installed the WhatsApp app and use the app to securely make calls, send text messages and videos, and transfer files. *Id.* at 65 ¶¶ 17-18.

b. NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. (collectively, "NSO") are technology companies incorporated in Israel. *Id.* at 63-64 ¶¶ 5-6. NSO develops, tests, uses, distributes, and causes to be used a suite of surveillance technology, known as "spyware." *Id.* at 66 ¶ 24. NSO's spyware can be surreptitiously installed on a victim's phone, without the victim taking any action. *Id.* at 66-67 ¶ 26. Once installed on a phone, NSO's spyware can capture an array of private information, including the phone's real-time location, camera, microphone, memory, and hard drive. *Id.* at 67 ¶ 27; *id.* at 107; *id.* at 116. It can also intercept communications sent to and from a device (after decryption), including communications sent

over WhatsApp, iMessage, Skype, Facebook Messenger, and other services. *Id.* at 67 ¶ 27; *id.* at 109; *id.* at 116.

NSO develops, markets, and licenses its spyware to customers for a profit—sometimes through arrangements with private resellers. *Id.* at 67 ¶ 29; *see id.* at 143-49 (contract between private reseller of NSO spyware and the Republic of Ghana). When NSO licenses its spyware, NSO often installs the product, trains the customer on its operation, and tests its functionality. *Id.* at 137-39. NSO then provides continuing services to the customer, such as transmitting the data collected—*e.g.*, the target's private communications and real-time location, *id.* at 110; *id.* at 124—as well as providing technical support, *id.* at 67 ¶ 29. NSO's customers include various foreign governments. *Id.* at 70 ¶ 43; *id.* at 143-49.

Public reports cited in WhatsApp's complaint document that NSO spyware has been used to commit serious human-rights abuses. *See id.* at 70 ¶ 43 n.2. For instance, NSO's spyware was reportedly used to track contacts of Saudi journalist and Washington Post columnist Jamal Khashoggi before his murder.[1] The spyware has also been reportedly used to track other journalists, anti-corruption activists, human-rights lawyers, and senior government officials.[2]

---

[1] DJ Pangburn, *Israeli Cyberweapon Targeted the Widow of a Slain Mexican Journalist*, Fast Company (Mar. 20, 2019), https://www.fastcompany.com/90322618/nso-group-pegasu cyberweapon-targeted-the-widow-of-a-slain-mexican-journalist.

[2] David D. Kirkpatrick & Azam Ahmed, *Hacking a Prince, an Emir and a Journalist to Impress a Client*, N.Y. Times (Aug.

2. To facilitate its distribution and administration of spyware, NSO leased and caused to be leased a network of computer servers. C.A. E.R. 68-69 ¶ 34. Then, between January 2018 and May 2019, NSO created and caused to be created numerous WhatsApp accounts and repeatedly agreed to WhatsApp's terms. *Id.* at 68 ¶ 30. NSO violated those terms by, among other things, reverse-engineering the WhatsApp app; identifying and testing for vulnerabilities; developing its own proprietary software that could emulate ordinary WhatsApp network traffic and thus circumvent technical restrictions built into WhatsApp's servers; and testing that software. *Id.* at 69 ¶¶ 35, 37. The software facilitated the transmission of what appeared to be legitimate calls to WhatsApp users. *Id.* at 69 ¶ 37. In fact, those calls concealed malicious code that could be injected into the memory of a WhatsApp user's device, even if the user did not answer the call. *Id.* The code connected the devices to NSO's servers, *id.* at 68 ¶ 32, allowing the capture and tracking of the user's private data and communications, *id.* at 70 ¶ 41. NSO's servers operated as the nerve center through which NSO collected data from its targets and controlled the use of its spyware. *Id.* at 67 ¶ 28.

Between April 29, 2019 and May 10, 2019, NSO transmitted malicious code over WhatsApp servers to infect the devices of approximately 1,400 WhatsApp users. *Id.* at 70 ¶ 42. The victims of NSO's attack

---

31, 2018), https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html.

included attorneys, journalists, human-rights activists, political dissidents, diplomats, and other foreign government officials. *Id.*[3]

B. Procedural Background

1. On October 29, 2019, Meta Platforms, Inc. ("Meta") and WhatsApp LLC (together, "WhatsApp") sued NSO in the U.S. District Court for the Northern District of California. C.A. E.R. 62. WhatsApp asserted claims under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, as well as claims for breach of contract and trespass to chattels. *See* C.A. E.R. 63 ¶ 2. WhatsApp's claims arise from NSO's intentional, deceptive, and unauthorized accessing of WhatsApp servers, *id.* at 71-72 ¶¶ 50, 54, 59, to inject malicious code onto WhatsApp users' devices, *id.* at 73 ¶ 63, which also breached WhatsApp's terms, *id.* at 74 ¶ 71.

---

[3] NSO asserts that WhatsApp's notification of its users of NSO's attack "'killed' a significant investigation by European governments into an Islamic State terrorist." Pet. 8. This portrayal has neither support in the record nor relevance to NSO's petition. To protect user privacy, WhatsApp has a policy of informing users about app vulnerabilities. At the same time, WhatsApp cooperates with valid law-enforcement requests for data. In fact, as described in Meta's regular global transparency report, Meta responds to thousands of law-enforcement requests, including requests for data from WhatsApp. *See* Meta, Government Requests for User Data, https://transparency.fb.com/data/government-data-requests/. NSO's suggestion that WhatsApp's practices "frustrate[]" investigations (Pet. 8) is thus baseless.

NSO moved to dismiss for lack of subject-matter jurisdiction, arguing that "the doctrine of derivative sovereign immunity" barred WhatsApp's suit. Dist. Ct. Dkt. 45, at 9.[4] NSO conceded that it could "not claim immunity for itself under the [FSIA]" but maintained that it was still "entitled to *derivative* sovereign immunity" as an agent of unidentified foreign governments. Dist. Ct. Dkt. 62, at 9.

2. The district court denied NSO's immunity claim. Pet. App. 32-41. The court began by noting the parties' "agree[ment]" that NSO fails to meet the FSIA's definition of a "foreign state[]" and thus "cannot directly avail [itself] of th[at] [statute]." *Id.* at 32. The court then held that NSO cannot avail itself of common-law foreign sovereign immunity or derivative sovereign immunity either. *Id.* at 33-41.

NSO filed an interlocutory appeal in the Ninth Circuit, basing its immunity argument exclusively on common-law foreign sovereign immunity and abandoning its prior claim to derivative sovereign immunity. *See* Br. for Appellants, C.A. Dkt. 24., at 30-50. WhatsApp moved to dismiss the appeal for lack of interlocutory appellate jurisdiction, *see* C.A. Dkt. 13-1, and the motion was referred to the merits panel, *see* C.A. Dkt. 18.

3. While NSO's appeal was pending, the Department of Commerce published a final rule adding NSO to the federal government's Entity List. *See* Addition of Certain Entities to the Entity List, 86 Fed. Reg.

---

[4] Citations to "Dist. Ct. Dkt." refer to the district court's docket in this case: No. 4:19-cv-07123 (N.D. Cal.).

60759 (Nov. 4, 2021).[5] The Entity List identifies entities reasonably believed to be involved in activities contrary to the United States' national-security or foreign-policy interests and subjects those entities to strict export-licensing requirements. *Id.* The End-User Review Committee (ERC), composed of representatives of the Departments of Commerce, State, Defense, Energy, and, where appropriate, Treasury, makes all decisions about additions to the Entity List. *Id.* And the ERC added NSO to the Entity List because "investigative information has shown" that NSO "developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers." *Id.*

4. On November 8, 2021, a panel of the Ninth Circuit unanimously affirmed the district court's denial of foreign sovereign immunity to NSO. Pet. App. 2-3.

a. At the outset, the court held that it had jurisdiction to hear NSO's interlocutory appeal under the collateral-order doctrine. *Id.* at 6. The court "conclude[d] that the FSIA governs NSO's claim of immunity" and that denials of FSIA immunity can be immediately appealed. *Id.*

b. The court then considered whether a "private compan[y]" like NSO can assert common-law foreign sovereign immunity if it alleges that it is acting as an

---

[5] *See also* U.S. Dep't of Commerce, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

agent of foreign governments. *Id.* at 2. "The law governing this question has roots extending back to our earliest history as a nation," the court explained, and that law "leads to a simple answer—no." *Id.*

The court noted that the FSIA makes sovereign immunity available to entities owned by foreign states but not to private entities. *Id.* at 14; *see* 28 U.S.C. § 1603(b). It then rejected NSO's argument that even though the FSIA does not afford it immunity because it is a private company, NSO could nonetheless invoke a form of common-law sovereign immunity that the Supreme Court held was available to individual foreign officials in *Samantar v. Yousuf*, 560 U.S. 305 (2010).

The court found NSO's logic flawed. Although "the FSIA [is] silent about immunity for individual officials, that is not true for entities—quite the opposite." Pet. App. 12. The FSIA, the court explained, "occupies the field of foreign sovereign immunity as applied to *entities* and categorically forecloses extending immunity to any entity that falls outside the FSIA's broad definition of 'foreign state.'" *Id.* at 2-3. The court added that "[t]he idea that foreign sovereign immunity could apply to non-state entities is contrary to the originating and foundational premise of … immunity doctrine." *Id.* at 12.

The court therefore concluded that the FSIA, "the comprehensive framework Congress enacted for resolving any entity's claim of foreign sovereign immunity," precluded NSO's claim. *Id.* at 19. While the court found no need to specifically address NSO's assertion that it could claim protection under the com-

mon law, it noted that "[t]here is not a single documented instance of the State Department recommending conduct-based immunity for a foreign private corporation." *Id.* at 18 n.8. And it found the absence of any Judicial or Executive Branch precedent for NSO's theory to be "a compelling fact indeed." *Id.* at 18.

5. The court of appeals denied NSO's petition for rehearing and rehearing en banc, which asserted the same purported conflicts and policy arguments asserted here. *Id.* at 85. No judge dissented from that decision or requested a vote on rehearing en banc. The court stayed its mandate pending the filing of a certiorari petition. C.A. Dkt. 90.

REASONS FOR DENYING THE PETITION

The Ninth Circuit correctly resolved an issue that no other circuit had previously addressed—whether a private foreign company can obtain common-law foreign sovereign immunity. Contrary to NSO's submission, the decision below is consistent with decisions from other circuits and with this Court's precedent. No other court has confronted, let alone embraced, NSO's assertion that a private entity can assert common-law sovereign immunity. And no other court has addressed, let alone rejected, the Ninth Circuit's holding that the FSIA comprehensively addresses immunity for entities and precludes resort to the common law.

NSO's assertion that the question presented is important enough to warrant review is also without merit. The question presented rarely arises, and

nothing but speculation supports NSO's claim of importance. In any event, this interlocutory petition would present an exceedingly poor vehicle in which to consider a private entity's immunity claim: even if such claims were theoretically available, which they are not, NSO's claim could not plausibly succeed. The Executive Branch has recently determined that NSO's spyware activities are contrary to U.S. national security and foreign policy, making NSO a singularly improbable candidate for immunity from claims that its spyware activities violated U.S. law. And neither the State Department nor any foreign government has ever endorsed NSO's bid for immunity. For all of those reasons, certiorari should be denied.

A. The Decision Below Does Not Conflict With The Decision Of Any Other Circuit

NSO contends that certiorari is warranted because the Ninth Circuit's decision purportedly conflicts with the decisions of two other courts of appeals. Pet. 11. But no conflict exists: neither the D.C. Circuit nor the Fourth Circuit held that private entities may obtain common-law foreign sovereign immunity.

1. The D.C. Circuit's decision in *Broidy Capital Management LLC v. Muzin*, 12 F.4th 789 (D.C. Cir. 2021), does not hold that private entities may obtain common-law foreign sovereign immunity. As NSO acknowledges, the court in *Broidy denied* a claim of common-law foreign sovereign immunity, Pet. 12; *Broidy*, 12 F.4th at 797-804, and it never specifically analyzed whether—let alone held that—a private entity could qualify for such immunity.

The facts of *Broidy* explain why the D.C. Circuit did not address the entity-immunity question. The defendants were principally natural persons, and the one entity defendant was owned by two of the individual defendants. *See id.* at 793. The D.C. Circuit accordingly viewed the case as involving individual natural-person defendants: the court began by noting the district court's statement that "because *the defendants are private individuals* and not a foreign state the FSIA does not apply." *Id.* at 794 (emphasis added). The court then described the relevant authorities as addressing (and rejecting) immunity claims of individuals like the defendants. *Id.* at 800 ("Past expressions of State Department policy do not support immunity for *private individuals* in the defendants' circumstances." (emphasis added)). Nothing in that analysis addressed *entities*.

If anything, the D.C. Circuit's language in *Broidy* suggests that the court believed that common-law foreign sovereign immunity is limited to individuals. The court noted that "[f]oreign sovereign immunity may, in certain circumstances, … protect *individuals* even though the FSIA does not." *Id.* at 798 (quotation omitted and emphasis added); *see also id.* (describing "conduct-based immunity" as reserved for an "act performed by the *individual* as an act of the State" (emphasis added)). And the court observed that "the Supreme Court in *Samantar* acknowledged that, in addition to the immunity of sovereign states that Congress codified in the FSIA, residual conduct-based immunity may protect *certain individual officials of foreign governments*." *Id.* at 796-97 (emphasis added).

NSO relies (Pet. 13) on one parenthetical in the D.C. Circuit's opinion describing *Samantar* as "holding the FSIA applies only to states and their 'agenc[ies] or instrumentalit[ies],' excluding private entities or individuals." *Broidy*, 12 F.4th at 802 (quotation omitted). But that parenthetical accurately describes the FSIA—the FSIA indeed does not provide immunity to private entities or individuals—and the Ninth Circuit agreed with that description. *See* Pet. App. 14-15. The parenthetical's reference to "entities" does not somehow suggest that the D.C. Circuit held that private entities, while excluded from the FSIA, are eligible for common-law immunity. Such a view would not comport with the court's many other references to the common-law immunity of "individuals" alone. As the Ninth Circuit recognized when distinguishing *Broidy*, "[t]he D.C. Circuit did not make an explicit finding that foreign sovereign immunity claims from foreign private entities should be analyzed under the common law." Pet. App. 15 n.5.

Even if NSO's strained reading of *Broidy*'s parenthetical were correct, at best it would represent the panel's implicit view offered in dicta. Such dicta would not bind any future D.C. Circuit panel, so it could not create a conflict with the decision below warranting this Court's intervention.

2. Nor does the Fourth Circuit's decision in *Butters v. Vance International, Inc.*, 225 F.3d 462 (4th Cir. 2000), create a conflict justifying this Court's review. *Contra* Pet. 12.

Butters did not base its holding on the common-law immunity that NSO invokes. *Butters* did hold that sovereign immunity protected a private entity—

albeit a domestic one rather than a foreign one like NSO. *See* Pet. App. 17 n.6 ("*Butters* did not discuss whether this … doctrine also extends to *foreign* contractors acting on behalf of foreign states."). But the Fourth Circuit squarely rested that holding on "derivative immunity *under the FSIA*." 225 F.3d at 466 (emphasis added). NSO relied on that derivative-immunity theory in the district court, *see* Dist. Ct. Dkt. 45, at 9-10, but abandoned it on appeal, *see* Br. for Appellants, C.A. Dkt. 24., at 30-50. The Fourth Circuit's application of a separate doctrine that NSO no longer invokes and that the Ninth Circuit did not address cannot create a conflict.

That is especially true because *Butters* is no longer good law: *Samantar* abrogated the Fourth Circuit's FSIA-based derivative-immunity theory. *Samantar* held that to qualify for FSIA immunity, a defendant must show that it is a "foreign state" or state instrumentality "within the meaning of the Act." 560 U.S. 305, 313 (2010). But rather than look to the meaning of the Act, *Butters* applied an atextual theory of "derivative immunity under the FSIA" to protect an entity that would *not* have qualified under the FSIA's terms. 225 F.3d at 466. As the D.C. Circuit explained in *Broidy*, "*Butters* predates *Samantar* and by its own terms applies the FSIA itself to a private actor's claim of immunity"—an approach "[t]he Supreme Court foreclosed … in *Samantar*." 12 F.4th at 802. Accordingly, the Ninth Circuit here correctly recognized that *Butters* lacks ongoing force. Pet. App. 17 n.6. And an abrogated decision cannot create a circuit conflict warranting this Court's review.

NSO argues that *Butters* only "*arguably* located the source of immunity in the FSIA," Pet. 12 (emphasis added)—but the Fourth Circuit's language unequivocally refutes that argument. *See Butters*, 225 F.3d at 466 (stating that the defendant was "entitled to derivative immunity *under the FSIA*" (emphasis added)); *id.* at 467 (describing its holding as what "[t]he Act requires"). Nor has the Fourth Circuit since adopted NSO's interpretation of its decision. NSO also maintains that even if *Butters* is a FSIA decision, it at least remains "instructive" when answering questions of common-law foreign sovereign immunity. Pet. 12 (quotation omitted). But that suggestion lacks merit because *Butters* sought only to apply the FSIA; it did not invoke common-law reasoning that could conceivably apply *outside* the FSIA. Because the Fourth Circuit mistakenly located its immunity theory *in* the FSIA, and because *Samantar* abrogated its analysis, *Butters* provides no support for NSO's conflict claim.[6]

B. The Decision Below Is Correct

NSO contends that the Ninth Circuit's decision is incorrect because, in NSO's view, the decision conflicts with this Court's holding in *Samantar*. Pet. 19-

---

[6] NSO cites two district court cases that purportedly apply *Butters* as a common-law immunity case. *See* Pet. 12. But the parties seeking immunity in both *Ivey for Carolina Golf Development Co. v. Lynch*, 2018 WL 3764264 (M.D.N.C. Aug. 8, 2018), and *Moriah v. Bank of China Ltd.*, 107 F. Supp. 3d 272 (S.D.N.Y. 2015), were not foreign entities but individuals. In any event, a district court's interpretation of *Butters* could not create a circuit conflict warranting certiorari.

21. In fact, the decision below accords with *Samantar*, this Court's understanding of the FSIA, and Executive Branch practice, which affords no example in history in which the government has supported an immunity claim like NSO's.

1. NSO contends (Pet. 19) that the decision below conflicts with *Samantar*, but that contention is incorrect, as the Ninth Circuit explained. Pet. App. 10-12. *Samantar* held that common-law immunity for "individual officials"—*i.e.*, "natural persons"—survived the FSIA. 560 U.S. 305, 315-16 (2010). That is because Congress did not "inten[d] to include individual officials within" the Act's scope, *id.* at 316-17, and "did not mean to cover … types of defendants never mentioned in the text," *id.* at 319. "The immunity of officials," the Court explained, "simply was not the particular problem to which Congress was responding when it enacted the FSIA." *Id.* at 323. Or as the Ninth Circuit put the point: *Samantar* held that "the FSIA did not address, *at all*, immunity for individuals or natural persons." Pet. App. 15; *see id.* at 11 (noting "the absence of any reference to individual foreign officials" in the FSIA). As to individual officials, then, there is a "gap left by Congress's silence" that courts may use federal common law to "fill[]." *Mobil Oil Corp. v. Higginbotham*, 436 U.S. 618, 625 (1978).

In contrast, the FSIA leaves no gap when it comes to the immunity of entities. To the contrary, "the types of defendants listed [in the FSIA] are *all entities*," Pet. App. 12 (quoting *Samantar*, 560 U.S. at 317), because Congress sought "to address a modern world where foreign state *enterprises* are every day participants in commercial activities," *Samantar*, 560

U.S. at 323 (quotation omitted and emphasis added). Specifically, the FSIA makes immunity available to "any *entity* [that] is a separate legal person, corporate or otherwise, and … which is an organ of a foreign state or political subdivision thereof, or a majority of whose shares or other ownership interest is owned by a foreign state or political subdivision thereof." 28 U.S.C. § 1603(b) (emphasis added). These entity-specific terms are "explicit and straightforward," *Dole Food Co. v. Patrickson*, 538 U.S. 468, 477 (2003)—and they extend immunity to entities that are "sovereign" or "have a sufficient relationship to a sovereign," Pet. App. 14, but not to private entities. Because the FSIA thus embodies a "comprehensive statutory scheme" governing which entities may obtain immunity, *Republic of Austria v. Altmann*, 541 U.S. 677, 699 (2004), "it is improper for courts to consider common-law principles" in that area, Pet. App. 10. The contrary result would allow courts to "rewrit[e] [the] rules that Congress has affirmatively and specifically enacted." *Mobil Oil Corp.*, 436 U.S. at 625. That is especially "danger[ous]" and unwarranted given the "foreign policy consequences" attached to sovereign immunity determinations. *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 116 (2013).

2. The court of appeals' analysis accords with this Court's general recognition that the FSIA creates a "comprehensive set of legal standards governing claims of immunity … against a foreign state or its political subdivisions, agencies or instrumentalities." *Verlinden B.V. v. Cent. Bank of Nigeria*, 461 U.S. 480, 488 (1983). While it is true that the FSIA is comprehensive only "within its field," Pet. 21, the FSIA's

"field" expressly governs immunity for entities. And an entity that does not qualify for immunity under the FSIA's terms cannot circumvent Congress's comprehensive scheme by claiming common-law immunity instead. NSO's contrary argument overlooks the principle that in the FSIA's treatment of entities, "[t]he expression of one thing implies the exclusion of another," Pet. App. 14 n.3, a principle that this Court has effectively applied in construing the FSIA, *see Dole Food*, 538 U.S. at 474 (reasoning that "indirect subsidiaries of the State of Israel" could not claim FSIA immunity because they did not "come within the statutory language" covering only direct subsidiaries). NSO thus errs in asserting (Pet. 19) that the FSIA has "nothing to say" about non-state entities. Rather, the FSIA "speaks directly to the question at issue," *i.e.*, *which* entities can qualify for immunity, and thus the statute precludes courts from resorting to "federal common law." *Am. Elec. Power Co. v. Connecticut*, 564 U.S. 410, 424 (2011) (alterations and quotation omitted).

3. NSO also asserts that the Ninth Circuit's decision is inconsistent with the "assumption that common-law principles of immunity were incorporated into our judicial system and that they should not be abrogated absent clear legislative intent to do so." Pet. 20 (quotation omitted). But no common-law principle of foreign sovereign immunity has ever protected private entities. "The idea that foreign sovereign immunity could apply to non-state entities is contrary to the originating and foundational premise of … immunity doctrine." Pet. App. 12. Rather, common-law

foreign sovereign immunity protects only *natural persons* who represent foreign governments—typically employees or officials. Both judicial precedent and Executive Branch practice uniformly limit common-law foreign sovereign immunity to individuals. *See* Pet. App. 18 ("[it] is a compelling fact indeed" that "neither the State Department nor any court has ever applied foreign official immunity to a foreign private corporation under the common law").

a. When tracing the history of common-law foreign sovereign immunity, *Samantar* referred solely to the "immunity of individual officials," 560 U.S. at 320; *see id.* at 321, and never suggested that entities might qualify. That is because the doctrine shields officials and agents from liability for acts taken "as representatives of their government[]"—"for example, an official sign[ing] a treaty or … a contract in the name of the government." Beth Stephens, *The Modern Common Law of Foreign Official Immunity*, 79 Fordham L. Rev. 2669, 2693 (2011). And it extends only to "official acts while [the defendant was] in office." *Yousuf v. Samantar*, 699 F.3d 763, 774 (4th Cir. 2012) (quotation omitted). Only natural persons—not entities—act as governmental "representatives" and serve "in office."

NSO cannot identify a single case supporting its position that common-law foreign sovereign immunity can apply to private entities. The majority of NSO's cited cases (Pet. 2-6) involve current or former government *officials*, who were natural persons. That

is true of NSO's pre-*Samantar* cases,[7] post-*Samantar* cases,[8] and foreign cases.[9] To the extent these authorities use the term "agent," they do so interchangeably and synonymously with "official."[10] Even in the handful of cases involving agents who were not formally

---

[7] *See Underhill v. Hernandez*, 168 U.S. 250, 252 (1897) (Venezuelan general); *Matar v. Dichter*, 563 F.3d 9, 10 (2d Cir. 2009) ("former head of the Israeli Security Agency"); *Belhas v. Ya'alon*, 515 F.3d 1279, 1285 (D.C. Cir. 2008) (former Israeli "Head of Army Intelligence"); *Velasco v. Gov't of Indonesia*, 370 F.3d 392, 395 (4th Cir. 2004) (Indonesian government officials); *In re Estate of Marcos*, 25 F.3d 1467, 1469 (9th Cir. 1994) (former "President of the Philippines"); *Chuidian v. Philippine Nat'l Bank*, 912 F.2d 1095, 1099 (9th Cir. 1990) (member of Philippine governmental commission); *Heaney v. Gov't of Spain*, 445 F.2d 501, 501 (2d Cir. 1971) (Spanish "consular representative"); *Herbage v. Meese*, 747 F. Supp. 60, 61 & n.2 (D.D.C. 1990) (British officials, including "the Secretary of State for the Home Department" and "former Director, U.K. Department of Public Prosecutions"); *Greenspan v. Crosbie*, 1976 WL 841, at *1-2 (S.D.N.Y. Nov. 23, 1976) (three of the "highest officials" of the Province of Newfoundland and Labrador); *Waltier v. Thomson*, 189 F. Supp. 319, 319-21 (S.D.N.Y. 1960) ("officer in charge of the Canadian Government Immigration Service"); *Lyders v. Lund*, 32 F.2d 308 (N.D. Cal. 1929) ("consul of Denmark at San Francisco").

[8] *See Doğan v. Barak*, 932 F.3d 888, 891 (9th Cir. 2019) (former "Israeli Defense Minister"); *Yousuf*, 699 F.3d at 766 ("high-ranking government official in Somalia"); *Smith v. Ghana Com. Bank, Ltd.*, 2012 WL 2923543, at *1 (D. Minn. July 18, 2012) (Ghana's President and Attorney General).

[9] *See Jones v. Ministry of Interior*, UKHL 26 (House of Lords, U.K. 2006) ("Lieutenant Colonel" of Saudi Arabia); *Church of Scientology Case*, 65 ILR 193, 198 (Fed. Supreme Ct., Ger. 1978) (head of London police force).

[10] *See, e.g.*, *Velasco*, 370 F.3d at 400 (referring to an "agent's conduct" in the context of holding that the FSIA's "commercial

government officials, the agents were still natural persons—not artificial entities.[11] *Butters* is the only case NSO cites that grants immunity to a private entity, but *Butters* did not rest on common-law immunity at all, and *Samantar* abrogated *Butters*' FSIA-based derivative-immunity theory. *See supra* at 13-15.[12]

b. Executive Branch immunity practice is in accord. "[T]his Court consistently has deferred to the

---

activity exception may be invoked against a foreign state only when its *officials* have actual authority" (emphasis added)); *Heaney*, 445 F.2d at 505 (noting plaintiffs' allegation that a consular official "was an 'employee or agent' of the Spanish Government at all relevant times").

[11] *See Mireskandari v. Mayne*, 800 Fed. App'x 519, 519-20 (9th Cir. 2020) (investigators for organ of foreign state); *Ivey for Carolina Golf Dev. Co. v. Lynch*, 2018 WL 3764264, at *7 (M.D.N.C. Aug. 8, 2018) (attorney appointed by German official to administer insolvency proceedings); *Moriah v. Bank of China Ltd.*, 107 F. Supp. 3d 272, 278 (S.D.N.Y. 2015) (advisor to Israeli government); *Rishikof v. Mortada*, 70 F. Supp. 3d 8, 10 (D.D.C. 2014) (delivery worker for Swiss Confederation); *Alicog v. Kingdom of Saudi Arabia*, 860 F. Supp. 379, 381 (S.D. Tex. 1994) (Texas residents hired by Saudi Arabia); *Am. Bonded Warehouse Corp. v. Compagnie Nationale Air France*, 653 F. Supp. 861, 863 (N.D. Ill. 1987) ("employees of Air France").

[12] NSO's reliance on the United States Convention on Jurisdictional Immunities of States and their Property (Pet. 7) is also flawed. As the Foreign Sovereign Immunity Scholars *Amici Curiae* Brief in the court below explained, the Convention's immunity provision "identifies a category of *natural persons* to be treated as a 'State' for the purposes of the Convention." C.A. Dkt. 47-2, at 21-22 (internal quotation and citation omitted). And the Convention "has not been ratified by the United States or even entered into force for other countries." *Id.* at 22 n.17.

decisions of the political branches—in particular, those of the Executive Branch—on whether to take jurisdiction over actions against foreign sovereigns and their instrumentalities." *Verlinden*, 461 U.S. at 486. And as the Ninth Circuit here explained, "[t]here is not a single documented instance of the State Department recommending conduct-based immunity for a foreign private corporation." Pet. App. 18 n.8 (collecting authority). Nor does NSO cite such an instance in its petition. Instead, the State Department's immunity practice has exclusively protected individuals or foreign-state-owned entities, not private entities. This unbroken Executive Branch practice is independently dispositive because it is "not for the courts … to allow an immunity on new grounds which the government has not seen fit to recognize." *Republic of Mexico v. Hoffman*, 324 U.S. 30, 35 (1945).

C. The Petition Does Not Present An Important And Recurring Question

NSO also argues that certiorari is warranted because, in its view, the case raises "an important question with significant foreign-policy implications." Pet. 14. That argument lacks merit. The issue here rarely arises, and NSO's foreign-policy speculation provides no basis for review.

1. The question presented hardly ever arises, demonstrating its lack of practical significance. The decision below is the *only* case that has resolved whether private entities may claim common-law foreign sovereign immunity. As noted, *Butters* resolved whether a private entity could claim derivative sovereign immunity under the FSIA—but that is a different form of immunity that *Samantar* abrogated. The

absence of cases resolving the question presented is strong evidence that the question is insufficiently important to justify the expenditure of this Court's scarce resources.

2. According to NSO, however, the issue here is important because the Ninth Circuit's decision will undermine the United States' interests in asserting immunity for its contractors in foreign courts. *See* Pet. 15-17. Certiorari is not warranted based on NSO's unsupported speculation about the impact of the decision below on U.S. overseas operations and foreign affairs. NSO's credibility in assessing that issue is, to put it mildly, suspect. The federal government has placed NSO on the Entity List precisely because its activities undermine U.S. national security and foreign policy, *see supra* at 7-8—making it an unlikely source for assessing U.S. foreign-policy interests.[13]

---

[13] Citing WhatsApp's court of appeals brief, NSO suggests that WhatsApp seeks to "discourage governments, expressly including the United States, from using technology like NSO's" or from using contractors in military or intelligence operations. Pet. 17. NSO ignores that WhatsApp's principal submission below was that "foreign-policy judgments are the province of the political branches, not the courts." Br. for Appellees, C.A. Dkt. 32, at 45. WhatsApp addressed NSO's policy arguments only in the alternative. *See id.* at 47 ("Even assuming that the separation of powers allowed this Court to expand artificial-entity immunity in contravention of the FSIA's text to account for foreign-policy considerations, those considerations only undermine NSO's immunity claim."). And WhatsApp's action seeks relief based only on *NSO*'s accountability for malicious spyware attacks against WhatsApp, in violation of U.S. law.

"The political branches"—not NSO—"have the responsibility and institutional capacity to weigh foreign-policy concerns." *Jesner v. Arab Bank, PLC*, 138 S. Ct. 1386, 1403 (2018). And here, the political branches have already spoken to whether private entities may obtain common-law foreign sovereign immunity—Congress through the FSIA, and the Executive Branch through its longstanding immunity practice discussed above. The United States has never expressed concern that its interests would be harmed by denying immunity to private contractors of foreign governments. During the lengthy proceedings in this case, the federal government never suggested immunity for NSO; rather, it placed NSO on the Entity List. And in case after case, the United States has consistently recognized common-law immunity only for individuals or foreign-state-owned entities, not for private entities. *See* Pet. App. 18 n.8 ("There is not a single documented instance of the State Department recommending conduct-based immunity for a foreign private corporation.").

NSO emphasizes a footnote in the government's amicus brief in a different case, addressing a different issue, Pet. 17-18; *id.* at 22, but that footnote does not assist NSO. In a 2021 amicus brief about whether an interlocutory appeal should be permitted when federal contractors invoke the United States' sovereign immunity, the government noted that the question whether it can argue that sovereign immunity shields its contractors in foreign courts "is not presented in this case." Br. for the United States as Amicus Curiae at 9 n.1, *CACI Premier Tech., Inc. v. Al Shimari*, No.

19-648 (U.S. Aug. 26, 2020). The government's observation that a question is not presented—without taking any stance on its merits—hardly supports NSO's position here.

In all events, the United States' interests are best served by respecting the balance Congress struck in the FSIA—extending immunity to state-owned entities, but not private entities selling their services to foreign governments and others. The "[c]omity and dignity interests" animating immunity for foreign states and their instrumentalities, *Republic of Philippines v. Pimentel*, 553 U.S. 851, 866 (2008), are absent for private companies—who need are not foreign officials or government employees and (like NSO) may work for *multiple* foreign governments. Even in the domestic context, there is "no authority for the notion that private persons performing Government work acquire the Government's embracive immunity." *Campbell-Ewald v. Gomez*, 577 U.S. 153, 166 (2016). Courts therefore should not override the political branches' refusal to accord immunity to private entities acting as contractual agents for foreign governments.

D. This Case Is An Unsuitable Vehicle For Certiorari And A Poor Candidate For Inviting The Government's Views

Even if the question presented warranted certiorari in theory (it does not), this case would present a singularly unsuitable vehicle in which to address it. The question presented is not outcome determinative because NSO would not prevail on its immunity claim even if private entities were eligible for common-law

sovereign immunity. And this case arises in an interlocutory posture with an undeveloped factual record and a threshold question of appellate jurisdiction. Nor is there any reason to delay this case further by inviting the Solicitor General to express the United States' views on the petition.

1. Even assuming that private entities were eligible to obtain common-law foreign sovereign immunity, NSO's immunity claim here would have no plausible chance of succeeding for two reasons.

First, recent Executive Branch action makes clear that NSO's immunity argument is untenable. As explained above, *see supra* at 7-8, on November 4, 2021, the federal government added NSO to the Entity List on the ground that NSO "developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers." 86 Fed. Reg. 60759. Nothing suggests that the Executive Branch would ever support immunity for an entity whose activities it has determined are contrary to U.S. national security or foreign policy—especially when those activities overlap with the activities for which the entity seeks immunity. To the extent the Court wishes to resolve whether a foreign private entity may assert common-law foreign sovereign immunity, it should await a case in which the foreign private-entity defendant is not so obviously unqualified. The United States' designation of NSO as a *persona non grata* thus affords an independently sufficient reason for denying the petition.

Second, NSO's claim would fail under the established foreign-official immunity framework. A "two-

step procedure" applies "when a foreign official" or agent "assert[s] immunity." *Samantar v. Yousuf*, 560 U.S. 305, 312 (2010). First, the official or sovereign he represents can "request a 'suggestion of immunity' from the State Department." *Id.* at 311. Second, absent a suggestion of immunity, a court "ha[s] authority to decide for itself whether all the requisites for such immunity exist." *Id.*

Here, NSO does not purport to have requested immunity from the State Department, and the State Department has never suggested that NSO should be immune. *See* Pet. App. 34. Nor has any foreign government stepped forward to support immunity for NSO. In fact, NSO's only basis for its claimed relationship with foreign governments is a self-serving declaration by its CEO, *see* C.A. E.R. 51-56, and NSO has never even identified which foreign governments it contracts with. So if the analysis were to proceed on NSO's flawed theory, the judiciary would have to decide for itself whether immunity may attach.

In making that determination, courts would ask whether "the ground of immunity is one which it is the established policy of the [State Department] to recognize." *Samantar*, 560 U.S. at 312 (noting that pre-FSIA courts applied this test) (citing *Republic of Mexico v. Hoffman*, 324 U.S. 30, 36 (1945)); *see Broidy Capital Mgmt. LLC v. Muzin*, 12 F.4th 789, 798 (D.C. Cir. 2021) (applying this test); *Doğan v. Barak*, 932 F.3d 888, 893 (9th Cir. 2019) (same). Under that test, NSO clearly cannot qualify for immunity, since no State Department guidance recognizes immunity for

private entities contracting with foreign governments—let alone private entities that the government has placed on the Entity List. *See supra* at 21-22.

2. The case's interlocutory posture likewise makes it an unsuitable vehicle in which to decide the question presented. *Contra* Pet. 18. Because the Ninth Circuit rejected NSO's immunity assertion, WhatsApp's claims can proceed to discovery and trial in district court. This Court ordinarily grants review after final judgment—not where, as here, a case arises in an interlocutory posture. *See* Robert Stern & Eugene Gressman, Supreme Court Practice, Ch. 4, § 4.18 (9th ed. 2008); *see also, e.g.*, *NFL v. Ninth Inning, Inc.*, 141 S. Ct. 56, 57 (2020) (mem.) (Kavanaugh, J., statement respecting the denial of certiorari) ("the interlocutory posture is a factor counseling against this Court's review at this time").

That practice makes good sense here. To succeed on its immunity claim (assuming *arguendo* it is eligible at all), NSO would have to show that it acted in an "official capacity" as an agent for foreign governments. *See, e.g.*, *Park v. Shin*, 313 F.3d 1138, 1144 (9th Cir. 2002); *see also Hoffman*, 324 U.S. at 33-34 (defendant engaged "in a private … venture" not in "public service of [a] government" lacks immunity). But it is highly unlikely that NSO can make that showing. *See* Br. for Appellees, C.A. Dkt. 32, at 54-59 (developing this argument in detail). NSO undertook its unlawful conduct as a for-profit company, not as a government agent: NSO itself conceived, executed, marketed, and sold its spyware for private commercial gain. *See* C.A. E.R. 63-64, 68-69. No foreign sovereign identified a need for NSO's services, retained

NSO to create a product, and directed NSO to deliver a product or service subject to government specifications and control. And although NSO claims to work exclusively for foreign governments, its sole support for that claim is a self-serving declaration by its CEO, and it has never even identified which governments it works for. *See supra* at 27. For these reasons, WhatsApp has consistently sought jurisdictional discovery to test whether NSO in fact acted in an official capacity. *See* Br. for Appellees, C.A. Dkt. 32, at 59-60. Such discovery and factual development would shed light on whether NSO's immunity claim has any factual foundation—and if it does not, then resolving the question presented here would make no difference in this case.[14]

Beyond that, WhatsApp contested interlocutory appellate jurisdiction in the Ninth Circuit, *see* Br. for Appellees, C.A. Dkt. 32, at 17-23; Mot. to Dismiss, C.A. Dkt. 13-1, and this Court would have to resolve that issue before it could reach the question presented. The Ninth Circuit found appellate jurisdiction under the collateral-order doctrine because "the FSIA governs NSO's claim of immunity." Pet. App. 6. While it is true that the FSIA governs (and displaces) common-law immunity for entities, it is not clear why the collateral-order doctrine should apply to a denial

---

[14] NSO asserts that the district court "found that NSO acted in its 'official capacity,'" Pet. 13 n.1, but the district court made that statement in the context of a motion to dismiss absent any discover, *see* Pet. App. 35. That statement in no way constitutes a "finding" on the issue.

of NSO's common-law immunity claim, which is not based on the FSIA.

Common-law immunity and FSIA immunity are critically different for purposes of the collateral-order doctrine. *See* Br. for Appellees, C.A. Dkt. 32, at 17-23. FSIA immunity is grounded in an "explicit statutory … guarantee that trial will not occur," *Midland Asphalt Corp. v. United States*, 489 U.S. 794, 801 (1989), and it protects a foreign state's "dignity interests" in avoiding any judicial process at all, *Republic of Philippines v. Pimentel*, 553 U.S. 851, 866 (2008). Those are hallmarks of an immunity that implicates the collateral-order doctrine. But any common-law immunity for a private entity could share neither trait: it would not rest on an explicit statutory guarantee and a private contractor has no dignity interest to protect. *See* Br. for Appellees, C.A. Dkt. 32, at 22. And contrary to NSO's contention (Pet. 19), a contractor-based immunity would operate as a defense to liability, rather than an immunity from suit, such that it can "be reviewed 'effectively' after a conventional final judgment." *Will v. Hallock*, 546 U.S. 345, 351 (2006).

In reviewing these same arguments, the D.C. Circuit observed that its interlocutory jurisdiction over a denial of common-law foreign sovereign immunity for individuals was "a close question." *Broidy*, 12 F.4th at 796. The court ultimately found jurisdiction because the defendants were "individual agents" of an identified "foreign state," and that foreign state possessed "dignitary interests in avoiding suit, not just ultimate liability." *Id.* at 796-97. The argument for interlocutory jurisdiction is far more attenuated here, because a *private, non-state entity contractor* cannot

plausibly claim to share the dignity interests of (never-identified) foreign states. If certiorari is ever warranted on the question presented, the Court should avoid this difficult jurisdictional issue by waiting for a case that arises after final judgment.

3. Finally, NSO argues that if the Court does not grant the petition outright, it should invite the Solicitor General to express the views of the United States. Pet. 21-22. That course is not warranted. The government has had ample time and opportunity to consider the question presented here, and it has not once suggested that common-law foreign sovereign immunity should apply to private entities—much less to a private entity that the Executive Branch has recently added to the Entity List. A certiorari petition is far too late in the day for NSO to request what it seemingly has never sought and definitively has never obtained: the support of the United States government for a claim of immunity from accountability in a United States court for violations of United States law. NSO emphasizes that the United States has "alerted the Court" to foreign-policy risks in *other* circumstances. Pet. 15. But that fact just underscores the government's silence over the years in *this* circumstance. That silence speaks volumes.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be denied.

Respectfully submitted.

Anton Metlitsky
O'MELVENY & MYERS LLP
Times Square Tower
7 Times Square
New York, NY 10036
(212) 326-2000

Michael R. Dreeben
Counsel of Record
Ephraim McDowell
O'MELVENY & MYERS LLP
1625 Eye Street N.W.
Washington, D.C. 20006
(202) 383-5300
mdreeben@omm.com

May 3, 2022