No. 20-16408

In the

United States Court of Appeals

For the Ninth Circuit

NSO Group Technologies Ltd. et al.,
Defendants-Appellants

v.

WhatsApp Inc., et al.,
Plaintiffs-Appellees

On Appeal from the United States District Court
for the Northern District of California
Case No. 4:19-cv-07123-PJH

Brief for Appellees

Yaira Dubin
Alec Schierenbeck
O'Melveny & Myers LLP
7 Times Square
New York, NY 10036
(212) 326-2000
ydubin@omm.com
aschierenbeck@omm.com

Michael R. Dreeben
Ephraim McDowell
O'Melveny & Myers LLP
1625 Eye Street, N.W.
Washington, DC 20006
(202) 383-5300
mdreeben@omm.com
emcdowell@omm.com

Counsel for Appellees WhatsApp Inc. and Facebook, Inc.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Appellees Facebook, Inc. and WhatsApp Inc. hereby disclose that Facebook, Inc. is a publicly traded company and has no parent corporation; no publicly held company owns 10% or more of its stock; and WhatsApp Inc. is a wholly owned subsidiary of Facebook, Inc.

Dated: December 16, 2020

By: /s/ Michael R. Dreeben
Michael R. Dreeben

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes

Other Authorities

TABLE OF AUTHORITIES
(continued)

Page(s)

Treatises

INTRODUCTION

Appellant NSO Group Technologies Ltd. is a private software company based in Israel that develops, tests, markets, distributes, and operates spyware for profit. NSO's spyware is designed to surreptitiously intercept communications and extract data from a victim's mobile device. NSO unlawfully used WhatsApp servers and the WhatsApp service to install its spyware on mobile devices of approximately 1,400 WhatsApp users worldwide, including journalists, attorneys, political dissidents, and human-rights activists, in violation of federal and state law.

After uncovering and stopping NSO's privacy abuses, WhatsApp sued NSO in federal district court. Rather than defend its conduct on the merits, NSO—a private company—has claimed foreign sovereign immunity for its actions. In so doing, NSO does not invoke the Foreign Sovereign Immunities Act ("FSIA"), the lone statutory framework governing foreign sovereign immunity claims by corporate entities. Instead, it relies solely on a novel common-law sovereign immunity defense and a self-serving declaration from its CEO asserting that NSO's spyware is used exclusively by undisclosed foreign governments. In NSO's view, a private company should be treated as a foreign sovereign and allowed to escape accountability for, and discovery into, unlawful acts based on the unverified allegations of its CEO. After the

district court correctly rejected NSO's unprecedented immunity theory, NSO lodged this appeal.

NSO's immunity claim is unsustainable on every level. At the threshold, this Court lacks jurisdiction over NSO's interlocutory appeal. The conduct-based immunity NSO claims operates as a defense to *liability*—not an immunity from *suit*—rendering the collateral-order doctrine inapplicable. Accordingly, NSO's appeal should be dismissed.

But even if this Court had jurisdiction, NSO's immunity theory would fail on the merits. Common-law conduct-based immunity has always been understood to protect only *natural persons* who represent foreign governments—typically governmental employees or officials—not private companies like NSO. That is why NSO cannot cite a single Judicial or Executive Branch precedent extending common-law conduct-based immunity to a private company.

Lacking support in existing law, NSO asks this Court to create a novel and sweeping common-law rule to protect private, for-profit companies whose goods and services are marketed to and purchased by unidentified foreign governments—and in at least one instance, sold through a private reseller, not NSO itself. But in the FSIA, Congress spoke directly to the issue of foreign sovereign immunity for corporate entities. And federal courts

cannot revise Congress's dictates through federal common law. That is doubly true in the field of foreign relations—long the political branches' exclusive province. Yet even if this Court had residual authority in this area after the FSIA's enactment, no policy justification could support NSO's proposed rule. Permitting private companies like NSO to act with impunity would serve no one's interests except for those of NSO and similar spyware providers. NSO's proposed immunity regime would create a gaping regulatory void, leaving targets of unlawful acts without redress.

Finally, even if conduct-based immunity could ever shield corporate entities (it cannot), NSO's immunity claim flouts the established requirements for that immunity. NSO's assertion of immunity based on a single untested declaration—lacking supporting documentation, identifying no governmental clients, and describing no details of any agreements with its clients (including what its spyware was used for)—is woefully inadequate. Even on the declaration's own terms, NSO engaged not in "official" actions, but rather private conduct for commercial gain. And a judgment here would enforce a rule of law against only NSO—not any of the unidentified foreign states that supposedly benefit from NSO's spyware, as would be required to support an immunity defense.

In short, NSO has taken an improper interlocutory appeal, seeking a novel form of common-law immunity that no court has ever recognized, all in an attempt to escape the rules Congress established in the FSIA and avoid any inquiry into its unlawful practices. This Court should dismiss NSO's appeal or, in the alternative, affirm the district court.

JURISDICTIONAL STATEMENT

The district court had jurisdiction under 28 U.S.C. §§ 1331, 1332, and 1367. ER64.[1] NSO has filed an interlocutory appeal from the district court's July 16, 2020 order denying NSO's motion to dismiss on sovereign-immunity grounds. ER9-15; ER46-50. As explained below, this Court lacks jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

1. Whether this Court has jurisdiction over NSO's interlocutory appeal.

2. Whether NSO is entitled to conduct-based foreign-official immunity, where it is a corporate entity that cannot satisfy the FSIA's express criteria for corporate immunity.

[1] "ER" refers to the Excerpts of Record; "ECF" refers to the district court's docket; "Dkt." refers to this Court's docket. All internal quotation marks are omitted unless otherwise indicated.

STATEMENT

A. Factual Background[2]

1. WhatsApp provides an end-to-end encrypted communication service available on mobile devices and computers. ER65 ¶ 17. Approximately 1.5 billion people across 180 countries have installed the WhatsApp app and use the app to make calls, send text messages and videos, and transfer files. ER65 ¶¶ 17-18. All of these communications are encrypted through a protocol that ensures no one other than the sender and intended recipient(s) can see them. ER65 ¶ 18. Facebook owns WhatsApp. ER65 ¶¶ 15-16. Both Facebook and WhatsApp are committed to protecting the security of people's private conversations, while honoring valid law-enforcement requests for user data and providing appropriate notice to users when permitted.[3]

To use WhatsApp, a person must create an account and consent to WhatsApp's terms. ER65 ¶ 19. Among other things, those terms require users to agree not to: (a) "reverse engineer" WhatsApp services; (b) transmit "harmful computer code through or onto" WhatsApp services; (c) "gain or

---

[2] The statement draws on the allegations in WhatsApp's complaint, which must "be taken as true" unless "contradicted by affidavit." *Mavrix Photo, Inc. v. Brand Techs, Inc.*, 647 F.3d 1218, 1223 (9th Cir. 2011).

[3] *See* WhatsApp: Information for Law Enforcement Authorities, https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities.

attempt to gain unauthorized access to [WhatsApp] Services or systems"; and (d) "collect the information of or about [WhatsApp] users in any impermissible or unauthorized manner." ER66 ¶ 22. The terms prohibit users from not only personally engaging in this conduct, but also assisting others in doing so. ER66 ¶ 23.

2. NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. (collectively, "NSO") are technology companies incorporated in Israel. ER63-64 ¶¶ 5-6. Q Cyber owns NSO. ER64 ¶ 6. NSO develops, tests, uses, distributes, and causes to be used a suite of surveillance technology, known as "spyware." ER66 ¶ 24. NSO's spyware can be surreptitiously installed on a victim's phone, without the victim taking any action. ER66-67 ¶ 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. ER67 ¶ 27; ER107; ER116. 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. ER67 ¶ 27; ER109; ER116.

NSO develops, markets, and licenses its spyware to customers for a profit—sometimes through arrangements with private resellers. ER67 ¶ 29; *see* ER143-49 (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. ER137-39. 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, ER110; ER124—as well as providing technical support, ER67 ¶ 29. NSO's customers include but are not limited to foreign governments. ER70 ¶ 43; ER143-49. NSO claims that it exclusively contracts with foreign governments, but its only basis for that claim is an unsupported declaration by its CEO. *See* ER51-56.

Public reports cited in WhatsApp's complaint document that NSO spyware has been used to commit serious human-rights abuses. *See* ER70, ¶ 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.[4] And it has reportedly been used to track other journalists, anti-corruption activists, human-rights lawyers, and senior government officials.[5]

---

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

[5] David D. Kirkpatrick & Azam Ahmed, *Hacking a Prince, an Emir and a Journalist to Impress a Client*, New York Times (Aug. 31, 2018), https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html.

3. To facilitate its distribution and administration of spyware, NSO leased and caused to be leased a network of computer servers. ER68-69 ¶ 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. ER68 ¶ 30. NSO then 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 then testing that software. ER69 ¶¶ 35, 37. The software facilitated the transmission of what appeared to be legitimate calls to WhatsApp users. ER69 ¶ 37. In fact, those calls concealed malicious code that could be injected into the memory of the WhatsApp user's device, even if the user did not answer the call. *Id.* The code connected the devices to NSO's servers, ER68 ¶ 32, enabling the capturing and tracking of the user's private data and communications, ER70 ¶ 41. NSO's servers operated as the nerve center through which NSO collected data from its targets and controlled the use of its spyware. ER67 ¶ 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. ER70 ¶ 42. The victims of NSO's attack included attorneys, journalists, human-rights activists, political dissidents, diplomats, and other foreign government officials. *Id.*

On May 13, 2019, Facebook announced that it had investigated and identified a vulnerability involving WhatsApp's service. ER71 ¶ 44. WhatsApp and Facebook closed the vulnerability, contacted law enforcement, and advised users to update the WhatsApp app. *Id.* NSO's cyberattack on WhatsApp users damaged WhatsApp's customer goodwill and forced it to incur costs investigating and preventing NSO's hacking activities.[6] ER71 ¶ 47; ER74 ¶ 73.

[6] NSO begins its brief with a supposed event that occurred in October 2019 when WhatsApp notified users that their devices had been compromised. Br. 1-2. This portrayal has neither support in the record nor relevance to this appeal. To protect user privacy, WhatsApp has a neutral policy of informing users about app vulnerabilities. At the same time, WhatsApp fully cooperates with valid law-enforcement requests for data. *See supra* note 3. In fact, as described in the annual Facebook Transparency Report, Facebook responds to thousands of law-enforcement requests, including requests for data from WhatsApp. *See* Facebook, Government Requests for User Data, https://transparency.facebook.com/government-data-requests. NSO's suggestion that WhatsApp's practices "frustrate … investigations" is baseless. Br. 2. So is its unfounded claim that in connection with the 2017 London terrorist attacks, WhatsApp "refused to turn over the terrorists' messages or assist in apprehending them." Br. 18. In reality, WhatsApp responded to several valid emergency requests relating to these attacks, quickly producing records to assist authorities.

B. Procedural Background

1. On October 29, 2019, Facebook and WhatsApp (together "WhatsApp") sued NSO and Q Cyber in the U.S. District Court for the Northern District of California. ER62. 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* ER63 ¶ 2. WhatsApp's claims arise from NSO's intentional, deceptive, and unauthorized accessing of WhatsApp servers, ER71-72 ¶¶ 50, 54, 59, to inject malicious code onto WhatsApp users' devices, ER73 ¶ 63, which breached WhatsApp's terms, ER74 ¶ 71. WhatsApp sought an injunction restraining NSO from accessing WhatsApp's servers, violating WhatsApp's terms, and impairing WhatsApp's service. ER75 ¶ 2. WhatsApp also sought compensatory, statutory, and punitive damages. ER75 ¶ 3.

2. NSO moved to dismiss for lack of subject-matter jurisdiction, arguing that "the doctrine of derivative sovereign immunity" barred WhatsApp's suit. ECF 45, at 9. NSO conceded that it could "not claim immunity for itself under the [FSIA]," but maintained that it was still "entitled to *derivative* sovereign immunity." ECF 62, at 9. In its motion to dismiss, NSO failed to assert the conduct-based immunity theory it now

raises on appeal. *See* ECF 45. Only in its reply brief did NSO assert that *Butters v. Vance International*, 225 F.3d 462 (4th Cir. 2000), "applied th[e] longstanding rule of [conduct-based] immunity." ECF 62, at 10.

The district court denied NSO's immunity claim. To start, the court noted 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." ER9. NSO's claim to immunity, the court explained, could derive only from the common-law doctrines of "foreign official immunity" or "derivative sovereign immunity." ER9-10. The court held that neither doctrine applied to NSO. ER11-15.

The court first concluded that NSO did not qualify for conduct-based foreign-official immunity because it could not satisfy that doctrine's established prerequisites. ER12. Because the State Department had not issued NSO "a suggestion of immunity," the court explained, NSO must show that its asserted "'ground of immunity'" reflects "'the established policy of the [State Department] to recognize.'" ER10-11 (quoting *Samantar v. Yousuf*, 560 U.S. 305, 312 (2010)). NSO could not make that showing, the court reasoned, because the effect of issuing a judgment against NSO would not "be to enforce a rule of law against" any foreign state. ER10 (quoting Restatement (Second) of Foreign Relations Law § 66(f) (1965)

("Restatement")). Specifically, none of NSO's "foreign sovereign customers would be forced to pay a judgment … if [WhatsApp] were to prevail in this lawsuit," and "the court can craft injunctive relief that does not require a foreign sovereign to take an affirmative action." ER12.

The court next concluded that "the derivative sovereign immunity doctrine articulated by the Fourth Circuit in *Butters*" also does not protect NSO because that doctrine—to the extent it exists at all—would not apply to foreign contractors of foreign sovereigns. *Id.* Although NSO suggested that *Butters* involved foreign-official immunity, the court recognized that NSO's suggestion impermissibly "merg[es] [the] two distinct doctrines [of] foreign official immunity and derivative sovereign immunity." ER11 n.1. And after observing that "the Ninth Circuit has not held that the doctrine of derivative sovereign immunity [for domestic federal contractors] applies to foreign contractors of foreign sovereigns," the court found "no compelling reason to" adopt such a rule. ER13-14. Foreign sovereign immunity and the defense available to federal contractors have different rationales, the court reasoned, and the "grace and comity" interests justifying immunity for foreign *states* do not extend to foreign *contractors*. ER14.

Having rejected NSO's assertions of immunity, the court went on to deny NSO's motion to dismiss for lack of personal jurisdiction, ER15-32, and

for failure to join necessary parties, ER32-35. The court also denied NSO's Rule 12(b)(6) motion challenging WhatsApp's CFAA claim, but granted it on the trespass-to-chattels claim, with leave to amend. ER35-44.

3. NSO filed an interlocutory appeal in this Court on the immunity issue. ER46-50. It also moved to stay all district-court proceedings—including discovery—pending appeal. ECF 117. The district court granted NSO's motion. ECF 155. Meanwhile, WhatsApp moved to dismiss NSO's interlocutory appeal for lack of jurisdiction. Dkt 13-1. A motions panel of this Court denied WhatsApp's motion "without prejudice to renewing the arguments in the answering brief." Dkt. 18.

SUMMARY OF ARGUMENT

On appeal, NSO claims that U.S. courts cannot hold it accountable for its cyberattacks against WhatsApp because, when NSO hacked computers in the United States, NSO acted as an alleged "agent" of foreign governments. But NSO cannot identify a single valid legal authority supporting its supposed common-law sovereign immunity for corporate agents of unidentified foreign governments. Common-law conduct-based foreign-official immunity applies only to natural persons, not corporations. And the only factual basis NSO provides for its purported "agent" status is a single declaration from its CEO stating that NSO performs largely unspecified work

for unidentified sovereigns. No foreign sovereign—much less the U.S. State Department—has come forward to endorse NSO's immunity claim. Granting NSO immunity here would dramatically expand common-law immunity and provide a roadmap for private companies to flagrantly violate U.S. law without repercussions.

I. Initially, the Court lacks jurisdiction over NSO's improper interlocutory appeal. While the collateral-order doctrine confers jurisdiction over denials of immunities from suit, it confers no jurisdiction over denials of defenses to liability. Conduct-based immunity—the only doctrine NSO invokes on appeal—is a defense to liability, because it focuses on the effect of *judgments* on foreign states. Because the district court's denial of NSO's defense can be effectively reviewed after final judgment, the collateral-order doctrine does not apply.

II. In any event, NSO's immunity claim fails on the merits. Having abandoned any claim to derivative foreign sovereign immunity—the theory NSO pressed below—NSO now stakes its entire case on conduct-based foreign-official immunity. But NSO does not qualify for conduct-based immunity under established law, and the Court lacks authority to expand federal common law to include NSO's unprecedented claim.

A. Common-law conduct-based immunity applies only to natural persons, not artificial entities like NSO. NSO cites *no* contrary authority supporting its corporate immunity theory. Rather, judicial precedent, legal treatises, and Executive Branch practice all confirm that conduct-based immunity can apply only to natural persons who represent foreign governments. A private company that sells services used by unidentified foreign sovereigns cannot qualify.

B. Lacking support in existing law, NSO must ask the Court to dramatically expand the established parameters of conduct-based immunity to include activities of a private company that sells a good or service to an unidentified foreign government (even if not directly). But in the FSIA, Congress already codified the circumstances in which artificial entities may claim sovereign immunity. Because those circumstances are not present here—as NSO itself recognizes—NSO's requested immunity would contravene Congress's judgment. *Butters* provides no support for NSO's proposal: *Samantar* overruled that decision; and *Butters* erroneously equates contractors to foreign states with contractors to the United States. Even if policy considerations could ever justify disregarding Congress's judgment in the FSIA, no such considerations support conferring immunity

on a private company selling spyware that unidentified foreign governments use to spy on individuals.

III. Finally, even if conduct-based immunity could ever extend to a private corporation (it cannot), NSO would not qualify. Neither the State Department nor any foreign government has endorsed NSO's immunity claim, and that alone should be dispositive. Nor can NSO satisfy either of the criteria this Court has used to evaluate conduct-based immunity.

A. First, NSO did not undertake its challenged conduct in an "official" capacity. Instead, NSO built and marketed its spyware (sometimes through third-party resellers), hacked into WhatsApp's servers, and orchestrated cyberattacks on journalists, human-rights activists, and political dissidents for private commercial gain. Indeed, the limited record suggests that NSO sometimes contracted with private intermediaries, not foreign sovereigns. NSO's profit-driven acts cannot be considered "official" in nature.

B. Second, a judgment against NSO would not enforce a rule of law against a foreign state—a necessary component of establishing conduct-based immunity. NSO would pay any damages. And NSO cannot seriously contend that an injunction against it would alter any foreign state's conduct when NSO has not even identified the foreign states with which it contracts or the bounds of its supposed agreements with those states.

STANDARD OF REVIEW

This Court reviews issues of common-law sovereign immunity de novo. *Doğan v. Barak*, 932 F.3d 888, 892 (9th Cir. 2019). It can affirm the decision below on any basis supported by the record. *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1047 (9th Cir. 2009).

ARGUMENT

I. This Court Lacks Appellate Jurisdiction Over The District Court's Interlocutory Order

A. As WhatsApp explained in its motion to dismiss in this Court, Dkt. 13-1; *see* Dkt. 15, no jurisdiction exists over NSO's interlocutory appeal. Section 1291 confers jurisdiction to review "final decisions of the district courts." 28 U.S.C. § 1291. Only a "small class" of interlocutory orders qualify as "final decisions." *Cohen v. Beneficial Indus. Loan Corp.*, 337 U.S. 541, 545 (1949). Under the collateral-order doctrine, an interlocutory order is "final" if it "(1) conclusively determine[s] the disputed question, (2) resolve[s] an important issue completely separate from the merits of the action, and (3) [is] effectively unreviewable on appeal from a final judgment." *Puerto Rico Aqueduct & Sewer Auth. v. Metcalf & Eddy, Inc.*, 506 U.S. 139, 144 (1993). To ensure that the collateral-order doctrine's "narrow exception should stay that way," "the conditions for collateral order appeal [are] stringent[ly]"

applied. *Digital Equip. Corp. v. Desktop Direct, Inc.*, 511 U.S. 863, 868 (1994).

The doctrine's third requirement—that an order be effectively unreviewable after final judgment—is determinative here. That requirement distinguishes denials of an immunity from suit, which may be immediately appealable, from denials of a "defense to liability," which are not. *SolarCity Corp. v. Salt River Project Argic. Improvement & Power Dist.*, 859 F.3d 720, 725-26 (9th Cir. 2017) (no appellate jurisdiction over denial of state-action antitrust immunity because it is a defense to liability). While an immunity from suit "frees one who enjoys it from a lawsuit whether or not he acted wrongly," a defense to liability protects a defendant only from a judgment against him. *Richardson v. McKnight*, 521 U.S. 399, 403 (1997). And while an immunity from suit "would be effectively lost" absent immediate review, *Will v. Hallock*, 546 U.S. 345, 350-51 (2006), a defense to liability "can be protected by a post-judgment appeal," making earlier review unnecessary, *SolarCity*, 859 F.3d at 725. Because litigants seeking interlocutory appeal can "loosely … describe[]" "virtually every right … as conferring a 'right not to stand trial,'" "§ 1291 requires courts of appeals to view claims of a 'right not to be tried' with skepticism, if not a jaundiced eye." *Digital Equip.*, 511 U.S. at 873.

B. Although its motion to dismiss argued only that NSO was "entitled to derivative sovereign immunity," ECF 45, at 10, NSO no longer presses that argument on appeal, Br. 42-43. Having waived independent reliance on derivative foreign sovereign immunity, NSO asks this Court to exercise interlocutory review over the district court's denial of "conduct-based foreign sovereign immunity." Br. 27. As explained below, artificial entities like NSO are categorically ineligible for that form of so-called immunity. But even if conduct-based "immunity" could apply here, it operates as a mere defense to liability, which precludes jurisdiction over this interlocutory appeal.

1. Conduct-based immunity extends to foreign officials and agents "for 'acts performed in [their] official capacity if the effect of exercising jurisdiction would be to enforce a rule of law against the state.'" *Doğan*, 932 F.3d at 893-94. The last part of this test—whether exercising jurisdiction would enforce a rule of law against a foreign state—turns on the nature of the *judgment* granted. Conduct-based immunity bars actions where "a *judgment* against the official"—whether money damages or injunctive relief—"would bind (or be enforceable against) the foreign state." *Lewis v. Mutond*, 918 F.3d 142, 146 (D.C. Cir. 2019) (emphasis added). For instance, if a judgment must "draw on the [foreign state's] treasury or force the state to take specific action," then the defense is generally available. *Id.* at 147.

Conversely, if the judgment runs only against the agent in a personal capacity, then the defense is generally unavailable. *See id.* Because the conduct-based-immunity test focuses on the effect of an adverse judgment, a defendant's argument that he must "defend [his actions] in U.S. courts," or be taken "away from [his] official duties," is insufficient to trigger the defense. *Id.*

Accordingly, conduct-based immunity operates as a defense to *liability*, not wholesale immunity from suit. Longstanding Executive Branch precedent supports this view: A 1797 opinion by Attorney General Lee (cited by NSO, Br. 7) explained that while conduct-based foreign-official immunity could apply as a defense on the merits in a suit against a British official, the plaintiff was still "entitled to a trial according to law." 1 Op. Att'y Gen. 81 (1797); *see* Professors Amicus Br., *Samantar v. Yousuf*, 2010 WL 342033, at *7 (Jan. 2010) ("Lee's position appears to have been that the claim of official authority could be a defense on the merits, not an immunity from suit."). And here, the district court's analysis confirms that conduct-based immunity is a liability defense: the court rejected NSO's claim after determining that NSO's "foreign sovereign customers would [not] be forced to pay a *judgment* against defendants," and "the court [could] craft *injunctive relief* that does

not require a foreign sovereign to take an affirmative action." ER12 (emphasis added).

2. NSO errs (Br. 27-28) in relying on this Court's decision in *Doğan* as a basis for jurisdiction. *Doğan* came to this Court after final judgment, so the Court considered only whether conduct-based immunity applied in that case, not whether rejections of that defense satisfy the collateral-order doctrine. 932 F.3d at 892. And in considering the merits of the defendant's argument, the Court examined the plaintiffs' "claims for *relief*"—*i.e.*, their requested *judgment*. *Id.* at 894 (emphasis added). After the Court had concluded that conduct-based immunity applied in that case, it asked whether the Torture Victim Protection Act ("TVPA") "abrogate[s] common law foreign official immunity." *Id.* In explaining that it did not, the Court remarked that "the whole point of immunity is to enjoy 'an immunity from *suit*.'" *Id.* at 895 (quoting *Compania Mexicana de Aviacion, S.A. v. U.S. Dist. Ct.*, 859 F.2d 1354, 1358 (9th Cir. 1988) (per curiam)). Focusing on that one comment in the Court's opinion, NSO argues that denials of conduct-based immunity are subject to collateral-order review. Br. 28.

NSO's argument fails for multiple reasons. First, the case *Doğan* quoted, *Compania Mexicana*, addresses only FSIA immunity. 859 F.2d at 1358. FSIA immunity *is* an immunity from suit grounded in an "explicit

statutory … guarantee that trial will not occur." *Midland Asphalt Corp. v. United States*, 489 U.S. 794, 801 (1989). And FSIA immunity 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). Conduct-based immunity, which is a defense to liability, shares neither trait. Second, *Doğan*'s statement was unnecessary to the Court's only holding—that the official-immunity defense survives the TVPA. Finally, not only is the statement dicta, but it runs counter to this Court's prior holdings that multiple so-called "immunities" are in fact "defense[s] to liability" and therefore not subject to the collateral-order doctrine. *SolarCity*, 859 F.3d at 726 (state-action antitrust immunity); *Alaska v. United States*, 64 F.3d 1352, 1356 (9th Cir. 1995) (federal sovereign immunity).

NSO's reliance (Br. 29-30) on *Del Campo v. Kennedy*, 517 F.3d 1070 (9th Cir. 2008), which did not involve a conduct-based immunity claim at all, is even further afield. There, a company that contracted with a California county claimed it was "entitled to [Eleventh Amendment] state sovereign immunity" because it acted "as an arm of the state." 517 F.3d at 1074-75. Because the contractor in *Del Campo* sought to invoke Eleventh Amendment immunity—an established immunity from suit grounded in an "explicit … constitutional guarantee," *Midland Asphalt*, 489 U.S. at 801—it could obtain

interlocutory review. *Del Campo*, 517 F.3d at 1074-75. Here, by contrast, NSO asserts only a defense to liability, so *Del Campo* is irrelevant.[7]

Because the district court's order denying NSO conduct-based immunity is not subject to interlocutory review, this Court lacks jurisdiction, and NSO's appeal should be dismissed.

II. NSO Is Ineligible For Common-Law Conduct-Based Immunity Because It Is A Private Corporate Entity, Not A Natural Person

If the Court were to reach the merits, it should hold that NSO is not entitled to conduct-based immunity. NSO's motion to dismiss argued only that NSO was "entitled to derivative sovereign immunity under *Butters*." ECF 45, at 10. Changing tack on appeal, NSO now seeks common-law "conduct-based immunity" because it supposedly "is being sued for acts it took in its capacity as an agent" of foreign sovereigns. Br. 30. NSO's repackaged immunity claim fares no better.

NSO fails to identify a single authority applying common-law conduct-based immunity to a private company. Rather, that doctrine is, and always has been, limited to natural persons. Because no existing authority supports

[7] The remaining case law that NSO cites is inapt, not authoritative, or unreasoned. *See* Dkt. 13-1, at 15-16; Dkt. 15, at 6-8.

its argument, NSO must ask this Court for a dramatic expansion of common-law immunity.

This Court cannot expand the common law to reach private companies like NSO because doing so would contravene the political branches' judgment, as embodied in the FSIA and longstanding Executive Branch practice. NSO has conceded that it lacks immunity under the FSIA—the sole statute in which Congress addressed sovereign immunity for corporate entities. This Court cannot circumvent Congress's judgment by fashioning a novel common law rule that contradicts the FSIA's delineation of which corporations may obtain immunity. But even if the Court had that authority, policy interests preclude such an expansion. Expanding common-law immunity to cover NSO would license unlawful conduct by any private corporation that submitted a self-serving and unverified declaration asserting that its conduct benefited a foreign government. This Court should not endorse that new and dangerous regime.

A. Common-Law Conduct-Based Immunity Applies Only To Natural Persons, Not Artificial Entities

NSO's reliance on "[t]he same common-law doctrine that protects foreign officials," Br. 3, is wholly misplaced. Contrary to NSO's claims, an unbroken consensus of judicial precedent, legal treatises, and Executive Branch practice establishes that the doctrine applies to only natural persons.

The common law recognizes two forms of official immunity, neither of which applies to artificial entities. First, certain foreign officials have immunity because of their status, such heads of state and diplomats. *See Samantar*, 560 U.S. at 319 n.12; *Doğan*, 932 F.3d at 893. Second, conduct-based immunity can arise from certain "acts performed in [a defendant's] official capacity." *Id.* at 893-94.

NSO does not and cannot claim status-based immunity because a private company obviously cannot be a head of state or diplomatic envoy. Instead, NSO seeks conduct-based immunity as a purported "agent of a foreign sovereign." Br. 30. But conduct-based immunity, too, applies only to natural persons. No authority has *ever* recognized conduct-based immunity for a corporate contractor like NSO.

Judicial Precedent: Both this Court and the Supreme Court have contemplated only that conduct-based immunity may "extend[] to *individual* foreign officials." *Doğan*, 932 F.3d at 893 (emphasis added); *see Samantar*, 560 U.S. at 321 (referring to "the immunity of individual officials"). That is because the doctrine shields officials and agents from liability for acts taken "as the 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). Only natural persons—not private companies—act as governmental "representatives" and serve "in office."

For its part, NSO cannot identify a single case supporting its position that conduct-based immunity can apply to corporations. The vast majority of NSO's cited authorities instead involve current or former foreign government *officials*, who of course were natural persons: that is true of

NSO's pre *Samantar* cases,[8] post-*Samantar* cases,[9] and foreign cases.[10] To the extent these authorities use the term "agent," they do so interchangeably and synonymously with "official."[11] Even in the handful of cases involving

---

[8] *See 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"); *Underhill v. Hernandez*, 168 U.S. 250, 252 (1897) (Venezuelan general); *Greenspan v. Crosbie*, 1976 WL 841, at *1-2 (S.D.N.Y. 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").

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

[10] *See Jones v. Ministry of Interior*, UKHL 26 (House of Lords, U.K. 2006) ("Lieutenant Colonel" of Saudi Arabia); *Jaffe v. Miller*, 95 ILR 446, 460 (Ontario Ct. App., Canada 1993) (Florida state officials); *Church of Scientology Case*, 65 ILR 193, 198 (Fed. Supreme Ct., Germany 1978) (head of London police force).

[11] *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 activity exception may be

agents who were not formally government officials, the agents were still natural persons—not artificial entities.[12]

The *only* case NSO cites involving an artificial-entity agent is the Fourth Circuit's now-abrogated decision in *Butters*. But *Butters* did not even mention the doctrine of conduct-based immunity. Instead, *Butters* applied what it called "derivative immunity under the FSIA," 225 F.3d at 466, to immunize a foreign government's private agent. After *Samantar*, that analysis and holding are no longer good law. *See infra* at 39-45.

Legal Treatises: The Restatement (Second) of Foreign Relations Law confirms that conduct-based immunity applies only to natural persons.[13]

---

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").

[12] *See Ivey for Carolina Golf Dev. Co. v. Lynch*, 2018 WL 3764264, at *7 (M.D.N.C. 2018) (attorney appointed by German official to administer insolvency proceedings); *Mireskandari v. Mayne*, 2016 WL 1165896, at *3 (C.D. Cal. 2016) (investigators for organ of foreign state); *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 (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").

[13] This Court has previously used the Restatement as a guide in analyzing official immunity, *Doğan*, 932 F.3d at 893-94, and it can play a similar role

Section 66 addresses when foreign sovereign immunity may extend beyond "the state itself." Restatement § 66(a). It first says that only "corporation[s] created under [a state's laws] and exercising functions comparable to those of an agency of the state" may claim immunity. *Id.* § 66(g). It then provides that individual foreign officials may claim immunity based on their status as "head of state" or "foreign minister," or where "any other public minister, official, or agent of the state" performs acts "in his official capacity if the effect of exercising jurisdiction would be to enforce a rule of law against the state." *Id.* §§ 66(b), (e), (f).

Contrary to NSO's argument, the Restatement's use of the phrase "agent of the state" clearly encompasses only natural persons. The term "agent" follows the terms "public minister" and "official," which refer to natural persons. *Id.* § 66(f); *see Samantar*, 560 U.S. at 317 ("[A] word may be known by the company it keeps"). The provision also speaks of "acts performed in *his* official capacity," which only makes sense in reference to natural persons. Restatement § 66(f) (emphasis added). The Restatement's "Illustrations" of conduct-based immunity both describe incidents involving

---

here whether or not it fully captures the common law of foreign-official immunity. *See Samantar*, 560 U.S. at 321 n.15 (reserving this question). Indeed, many of NSO's favored authorities rely on the Restatement. *See, e.g.*, *Rishikof*, 70 F. Supp. 3d at 12; U.S. Statement of Interest, *Matar v. Dichter*, 05-cv-10270, at 8 (S.D.N.Y. 2006).

natural persons. *Id.* Illustrations 2-3. And the obvious exclusion of corporations from the category "agents" is reinforced by the Restatement's separate provision addressing criteria for immunity of certain state-owned corporations—criteria that do not apply to NSO. This provision would make little sense if corporations that fail to satisfy its strictures could instead claim immunity as foreign "agents." *See id.* § 66(g).

Executive Branch Practice: Executive Branch practice—critical to assessing claims of common-law sovereign immunity—confirms that conduct-based immunity is limited to natural persons. Because foreign sovereign immunity is not a constitutional command but "'a matter of grace and comity on the part of the United States," courts "defe[r] to the decisions of the political branches" about whether immunity applies in a given case. *Verlinden B.V. v. Cent. Bank of Nigeria*, 461 U.S. 480, 486 (1983). Even when the political branches have made no such decision, "[t]he court grants immunity … if it determines that 'the ground of immunity is one which it is the established policy of the [State Department] to recognize.'" *Doğan*, 932 F.3d at 893. 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).

NSO offers no example of the Executive Branch recognizing or recommending conduct-based immunity for an artificial entity. Its cited Executive Branch sources solely discuss conduct-based immunity for natural persons.[14]

NSO's failure to cite any Executive Branch authority advocating conduct-based immunity for an artificial entity was not some oversight. To the contrary, a review of State Department sovereign-immunity decisions reveals not a single instance in which the Department requested immunity for a private corporation acting as a foreign state's agent. For example, a collection of decisions from 1952 to 1977—the period between the Department's adoption of the modern "restrictive theory" of immunity and the FSIA's enactment—features "only four decisions related to official

[14] *See* U.S. Amicus Br., *Mutond v. Lewis*, 2020 WL 2866592, at *16 (May 2020) (emphasizing that "the Executive has 'sometimes suggested immunity under the common law for individual officials even when the foreign state did not qualify"); U.S. Amicus Br., *Samantar v. Yousuf*, 2010 WL 342031, at *6 (Jan. 2010) (arguing that the common law governs "the immunity of individual foreign officials"); U.S. Statement of Interest, *Matar*, at 4 ("individual foreign officials have long been recognized to hold immunity … with respect to their official acts"); 1 Op. Att'y Gen. 81 (1797) (recognizing immunity of individual British official); 1 Op. Att'y Gen. 45, 46 (1794) (recognizing immunity of governor of a French island).

immunity," *Samantar*, 560 U.S. at 323 n.18, none of which requested immunity for any artificial entity, *see* Sovereign Immunity Decisions of the Dept. of State, May 1952 to Jan. 1977 (M. Sandler, D. Vagts, & B. Ristau eds.), in Digest of U.S. Practice in International Law 1977, at 1020-1081 ("1977 Digest"). A collection of U.S. practice from 1991-1999 likewise offers no evidence that the Executive Branch ever suggested immunity for a private company like NSO. *See* Digest of U.S. Practice in International Law 1991-1999, at 1183-1339 (S. Cummins & D. Stewart eds.) ("1999 Digest").

These collections instead confirm that the Executive Branch has recommended immunity for an artificial entity only where the entity was an organ of, or owned by, a foreign state—the same immunity rule for state-affiliated entities now codified in the FSIA, 28 U.S.C. § 1603, which NSO concedes it cannot meet. *See, e.g.*, 1977 Digest, at 1047 (addressing immunity request for a maritime vessel owned by the Cuban Government); *id.* at 1048 (addressing immunity request for an "entity created by the Government of Venezuela"). Correspondingly, the Executive Branch has recommended immunity for a foreign official or agent only when the defendant was a natural person. *See, e.g.*, *id.* at 1053-54 (recognizing immunity for head of state of Saudi Arabia); 1999 Digest, at 1266 (suggesting immunity for President of Haiti).

Recent State Department practice is of a piece, suggesting common-law foreign-official immunity only for natural persons. *See* Digest of U.S. Practice in International Law 2019, Head of State and Other Foreign Official Immunity, at 333-345 (C. Guymon ed.); *id.* at 338 (suggesting immunity for Israeli Defense Minister); *id.*, at 342 (suggesting immunity for French Foreign Minister); Digest of U.S. Practice in International Law 2018, Head of State and Other Foreign Official Immunity, at 410-13 (C. Guymon ed.) (suggesting immunity for then-president of the Democratic Republic of the Congo). NSO's claim of conduct-based corporate immunity is thus devoid of support from Executive Branch authority—or any authority for that matter.

B. This Court Should Not Expand Common-Law Conduct-Based Immunity To This Novel Context

Because no recognized basis exists for the immunity it claims, NSO must ask this Court to fashion a novel form of common-law immunity that would protect the conduct of a corporate "agent" simply because its products or services are eventually used by unidentified foreign sovereigns. But the Judiciary lacks power to fashion novel common-law rules on subjects that Congress has addressed, as Congress did with foreign sovereign immunity in the FSIA. There, Congress expressly defined the circumstances in which corporations may obtain sovereign immunity—requirements that NSO plainly, and concededly, fails to satisfy. Accordingly, this Court cannot

entertain NSO's attempt to escape the FSIA through newly created common law. Even if courts had such common-lawmaking authority, separation-of-powers principles and policy concerns would preclude an unprecedented expansion of common-law foreign-official immunity to cover private companies that sell goods or services used by foreign-state clients.

1. Courts Cannot Create A Common-Law Rule That Would Allow NSO To Circumvent Congress's Judgment In The FSIA

a. A long line of cases bars federal common-lawmaking on subjects that Congress has addressed. "Judicial lawmaking in the form of federal common law plays a necessarily modest role under a Constitution that vests the federal government's 'legislative powers' in Congress." *Rodriguez v. Fed. Deposit Ins. Corp.*, 140 S. Ct. 713, 717 (2020). Because "[f]ederal common law is subject to the paramount authority of Congress," courts may only "resort[] to [it] in the absence of an applicable Act of Congress." *City of Milwaukee v. Illinois & Michigan*, 451 U.S. 304, 313-14 (1981). "When Congress addresses a question[,] … the need for" the "unusual exercise of law-making by federal courts disappears." *Id.* at 314; *see, e.g.*, *Am. Elec. Power Co. v. Connecticut*, 564 U.S. 410, 424 (2011) (Clean Air Act "speaks directly to emissions of carbon dioxide from the defendants' plants" and thus "displace[s] any federal common-law right" on the subject).

Common-lawmaking authority is especially circumscribed in the field of foreign affairs. "The political branches, not the Judiciary, have the responsibility and institutional capacity to weigh foreign-policy concerns." *Jesner v. Arab Bank, PLC*, 138 S. Ct. 1386, 1403 (2018). Courts therefore must "ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches." *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 116 (2013). And "the danger of unwarranted interference in the conduct of foreign policy is magnified" where "the question is not what Congress has done but instead what courts may do." *Id.*

b. In the FSIA, Congress established the sole circumstances under which artificial entities may obtain foreign sovereign immunity. That express congressional delineation precludes NSO's proposed novel common-law rule of corporate immunity.

The FSIA directly addresses when a "separate legal person, corporate or otherwise" may invoke foreign sovereign immunity. 28 U.S.C. § 1603(b)(1). First, an entity may be immune if it is "an organ of a foreign state or political subdivision thereof." *Id.* § 1603(b)(2). Second, an entity may be immune if "a majority of [its] shares or other ownership interest is owned by a foreign state or political subdivision thereof." 28 U.S.C. §

1603(b)(2). NSO admits that it satisfies neither of these prerequisites and is not entitled to FSIA immunity. *See* ER9.

The FSIA establishes the "*comprehensive* … set of legal standards governing claims of immunity in every civil action against a foreign state or its political subdivisions, agencies, or instrumentalities." *Republic of Austria v. Altmann*, 541 U.S. 677, 691 (2004) (emphasis added). "The key word there—which goes a long way toward deciding this case—is *comprehensive*." *Republic of Argentina v. NML Capital, Ltd.*, 573 U.S. 134, 141 (2014). The Supreme Court has "used that term often and advisedly to describe the Act's sweep." *Id.* (citing cases). Accordingly, immunity claims must "stand on the Act's text"—and where, as here, they cannot, they "must fall." *Id.* at 142.

The Supreme Court's decision in *Dole Food Co. v. Patrickson*, 538 U.S. 468 (2003), proves the point. There, two companies that were "indirect subsidiaries of the State of Israel" sought FSIA immunity. *Id.* at 473-74. The Court rejected their immunity claims, holding that they could not satisfy the FSIA's definition of "instrumentality of a foreign state," since Israel did not directly own "a majority of [their] shares." *Id.* at 474. It made no difference, the Court reasoned, "that the State of Israel exercised considerable control over [the companies'] operations." *Id.* at 477. The FSIA's terms "are explicit

and straightforward," and recognizing the defendants' immunity claim "would render [those terms] superfluous." *Id.* at 477.

The FSIA's explicit terms similarly preclude common-law corporate-agent immunity here. Just as the companies in *Dole* could not circumvent the FSIA's requirements for state-affiliated corporations by claiming that Israel exercised control over them, NSO cannot do so by claiming that it acts as an agent for (unidentified) foreign sovereigns. Neither "control" nor "agency" principles are criteria in the FSIA's text for recognizing artificial-entity immunity—and that text, as noted, is "*comprehensive*." *NML Capital*, 573 U.S. at 141. It would make no sense to "allow[] litigants to accomplish indirectly what the [FSIA] barred them from doing directly." *Chuidian*, 912 F.2d at 1102.

c. *Samantar* is fully consistent with this reasoning. There, the Court held only that common-law immunity for "individual officials"—*i.e.*, "*natural persons*"—survived the FSIA. *Samantar*, 560 U.S. at 315-16 (emphasis added). And it did so after concluding that "[t]he immunity of officials simply was not the particular problem to which Congress was responding when it enacted the FSIA." *Id.* at 323. As the Court explained, Congress did not "inten[d] to include individual officials within" the Act's provisions. *Id.* at 316. Because the FSIA does not address the immunity

available to "natural persons" at all, *id.*, "there is [a] gap for the federal common law" of foreign-official immunity "to fill." *Native Vill. of Kivalina v. ExxonMobil Corp.*, 696 F.3d 849, 856 (9th Cir. 2012).

By contrast, the FSIA *does* address the immunity available for corporations and other artificial "entit[ies]." *Samantar*, 560 U.S. at 315. Indeed, Congress specifically adopted the FSIA "to address 'a modern world where foreign state *enterprises* are every day participants in commercial activities." *Id.* at 323 (emphasis added). In framing the FSIA's terms, Congress carefully defined the limits on entity-based immunity. *See Dole Food*, 538 U.S. at 478. The FSIA therefore "addresse[d] [the] question" of when corporations may obtain foreign sovereign immunity, and it bars any statutory immunity claim by NSO. *City of Milwaukee*, 451 U.S. at 314.

Thus, unlike with the immunity claims of individual foreign officials, "legislative action has displaced the common law," and "there is no gap for federal common law to fill." *Native Vill. of Kivalina*, 696 F.3d at 856; *see* Ingrid Wuerth, *Foreign Official Immunity Determinations in U.S. Courts: The Case Against the State Department*, 51 Va. J. Int'l L. 915, 968 (2011) (the FSIA "constrains the courts' development of federal common law"). When it comes to judicial lawmaking, "[t]here is a basic difference between filling a gap left by Congress' silence and rewriting rules that Congress has

affirmatively and specifically enacted." *Mobil Oil Corp. v. Higginbotham*, 436 U.S. 618, 625 (1978). NSO's request would impermissibly rewrite the FSIA's rules for corporate immunity. Indeed, it would seemingly bestow immunity on corporate contractors even if the FSIA's exceptions to immunity for state-owned corporations would not apply. *See* 28 U.S.C. § 1605 (listing exceptions). And Congress's judgment in the FSIA to limit when foreign corporations can assert immunity deserves special weight because of the "foreign policy consequences" attached to sovereign-immunity determinations. *Kiobel*, 569 U.S. at 116. The Court thus lacks authority to second-guess Congress's considered judgment.

2. *Butters* Does Not Support NSO's Conduct-Based Immunity Claim

The only decision NSO cites that afforded immunity to an artificial entity—the Fourth Circuit's decision in *Butters*—does not support NSO's conduct-based immunity claim. *Butters* granted immunity to a contractor acting on a foreign state's behalf under a theory entirely distinct from NSO's version of conduct-based immunity: "derivative immunity under the FSIA." 225 F.3d at 466. The Supreme Court's decision in *Samantar*, limiting FSIA immunity to the FSIA's terms, abrogates *Butters*. In any event, *Butters*' reasoning from analogy to *domestic* contractors is unsound. And NSO's

attempt to repackage *Butters* as a conduct-based immunity case is irreconcilable with *Butters*' own analysis.

a. *Butters* erroneously held that an immunity defense afforded to contractors working for the federal government, *see Campbell-Ewald Co. v. Gomez*, 577 U.S. 153, 166 (2016), should extend to contractors working for foreign governments. There, Saudi Arabia hired a U.S. company to perform security services for a member of the royal family. *Butters*, 225 F.3d at 464. When an employee of the company sued for gender discrimination, the Fourth Circuit held that the FSIA immunized the company because it had performed the acts in question on a foreign government's behalf. *Id.* at 464-65. According to the court, although the company was neither a foreign state nor an agency or instrumentality of a foreign state as defined by the FSIA, the company was nevertheless "entitled to derivative immunity under the FSIA." *Id.* at 466. Citing case law holding "that contractors and common law agents acting within the scope of their employment for the United States have derivative sovereign immunity," the Fourth Circuit believed that it was "but a small step to extend this privilege to the private agents of foreign governments." *Id.*

Samantar repudiates *Butters*' holding. *Samantar* makes clear 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. at 313. It thus precludes the possibility of implied *derivative* immunity under the FSIA, as contemplated by *Butters*. Because the concept of derivative sovereign immunity lacks grounding in the FSIA's text, *Butters* is no longer good law.

b. The remainder of *Butters*' reasoning is no more defensible. No other court of appeals, before or after *Butters*, has endorsed its theory of derivative foreign sovereign immunity, and no court has applied *Butters* to shield an artificial entity. That lack of support is unsurprising: the rationale underlying the federal-contractor defense *Butters* relied on does not extend to contractors for foreign governments.

Domestic "derivative sovereign immunity" reflects that the United States and its agents have "the same interest in getting the Government's work done." *Boyle v. United Techs. Corp.*, 487 U.S. 500, 505 (1988). In that context, federal courts have created a common-law rule to protect unique federal interests. *Id.* at 504-05. "The United States does not," however, "share an interest with the agents of a foreign sovereign, and those interests will routinely diverge, as they do in this case." *Broidy Cap. Mgmt. LLC v. Muzin*, 2020 WL 1536350, at *7 (D.D.C. 2020). As a result, the "step" from

the domestic federal context to the foreign context is hardly "small." *Butters*, 225 F.3d at 466.

Courts' refusal to extend the federal-contractor defense to state contractors underscores the point. Even though a state's sovereign immunity is embedded in "our constitutional design," *Franchise Tax Bd. of Cal. v. Hyatt*, 139 S. Ct. 1485, 1492 (2019), "[n]either the Supreme Court nor the Ninth Circuit nor any other court … has applied the defense" available to federal contractors "to state contractors," *United States ex rel. Ali v. Daniel, Mann, Johnson & Mendenhall*, 355 F.3d 1140, 1147 (9th Cir. 2004). NSO's suggestion that federal courts create a common-law rule protecting foreign-government contractors—even when domestic-state contractors lack such protection—is therefore untenable.

c. Apparently conceding that derivative foreign sovereign immunity does not exist, NSO disavows *Butters*' actual reasoning. *See* Br. 42 (referring to "So-Called 'Derivative Sovereign Immunity'"). Instead, NSO attempts to recast *Butters* as "consistent with the common law" of foreign-official immunity, Br. 11, and even claims that *Butters*' theory of derivative foreign sovereign immunity is "merely another name for conduct-based immunity," *id.* at 43. That effort fails for four reasons. *See* ER11 n.1 (holding that NSO

cannot use *Butters* to "merg[e] two distinct doctrines, foreign official immunity and derivative sovereign immunity").

First, *Butters* neither mentioned conduct-based immunity, nor performed any of the analysis required to recognize a conduct-based immunity claim, such as determining whether the immunity sought aligned with the "established policy of the [State Department]." *Samantar*, 560 U.S. at 312.

Second, NSO's contention (Br. 43) that *Butters*' reasoning did not depend on its "analogy" to the federal-contractor defense is irreconcilable with the court's opinion. Not only did *Butters* extensively discuss the seminal federal-contractor decision, *Yearsley v. W.A. Ross Constr. Co.*, 309 U.S. 18 (1940), as well as additional federal-contractor cases, *see Mangold v. Analytic Servs., Inc.*, 77 F.3d 1442 (4th Cir. 1996), but it expressly stated that its holding would "*extend*" the immunity available to federal contractors to "the private agents of foreign governments," *Butters*, 225 F.3d at 466 (emphasis added).

Third, contrary to NSO's submission (Br. 43), *Butters*' citation of *Alicog v. Kingdom of Saudi Arabia*, 860 F. Supp. 379 (S.D. Tex. 1994), does not suggest that *Butters* grounded its reasoning in conduct-based immunity. In *Alicog*, a district court held that American citizens—not artificial entities—

working on Saudi Arabia's behalf were immune as "agents of the Saudi government." *Id.* at 384. But *Alicog* "stated that its decision as to the American defendants' immunity was made '*under Texas law*'" and did not even purport to apply "the common law of foreign-official immunity." *Broidy*, 2020 WL 1536350, at *7 (quoting *Alicog*, 860 F. Supp. at 381).

Finally, the derivative immunity recognized in *Butters* cannot be "identical" to conduct-based immunity because the two immunities have different doctrinal requirements. Br. 45. The federal-contractor defense that *Butters* extended does not shield a contractor who violates "federal law and the Government's explicit instructions." *Campbell-Ewald*, 577 U.S. at 166. That is why this Court has concluded that the defense protects federal contractors only "from *state tort liability*." *Ali*, 355 F.3d at 1147 (emphasis added).

Conduct-based immunity, by contrast, shields a foreign official or agent from liability *irrespective* of whether she has violated federal law. *See, e.g., Doğan*, 932 F.3d at 889-90 (holding that conduct-based immunity precluded liability under the federal TVPA). That difference matters here: WhatsApp alleges that NSO violated the federal CFAA, so even if the contractor defense were available to contractors for foreign states, it would not shield NSO from liability in this case. *See* ER71-72 ¶¶ 49-57; ER35-40

(denying NSO's motion to dismiss WhatsApp's CFAA claim). This presumably explains NSO's effort to transmute *Butters*' derivative-immunity analysis into the conduct-based immunity that can protect against federal-law claims. But because the federal-contractor defense and conduct-based immunity offer divergent protections, the former cannot be "merely another name for conduct-based immunity." Br. 43.

3. Policy Interests Counsel Against NSO's Proposed Expansion Of Common-Law Conduct-Based Immunity.

Lacking support in case law, statutory text, or Executive Branch practice, NSO resorts to policy arguments. NSO contends that foreign sovereigns' interests in "crime prevention and national security" justify applying conduct-based immunity to corporations acting on their behalf. Br. 48-50. But foreign-policy judgments are the province of the political branches, not the courts. And in any event, foreign-policy considerations cut *against* NSO's claimed immunity here.

a. As explained above, the political branches—not courts—bear responsibility for determining foreign policy. *See supra* at 30-31. This remains true even when the policy stakes are high. In *NML Capital*, for example, both Argentina and the United States urged the Supreme Court to consider the "worrisome international-relations consequences" that would

flow from the failure to grant foreign sovereigns an immunity not present in the FSIA's text. 573 U.S. at 146. These consequences included the danger of a "substantial invasion of foreign states' sovereignty," a blow to "international comity," the potential for "reciprocal adverse treatment of the United States in foreign courts," and "harm to the United States' foreign relations more generally." *Id.* Yet the Court rebuffed the parties' invitation to consider these policy consequences: such "apprehensions," the Court made clear, "are better directed to that branch of government with authority to amend the [FSIA]." *Id.*

Precisely because courts lack authority to freelance on foreign affairs, they look to the State Department's recommendations and "established policy" when deciding whether to validate claims of common-law immunity. *See Doğan*, 932 F.3d at 893. That deferential practice reflects an abiding concern that "the courts should not so act as to embarrass the executive arm in its conduct of foreign affairs." *Hoffman*, 324 U.S. at 35. While NSO points to hypothetical consequences of a failure to grant private corporations immunity, "recognition by the courts of an immunity upon principles which the political department of government has not sanctioned may be equally embarrassing to it in securing the protection of our national interests and their recognition by other nations." *Id.* at 36.

This case is a particularly poor candidate for judicial policymaking. Even though private companies have long contracted with foreign governments, NSO can point to no instance where the political branches have granted immunity to such a company. *See supra* at 31-33. And the limited pre-discovery factual record—consisting of a self-serving NSO declaration (ER51-56) and a contract showing that NSO does *not* solely contract with foreign governments (ER143-49)—provides further ground for judicial caution.

b. 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. The balance Congress struck in the FSIA—extending immunity only to state instrumentalities, but not private corporations selling their services to foreign governments—is sound.

First, the "[c]omity and dignity interests" that animate sovereign immunity for foreign states and their instrumentalities are absent for private contractors—who need not be foreign officials, or even governmental employees. *Pimentel*, 553 U.S. at 866. As the United States itself has recognized, "government contractors lack sovereign dignitary interests"—even when they perform work on a sovereign's behalf. U.S. Amicus Br., *CACI*

Premier Tech., Inc. v. Al Shimari, No. 19-648, at 13 n.3 (Aug. 2020). This reality explains why there is "no authority for the notion that private persons performing Government work acquire the Government's embracive immunity." *Campbell-Ewald*, 577 U.S. at 166. And it explains why this Court has refused to extend the immunity afforded to American states "to private parties whose only relationship to the sovereign is by a contract." *Del Campo*, 517 F.3d at 1076.

Second, granting immunity to private businesses whose products are ultimately used by a foreign sovereign would create an unacceptable risk of unsanctioned conduct. Unlike with state-affiliated entities and officials, sovereigns will often be unable to supervise and regulate the actions of independent private entities.[15] And a private company's profit motive will inevitably mean that its incentives conflict with those of its public clients. As the U.N. General Assembly recently observed, for instance, states "must be particularly vigilant" when relying on services from "private commercial

[15] *See* U.S. Senate Committee on Armed Services, *Inquiry Into the Role and Oversight of Private Security Contractors in Afghanistan* (Sept. 28, 2010) (inadequate government supervision of military contractors led to "dangerous failures" and "funneling [of] U.S. taxpayer[] dollars to Afghan warlords and strongmen linked to murder, kidnapping, [and] bribery"), https://fas.org/irp/congress/2010_rpt/sasc-psc.pdf.

actors that are motivated primarily by profit, fostering situations in which human rights are subordinated to goals of efficiency."[16]

These risks are particularly acute for multinational businesses—like NSO—that sell their services to *multiple* foreign clients (as well as private resellers, *see* ER143-49). When a state or state-run entity violates the law, aggrieved parties know where to seek political (if not judicial) redress: from the state itself. But when a multinational business serving multiple clients does the same, "[i]t is often unclear how, when, where, and which authorities are responsible for investigating, prosecuting, and punishing such crimes."[17] Because commercial contractors such as NSO will otherwise fall into a regulatory void, U.S. courts must provide a forum for the victims harmed by these contractors to hold them accountable.[18]

---

[16] U.N. Gen. Assembly, Human Rights Council, *Impact of the Use of Private Military and Security Services in Immigration and Border Management on the Protection of the Rights of All Migrants*, at 17 (July 9, 2020), https://undocs.org/A/HRC/45/9.

[17] Peter Singer, *Outsourcing War*, Brookings Institution (Mar. 1, 2005), (detailing the "unregulated nature" of the global military-contractor industry), https://www.brookings.edu/articles/outsourcing-war/.

[18] *See* U.N. Gen. Assembly, *Report of the Open-Ended Intergovernmental Working Group*, at 3 (Dec. 24, 2010), (describing "human rights challenges brought about by the increase in the outsourcing of security-related State functions to private companies, particularly given that such companies frequently operate transnationally"),

Third, transparency interests require denying immunity to private companies. States may contract with private entities precisely because they want the additional secrecy that comes from accomplishing objectives through an independent actor whose conduct cannot be easily traced back to a sovereign.[19] This case illustrates the point: the roster of NSO's sovereign clients remains shrouded—indeed, NSO sometimes operates through resellers, further distancing it from sovereign governments, ER143-49—even as NSO claims that its sovereign-client relationships require this Court to grant it immunity. To promote transparency in international affairs, immunity doctrine should shield only actions undertaken by a state or its organs or owned enterprises—not actions laundered through a private entity like NSO.

Fourth, granting immunity to NSO would exacerbate the troubling trend of governments unduly relying on private companies. Our

---

https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session22/AHRC2241_English.pdf.

[19] *See* Sean McFate, Mercenaries and War: Understanding Private Armies Today, National Defense University Press, at 24 (Dec. 2019) ("One attraction is the industry's covert nature. When the you want to keep a secret, sometimes the private sector is murkier than government agencies."), https://ndupress.ndu.edu/Portals/68/Documents/strat-monograph/mercenaries-and-war.pdf.

international system has long entrusted states with responsibilities and powers that private actors cannot and should not share.[20] Yet recent decades have seen a proliferation of private contractors performing tasks like raising armies, conducting intelligence, and even making war. *See Broidy Cap. Mgmt., LLC v. State of Qatar*, 2020 WL 7051945, at *7 (9th Cir. Dec. 2, 2020) (noting "that there are bad actors in the commercial sphere who" conduct "clandestine surveillance and espionage"). Scholars and international organizations have warned of the dangers posed by this trend.[21] Granting NSO immunity here would be a boon to the marketplace for private actors with sweeping powers and little transparency. This Court should not be the first to go down that path—especially in the face of contrary congressional and executive will.

---

[20] *See* U.N. Gen. Assembly, *Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, at 4 (Aug. 25, 2010) (affirming the existence of "inherently state functions" that should "not under any circumstances be outsourced"), https://undocs.org/A/65/325.

[21] *See, e.g.*, Raenette Taljaard, *Private military companies: The danger of latter-day mercenaries*, International Herald Tribune (Jan. 17, 2004), ("the nation-state is losing its jealously guarded monopoly on the use of force," "pos[ing] a serious threat to international peace and security"), https://www.nytimes.com/2004/01/17/opinion/private-military-companies-the-danger-of-latterday-mercenaries.html.

III. Even If Corporations Could Ever Be Eligible For Common-Law Conduct-Based Immunity, NSO Could Not Satisfy That Doctrine's Requirements

As just explained, corporate entities can never obtain common-law conduct-based immunity. But even if corporations could be *eligible* for conduct-based immunity, NSO would not be *entitled* to that immunity here. Neither the State Department nor any foreign government has requested immunity for NSO. And NSO premises its immunity claim on its CEO's threadbare declaration that unidentified foreign governments use NSO's spyware. That showing—called into question by other evidence showing that NSO also contracts with *private* entities—comes nowhere close to meeting conduct-based immunity's established doctrinal requirements.

A "two-step procedure" applies "when a foreign official" or agent "assert[s] immunity." *Samantar*, 560 U.S. at 312. 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 not suggested that NSO is immune. ER11. So if analysis were to proceed on

NSO's flawed theory, the Court would have to decide for itself whether immunity may attach.

In making that determination, the Court must ask whether "the ground of immunity is one which it is the established policy of the [State Department] to recognize." *Doğan*, 932 F.3d at 893. The Supreme Court has suggested that the State Department's test for immunity provides the exclusive grounds for analyzing whether conduct-based foreign-official immunity protects a defendant. *See Samantar*, 560 U.S. at 312 (noting that pre-FSIA courts applied this test) (citing *Hoffman*, 324 U.S. at 36); *see also Broidy*, 2020 WL 1536350, at *6-8 (applying this test). If the State Department's test must be satisfied before a court grants immunity, then NSO clearly cannot qualify: as already explained, NSO identifies no State Department guidance recognizing immunity for foreign-government contractors. *See supra* at 30-33.

The same result obtains if this Court follows the analysis in *Doğan*, which stated that "[c]ommon-law foreign sovereign immunity extends to individual foreign officials for [1] 'acts performed in [a foreign agent's] official capacity" if [2] "the effect of exercising jurisdiction would be to enforce a rule of law against the state.'" 932 F.3d at 893-94. While NSO admits that it must satisfy the first precondition—*i.e.*, its relevant conduct

must have been performed in an "official capacity," Br. 30-31—it disputes that it must satisfy the second. NSO loses on the first precondition alone: NSO did not engage in the conduct exposing it to liability exclusively or even primarily when acting in an "official capacity" for foreign sovereigns. But regardless, the second precondition is valid, and NSO cannot meet it either.[22]

A. NSO Did Not Act In An Official Capacity

1. When a foreign official or agent asserts conduct-based immunity, the ultimate question is whether the relevant suit "is merely a disguised action against the nation that [the defendant] represents." *Park v. Shin*, 313 F.3d 1138, 1144 (9th Cir. 2002).[23] If the suit challenges actions the defendant has taken in an official governmental capacity, then it is more likely to be treated as "the practical equivalent of a suit against the sovereign directly," and thus barred. *Chuidian*, 912 F.2d at 1101. That result aligns with "the

[22] As noted earlier, the district court rejected not only NSO's claim to conduct-based immunity, but also any claim to so-called "derivative sovereign immunity," as articulated by *Butters*. ER9, 14-15. On appeal, NSO has expressly waived independent reliance on derivative sovereign immunity, instead characterizing it as "merely another name for conduct-based immunity." Br. 42-43.

[23] Many of the Ninth Circuit decisions discussed in this section arose under the FSIA because, pre-*Samantar*, this Circuit analyzed foreign-official immunity issues under the FSIA rather than the common law. Such decisions nonetheless remain persuasive authority because they applied the same "official capacity" test as applies under the common law. *Cf. Doğan*, 932 F.3d at 896 (citing pre-*Samantar* decision as persuasive).

'restrictive' principle of sovereign immunity" (codified in the FSIA), "which limits the immunity of a foreign state to its inherently governmental or public acts." *In re Estate of Marcos*, 25 F.3d at 1472.

Correspondingly, immunity does *not* attach when a defendant acts outside the scope of any official capacity. "Obviously," if the defendant "act[s] as an individual and not as an official, a suit directed against that action is not a suit against the sovereign." *Chuidian*, 912 F.2d at 1106. Such a suit "does not implicate any of the foreign diplomatic concerns involved in bringing suit against another government in United States courts." *In re Estate of Marcos*, 25 F.3d at 1472. Nor does it "have the effect of interfering with the sovereignty of the foreign state that employs the [defendant]." *Park*, 313 F.3d at 1144.

To determine whether a defendant engaged in official conduct, the Court asks whether the defendant was "acting exclusively or even primarily as an agent of [a foreign sovereign] when [it]" took the challenged actions. *Id.* A defendant engaged "in a private … venture" not in "public service of [a] government" lacks immunity. *Hoffman*, 324 U.S. at 33-34; *see El-Fadl v. Cent. Bank of Jordan*, 75 F.3d 668, 671 (D.C. Cir. 1996) (defendant's "personal []or private" activities would not be immune); *Lyders*, 32 F.2d at 309 (acts of officials "in connection with their private business" not

immune).[24] In *Park*, for instance, a Korean official stationed at the Consulate in San Francisco was sued by his domestic employee for acts arising out of her employment. 313 F.3d at 1140. The court held that the defendant was not "acting within the scope of his official duties" because "he hired [the plaintiff] as a personal family employee, paid her with family funds, and required her to perform work benefiting the Consulate only on a few days each month." *Id.* at 1144. For that reason, "an adverse judgment against [the] defendant would in no way interfere with the sovereignty or policy-making power of the Republic of Korea." *Id.*

2. In this case, NSO undertook its unlawful conduct as a for-profit company, not as a government agent. 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. *Contra Butters*, 225 F.3d at 464, 466 (immunity where foreign sovereign hired defendant to provide security to a government official, and defendant "was following [the sovereign's] orders" when acting unlawfully). Rather, NSO's spyware was its own brainchild: conceived, executed, marketed, and

[24] *See also* Digest of U.S. Practice in International Law 2015, at 426 (C. Guymon ed.) (no conduct-based immunity when "the conduct alleged was not taken in an official capacity, as might be the case in a suit challenging an official's purely private acts, such as personal financial dealings").

sold by NSO (or third-party resellers with whom NSO contracts). ER19. And NSO determined to set up the infrastructure for its spyware as a private commercial venture.

To begin, NSO engaged in much of the unlawful conduct at issue before it contracted with any foreign sovereign at all. On its own accord, NSO created false WhatsApp accounts and reverse-engineered the app, in violation of WhatsApp's terms of service. ER68-69 ¶¶ 30, 35. Using the information it gained from this attack, NSO independently developed spyware, tested it on WhatsApp systems, and marketed it to potential customers. ER 63-64 ¶ 5; ER69 ¶ 35. NSO does not argue that any foreign government commissioned or directed it to take these acts. *See* ER54-55 (NSO declaration). And these acts alone violated statutory and common-law prohibitions, *see* ER71-74 ¶¶ 49-78, and caused WhatsApp injury, *see* ER72-74 ¶¶ 57, 64-65, 71, 73, 78. Because these actions predated any foreign-sovereign involvement, NSO took them in a private, commercial capacity. *Contra* Br. 32.

Following its unlawful creation and marketing of the spyware, NSO sometimes sold it to private intermediaries that subsequently licensed it to foreign governments. ER143 (agreement between "Infraloks Development Limited" to "resell[] and supply[]" NSO spyware to the Republic of Ghana).

NSO therefore did not even necessarily contract *directly* with foreign governments at all.

Yet even assuming that NSO sometimes did so, simply contracting with a foreign government is not itself a "public" act. *Hoffman*, 324 U.S. at 33 (no immunity for "privately owned and operated Mexican corporation" engaged "in a private freighting venture" merely because it contracted with the Mexican government). As NSO admits, "selling [its] [spyware] technology" is its "*business* model." *See* ECF 45, at 6 (emphasis added). And even upon entering a licensing agreement, NSO takes independent actions without foreign-government direction: it alone, for instance, is "responsible for the system setup and training before its hand-over to the customer," ER137, and for maintaining the servers necessary to download and update spyware on targeted devices, ER67-68 ¶¶ 28, 32. Likewise, NSO monitors its customers' activities so that it can "suspend or terminate service to customers engaged in any improper use" of its spyware, ER54 ¶ 12—actions *contrary* to foreign governments' official interests.

Disregarding this large swath of private, commercial conduct, NSO asserts that all of its actions were "official" because unidentified "foreign state customers[]" subsequently "use[d] … its technology." Br. 32. But to determine whether NSO acted in an official capacity, the Court must look at

NSO's case-related conduct as a whole and ask whether NSO "act[ed] exclusively or even primarily as an agent of [foreign governments]." *Park*, 313 F.3d at 1144. Even assuming that some of NSO's private actions conferred a downstream "benefit[]" on a foreign government, that fact would not establish that NSO acted in an official capacity. *See id.* NSO's contention that an act is "official," so long as "it is not entirely unrelated to the official activities" of sovereign governments would create boundless immunity for any private contractor whose products are used by governments. Br. 33. No U.S. court has adopted that rule, leaving NSO to rely on a German Supreme Court decision that did not involve a government contractor at all. *See Church of Scientology Case*, 65 ILR at 195 (holding that head of New Scotland Yard was immune from suit to enjoin him from complying with a document request).

Even if there were ambiguity about whether NSO acted in an official capacity, that would not be a reason to grant NSO's motion to dismiss. Rather, in that scenario, a court must allow "jurisdictional discovery," giving the plaintiff "ample opportunity to secure and present evidence relevant to the existence of jurisdiction." *Phoenix Consulting Inc. v. Republic of Angola*, 216 F.3d 36, 40 (D.C. Cir. 2000); *accord Laub v. Dep't of Interior*, 342 F.3d 1080, 1093 (9th Cir. 2003). The district court noted that "the boundary

between [NSO's] conduct and [its] clients' conduct is not clearly delineated or definitively resolved." ER19. If so, then WhatsApp must be allowed discovery into which conduct was NSO's and whether it was private or public (again assuming that NSO could even possibly qualify for immunity despite its artificial-entity status).

NSO asserts that WhatsApp has not "contradicted" the declaration of NSO's CEO stating that NSO sells its products only to (unidentified) governments. Br. 31. But that is wrong: even without discovery, WhatsApp has shown that NSO sometimes sells its spyware to private re-sellers that later license it to governments. ER143-49. Regardless, even if NSO's vague declaration were true, it would show only that NSO makes money exclusively through government contracts; it would not establish that NSO committed its allegedly unlawful acts—including its design and marketing activities predating any contracts and conspiracy with its customers—in an official capacity. On that official-capacity issue, the declaration contains no specific facts "contradict[ing]" WhatsApp's allegations discussed above. *Mavrix Photo*, 647 F.3d at 1223. Because "factual disputes [are resolved] in the plaintiff's favor" on jurisdictional motions to dismiss, *id.*, WhatsApp's claims could proceed even under NSO's flawed immunity theory.

Indeed, dismissing the case based on NSO's vague declaration would create an exceedingly dangerous precedent. It would mean that any private company could avoid accountability for its unlawful acts simply by submitting a declaration stating that it undertook those acts as an "agent" of a foreign government—without even identifying that government or the terms of the company's agreement with it. And without discovery, a plaintiff would be unable to disprove the company's declaration. Allowing dismissal in this scenario would thus provide all government contractors with a blueprint to get meritorious claims against them thrown out of U.S. courts.

3. Finally, seeking to evade the official-capacity requirement altogether, NSO makes the conclusory assertion that its official-capacity status is "undisputed." Br. 32. But that assertion cannot be squared with NSO's subsequent acknowledgement that WhatsApp has "argued … that NSO cannot seek conduct-based immunity from claims based on its design and marketing of technology" because those were private actions. *Id.*; *see* ECF 116, at 9, 13-15; ECF 144, at 9-10. And while the district court did not adopt that argument, ER11, this Court has authority to reach a contrary conclusion—and should do so here because NSO's official-capacity claim is meritless.

B. A Judgment Against NSO Would Not Enforce A Rule Of Law Against A Foreign State

1. Even if a defendant acts in an official capacity, this Court's common-law conduct-based immunity test further requires that "the effect of exercising jurisdiction would be to enforce a rule of law against the state." Restatement § 66(f); *see Doğan*, 932 F.3d at 894 (applying this test). This test looks to the remedy the plaintiff seeks, in order to discern whether "the state is the real party in interest" in a suit against an official. *Samantar*, 560 U.S. at 325. As a general rule, when a plaintiff's suit does not seek "to draw on the [foreign state's] treasury or force the state to take specific action," the state is not a real party in interest and the suit may proceed. *Lewis*, 918 F.3d at 147; *accord* ER12. In *Lewis*, for instance, the plaintiff sued high-ranking foreign officials "in their individual capacities," not "seeking compensation out of state funds." 918 F.3d at 147. Because the suit would not lead to "direct fiscal impacts on the foreign state," the court held that conduct-based immunity could not attach. *Id.* That is the case here.

NSO relies heavily (Br. 8, 9, 33) on *Rishikof v. Mortada*, 70 F. Supp. 3d 8 (D.D.C. 2014), a case granting conduct-based immunity to a Swiss Embassy employee because the plaintiff sought "to hold the Swiss Confederation jointly and severally liable for [its agent's] actions." *Id.* at 15. But the court recognized that if the plaintiff "had not sued the Swiss

Confederation for joint and several liability," and "instead chose to proceed exclusively against [the individual agent], then [the agent] would not be entitled to immunity." *Id.*

2. NSO argues that WhatsApp's position would "*categorically* exclude[] individual capacit[y] suits from the scope of conduct-based immunity." Br. 34 (emphasis added); *see also* U.S. Amicus Br., *Lewis*, 2020 WL 2866592, at *8 (similar). That is incorrect. "[W]hen a suit *nominally* brought against an individual official would in fact involve adjudicating ownership of a foreign state's assets or granting a damages remedy directly against the treasury of a foreign state," immunity may attach. Professors Amicus Br., *Samantar*, 2010 WL 342033, at *22; *see Bradford v. Dir. Gen. of R.R.s of Mex.*, 278 S.W. 251 (Tex. Civ. App. 1925) (immunity applied to contract suit against Mexican agent because Mexican government was real party in interest); U.S. Amicus Br., *Lewis*, 2020 WL 2866592, at *9 (rejecting "pleading distinction between personal- and official-capacity suits"). Accordingly, denying immunity here would not allow "circumvent[ion] [of] the FSIA" through the mere expedient of "filing an individual-capacity suit." Br. 41. Neither *Lewis* nor the Restatement disagrees with the proposition that immunity may apply where a suit is asserted only nominally against an

official in his personal capacity, but in fact would substantively enforce a rule of law against a foreign state. *Contra* Br. 38, 40.

This Court's decision in *Doğan* supports the foregoing analysis. There, the plaintiffs sued the former Israeli Defense Minister who allegedly "planned" and "directed" the military operation leading to the death of the plaintiffs' son. 932 F.3d at 891. Although the suit nominally sought damages from the defendant alone, not from the Israeli treasury, the Court recognized that allowing it "would be to enforce a rule of law against the state." *Id.* at 894. The defendant (himself a high-ranking official) "was instructed by the Prime Minister to conduct the operations," "Israel's Basic Law" fully authorized the defendant to do so, Israel "ratified the defendant's conduct," and "the State Department file[d] a Suggestion of Immunity on his behalf." *Id.* at 894, 897. In those circumstances, even a *nominally* personal-capacity suit would in fact coercively affect Israel's ability to undertake core sovereign acts. But *Doğan* does not disturb the general rule that personal-capacity suits seeking relief against a foreign agent alone may proceed. *Contra* Br. 35, 38.

3. As the district court correctly held, granting judgment against NSO here would not enforce a rule of law against a foreign state. NSO has never "argued that any of [its] foreign sovereign customers would be forced to pay

a judgment against [NSO] if [WhatsApp] were to prevail in this lawsuit." ER12. And the district court can "craft injunctive relief that does not require a foreign sovereign to take affirmative action" or restrain any sovereign acts. *Id.*

Nor is this a case where a personal-capacity suit *effectively* binds a foreign state, turning that state into the real party in interest. NSO's responsibility to pay damages out of its corporate coffers will not coerce any foreign government into altering its conduct. And an injunction restraining NSO from hacking WhatsApp's app and servers, ER75, will not obstruct foreign governments' "national-security and law-enforcement operations." *Contra* Br. 39. NSO has not even identified which foreign governments would suffer these supposed consequences. And it has never explained why a foreign state could not engage in the same conduct through its own officers, form a majority-state-owned company, or purchase a majority of NSO's shares. But even assuming *arguendo* that a remedy against NSO had some "attenuated" effect on unidentified foreign states' budgets or conduct, it would fall short of the "direct" consequences necessary to make a foreign state a real party in interest. *Lewis*, 918 F.3d at 147.

Confirming that a judgment against NSO would not apply a rule of law to any foreign state, none of the relevant factors that led to immunity in

Doğan is present here. No foreign leader has "instructed" NSO how to carry out its activities; no foreign law expressly empowers NSO's actions; no foreign government has "ratified [NSO's] conduct"; and the State Department has not "file[d] a Suggestion of Immunity on [NSO's] behalf." 932 F.3d at 894, 897. Unlike the defendant in *Doğan*, NSO has no valid basis for avoiding accountability. And while holding NSO accountable would not enforce a rule of law against a foreign state, doing so is essential to upholding the rule of law in U.S. courts.

CONCLUSION

NSO's appeal should be dismissed for lack of jurisdiction, or alternatively, the district court's decision should be affirmed.

Respectfully Submitted,

Dated: December 16, 2020

By: /s/ Michael R. Dreeben

Yaira Dubin
Alec Schierenbeck
O'Melveny & Myers LLP
7 Times Square
New York, NY 10036
(212) 326-2000
ydubin@omm.com
aschierenbeck@omm.com

Michael R. Dreeben
Ephraim McDowell
O'Melveny & Myers LLP
1625 Eye Street, N.W.
Washington, DC 20006
(202) 383-5300
mdreeben@omm.com
emcdowell@omm.com

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 20-16408

I am the attorney or self-represented party.

This brief contains 13,911 **words**, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- (•) complies with the word limit of Cir. R. 32-1.
- ( ) is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ( ) is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ( ) is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ( ) complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one):*
  - ( ) it is a joint brief submitted by separately represented parties;
  - ( ) a party or parties are filing a single brief in response to multiple briefs; or
  - ( ) a party or parties are filing a single brief in response to a longer joint brief.
- ( ) complies with the length limit designated by court order dated _____.
- ( ) is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Michael Dreeben **Date** Dec 16, 2020

*(use "*s/[typed name]*" to sign electronically-filed documents)*

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

CERTIFICATE OF SERVICE

I hereby certify that on December 16, 2020, I caused the foregoing to be electronically filed with the Clerk of the Court for the U.S. Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: December 16, 2020

/s/ Michael R. Dreeben
Michael R. Dreeben