DISSEMINATED BY MERCURY PUBLIC AFFAIRS, LLC, A REGISTERED FOREIGN AGENT, ON BEHALF OF Q CYBER TECHNOLOGIES LTD. MORE INFORMATION IS ON FILE WITH THE DEPT. OF JUSTICE, WASHINGTON, DC.

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

APPELLANTS' OPENING BRIEF

Jeffrey S. Bucholtz
KING & SPALDING LLP
1700 Pennsylvania Ave., NW
2nd Floor
Washington, DC 20006
jbucholtz@kslaw.com

Joseph N. Akrotirianakis
KING & SPALDING LLP
633 W. 5th Street
Suite 1600
Los Angeles, CA 90071
jakro@kslaw.com

Matthew V.H. Noller
KING & SPALDING LLP
621 Capitol Mall, Suite 1500
Sacramento, CA 95814
mnoller@kslaw.com

Counsel for Appellants
NSO Group Tech. Ltd. et al.

Dated: November 16, 2020

CORPORATE DISCLOSURE STATEMENT

Appellant NSO Group Technologies Ltd. is a privately-owned corporation whose parent company is Appellant Q Cyber Technologies Ltd., a privately-owned corporation whose parent company is OSY Technologies S.à.r.l. No publicly held corporation owns 10% or more of either Appellant's stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

In October 2019, a team of Western European law-enforcement officials were closing in on their man.[1] The target: an Islamic State terrorist who was planning an attack during the Christmas season. The terrorist was planning the attack using WhatsApp, an encrypted-messaging application owned by Appellees WhatsApp Inc. and Facebook Inc. (collectively "WhatsApp"). An "elite surveillance team" had been monitoring his WhatsApp messages with technology designed by Appellant NSO Group Technologies Ltd. A judge had authorized the investigators to use the technology, which let them track "what [the suspect] was doing, which mosque he was going to, who was talking to him, [and] whether the group was spread in neighboring countries."

Then, all of a sudden, the suspect's phone went dark. WhatsApp sent him, along with around 1,400 other users, a warning that his messages were being monitored. So he ditched the phone, denying investigators their main source of intelligence. As one European official put it, "WhatsApp killed the operation."

---

[1] These facts come from Dov Lieber et al., *Police Tracked a Terror Suspect—Until His Phone Went Dark After a Facebook Warning*, Wall St. J. (Jan. 2, 2020, 3:29 p.m.), https://on.wsj.com/38uXk5s.

This is one instance in a broader pattern. Foreign states, in Western Europe and throughout the world, frequently use technology like NSO's to investigate criminals who use WhatsApp to plan acts of terrorism, child exploitation, bank robbery, weapons trafficking, and other serious crimes. WhatsApp does not like that. It takes steps to frustrate such investigations, both by warning the targets of investigations and by refusing to cooperate with authorities in the aftermath of attacks. This conduct has "killed" or interfered with multiple lawful investigations in foreign countries.

Unsatisfied with even this level of interference, WhatsApp now wants U.S. courts to help it block foreign counterterrorism and law-enforcement investigations. But WhatsApp knows it cannot directly sue the foreign states and officials who conduct the investigations; those states and officials are plainly immune from suit. As a backdoor approach to the same goal, it has chosen to sue the foreign states' agents, NSO and its parent company Q Cyber Technologies Limited (collectively, "NSO"). NSO designs and markets its technology for the exclusive use of foreign states in lawful investigations. Foreign states, not NSO, operate the technology and choose how and when to use it. NSO provides limited

support, entirely at the direction of its foreign-state customers. And NSO's home state, Israel, oversees and regulates every aspect of NSO's business. These undisputed facts establish that NSO acts entirely in an "official capacity" as an "agent[] of foreign governments." ER 11.

By suing NSO for its conduct as an agent of foreign states, WhatsApp is asking U.S. courts to meddle in the sovereign affairs of those states. This Court should reject that request. The same common-law doctrine that protects foreign officials—known as "conduct-based immunity"—also protects NSO. It immunizes the agents (including private agents) of foreign states for actions they take in their official capacity as agents. As even the district court recognized, WhatsApp seeks to hold NSO liable for just such official conduct. ER 11.

The district court nonetheless denied NSO immunity for two misguided reasons. *First*, the court held that no foreign official or agent can receive conduct-based immunity unless a foreign state would have to pay a judgment against the official. That limitation conflicts with the common law, the governing cases, and the U.S. State Department's approach to conduct-based immunity. It also undermines foreign state immunity and exposes U.S. officials to retributive lawsuits abroad.

Second, the court held that NSO, as a foreign corporation, could not receive what the court believed to be a distinct form of immunity called "derivative sovereign immunity." But derivative sovereign immunity is not distinct from conduct-based immunity, and it is not limited to American companies. To hold otherwise, as the district court did, violates the principles underlying conduct-based immunity and threatens the United States' own reliance on private contractors for intelligence and military operations.

Under the proper test for common-law conduct-based immunity, NSO is immune from WhatsApp's lawsuit. This Court should reverse the district court's contrary holding and remand with instructions to dismiss the case.

JURISDICTIONAL STATEMENT

NSO contends that the district court lacks subject-matter and personal jurisdiction. The district court held otherwise in its order denying NSO's motion to dismiss on July 16, 2020. ER 10–32. NSO timely filed its interlocutory appeal from the district court's order on July 21, 2020. ER 46.

WhatsApp moved to dismiss the appeal. CA9 Dkt. No. 13-1. A motions panel of this Court denied that motion. CA9 Dkt. No. 18. For the reasons given below and in NSO's opposition to the motion to dismiss, the district court's denial of NSO's claim to foreign sovereign immunity is a collateral order over which this Court has appellate jurisdiction. *Compania Mexicana de Aviacion, S.A. v. U.S. Dist. Ct.*, 859 F.2d 1354, 1356 (9th Cir. 1988); *see generally* CA9 Dkt. No. 14; *infra* at 27–30.

STATEMENT OF THE ISSUE

Whether NSO enjoys conduct-based foreign official immunity for actions it takes in its official capacity as an agent of foreign sovereigns.

STATEMENT OF THE CASE

A. Legal Background

1. For more than 200 years, U.S. law has conferred immunity on foreign states and their officials. *Samantar v. Yousuf*, 560 U.S. 305, 311–12, 321 (2010). That doctrine "developed as a matter of common law." *Id.* at 311.

Under the common law, courts applied "a two-step procedure" to claims of foreign sovereign or foreign official immunity. First, "the sovereign could request a 'suggestion of immunity' from the State Department." *Id.* If the State Department recommended immunity, then

"the district court surrendered its jurisdiction." *Id.* If the State Department did not file a suggestion of immunity, then the court moved to the second step, where it "decide[d] for itself whether all the requisites for such immunity existed." *Id.* (cleaned up).

When analyzing immunity under the second step, "a district court inquired whether the ground of immunity is one which it is the established policy of the State Department to recognize." *Id.* at 312 (cleaned up). Thus, even if the State Department did not recommend immunity in the case at hand, "courts decided for themselves whether to grant immunity . . . by reference to State Department policy." *Jam v. Int'l Fin. Corp.*, 139 S. Ct. 759, 765–66 (2019). At both steps of the common-law immunity analysis, then, the governing principles were those articulated by the Executive Branch. It was "an accepted rule of substantive law governing the exercise of the jurisdiction of the courts that they accept and follow the executive determination." *Rep. of Mexico v. Hoffman*, 324 U.S. 30, 36 (1945).

2. Although common-law immunity was most often claimed by foreign states, it also protected foreign officials and other agents acting on the state's behalf. The Attorney General recognized this "conduct-

based" immunity as early as 1797. Statement of Interest of the United States of America at 6, *Matar v. Dichter*, No. 05-cv-10270 (S.D.N.Y. Nov. 17, 2006) ("*Matar* Statement"); *see* 1 Op. Att'y Gen. 45, 46 (1797) ("[I]f the seizure of the vessel is admitted to have been an official act, done by the defendant by virtue, or under color, of the powers invested in him as governor, . . . it will of itself be a sufficient answer to the plaintiff's action . . . ."); 1 Op. Att'y Gen. 81, 81 (1797) ("[I]t is as well settled in the United States as in Great Britain, that a person acting under a commission from the sovereign of a foreign nation is not amenable for what he does in pursuance of his commission, to any judiciary tribunal in the United States.").

Subsequent cases endorsed conduct-based immunity. *See Matar* Statement at 6–7. In *Underhill v. Hernandez*, 168 U.S. 250, 252 (1897), for example, the Supreme Court held that foreign officials are immune "for acts done within their own states, in the exercise of governmental authority, whether as civil officers or as military commanders."[2] The

[2] Although *Underhill* is often cited as applying the "act of state" doctrine, "sovereign immunity provided an independent ground" for its holding. *Banco Nacional de Cuba v. Sabbatino*, 376 U.S. 398, 430 (1964). The United States treats *Underhill* as an early expression of conduct-

basis for this immunity is that "the acts of the official representatives of the state are those of the state itself, when exercised within the scope of their delegated powers." *Underhill v. Hernandez*, 65 F. 577, 579 (2d Cir. 1895), *aff'd*, 168 U.S. 250; *accord Greenspan v. Crosbie*, 1976 WL 841, at *1–2 (S.D.N.Y. Nov. 23, 1976); *Waltier v. Thomson*, 189 F. Supp. 319, 320–21 (S.D.N.Y. 1960); *Lyders v. Lund*, 32 F.2d 308, 309 (N.D. Cal. 1929).

Conduct-based immunity extended beyond foreign officials to "agent[s]" and other "individual defendants [who] acted on behalf of the state." *Matar* Statement at 8, 10; *see Heaney v. Gov't of Spain*, 445 F.2d 501, 504 (2d Cir. 1971) (recognizing that common-law foreign sovereign immunity protects foreign agents for their official acts); *Belhas v. Ya'alon*, 515 F.3d 1279, 1285 (D.C. Cir. 2008) (finding this principle "well settled" by 1976). Because a "government does not act but through its agents," *Herbage v. Meese*, 747 F. Supp. 60, 66 (D.D.C. 1990), it was the agent's "act itself and whether the act was performed on behalf of the foreign state . . . that [was] the focus of the courts' holdings," *Rishikof v.*

---

based immunity. *E.g.*, Brief for the United States as Amicus Curiae at 13, *Mutond v. Lewis*, No. 19-185 (U.S. May 26, 2020) ("*Mutond* Amicus Br."); Brief for the United States as Amicus Curiae at 14, *Samantar v. Yousuf*, No. 12-1078 (U.S. Dec. 10, 2013) ("*Samantar II* Amicus Br.").

Mortada, 70 F. Supp. 3d 8, 13 (D.D.C. 2014). In other words, under the common law, "any act performed by the individual as an act of the State enjoys the immunity which the State enjoys." Hazel Fox, *The Law of State Immunity* 455 (2d ed. 2008).

3. In 1976, Congress passed the Foreign Sovereign Immunities Act to codify some aspects of foreign sovereign immunity. The FSIA supersedes the common law for foreign states and their agencies and instrumentalities. *Samantar*, 560 U.S. at 313. But it has no effect on conduct-based foreign sovereign immunity for foreign officials and agents, which remains a matter of common law. *Id.* at 321, 324.

a. Accordingly, courts after 1976 continued to recognize conduct-based immunity for foreign officials and other agents. *E.g.*, *Mireskandari v. Mayne*, 800 F. App'x 519, 519 (9th Cir. 2020); *Doğan v. Barak*, 932 F.3d 888, 893–94 (9th Cir. 2019); *Yousuf v. Samantar*, 699 F.3d 763, 774–75 (4th Cir. 2012); *Matar v. Dichter*, 563 F.3d 9, 14 (2d Cir. 2009); *Velasco v. Gov't of Indonesia*, 370 F.3d 392, 398–99 (4th Cir. 2004); *In re Estate of Ferdinand Marcos*, 25 F.3d 1467, 1472 (9th Cir. 1994); *Chuidian v. Philippine Nat'l Bank*, 912 F.2d 1095, 1106 (9th Cir. 1990); *Rishikof*, 70 F. Supp. 3d at 13; *Smith v. Ghana Commercial Bank, Ltd.*, 2012 WL

2930462, at *10 (D. Minn. June 18, 2012), *report and recommendation adopted*, 2012 WL 2923543 (D. Minn. July 18, 2012), *aff'd*, No. 12-2795 (8th Cir. Dec. 7, 2012); *Herbage*, 747 F. Supp. at 66; *cf. Am. Bonded Warehouse Corp. v. Compagnie Nationale Air France*, 653 F. Supp. 861, 863–64 (N.D. Ill. Feb. 17, 1987) (holding that defendants "sued in their respective capacities as employees of Air France" would be immune for official acts).

Although some of these decisions erroneously treated the FSIA rather than the common law as the source of conduct-based immunity, their reasoning is still "instructive for post-*Samantar* questions of common law immunity." *Yousuf*, 699 F.3d at 774. The United States has approved "the rationale for the immunity recognized in these cases" despite their misplaced reliance on the FSIA. *Matar* Statement at 13–14.

b. The post-1976 case law has also recognized that private agents of a foreign state enjoy conduct-based immunity when acting in their capacity as foreign agents.

For example, the Fourth Circuit held in *Butters v. Vance Int'l, Inc.*, 225 F.3d 462 (4th Cir. 2000), that a private security firm was immune for employment decisions it made while providing security services to Saudi

Arabia. *Id.* at 466. The court held, consistent with the common law, that "courts define the scope of sovereign immunity by the nature of the function being performed—not by the office or the position of the particular employee involved." *Id.* "All sovereigns," the court recognized, "need flexibility to hire private agents to aid them in conducting governmental functions." *Id.* Therefore, private "agents enjoy derivative sovereign immunity when following the commands of a foreign sovereign employer." *Id.*

Butters relied in part, *id.*, on *Alicog v. Kingdom of Saudi Arabia*, 860 F. Supp. 379 (S.D. Tex. 1994). Two of the defendants in *Alicog* were private citizens who had been hired by Saudi Arabia to book hotel rooms and furnish drivers and security guards. *Id.* at 381. A Saudi prince ordered the private defendants to confine the plaintiffs, the prince's servants, to the prince's hotel. *Id.* at 384–85. The court held that the private defendants were immune for following the prince's orders because they were acting as Saudi Arabia's agents at the time. *Id.* The Fifth Circuit summarily affirmed. *Alicog v. Kingdom of Saudi Arabia*, 79 F.3d 1145 (5th Cir. 1996) (table).

Other courts have reached the same conclusion. In *Moriah v. Bank of China*, 107 F. Supp. 3d 272 (S.D.N.Y. 2015), the court found a private Israeli citizen immune for actions he took "at the behest of the Israeli government." *Id.* at 277–78. The court found it "well-settled" that "conduct-based immunity . . . extends beyond current and former officials to individuals acting as an agent for the government." *Id.* at 277. And because the defendant acted at Israel's request, he was immune "as an agent of the Israeli government." *Id.* at 278. Similarly, the court in *Ivey ex rel. Carolina Golf Dev. Co. v. Lynch*, 2018 WL 3764264 (M.D.N.C. Aug. 8, 2018), held that a private attorney enjoyed common-law immunity for actions he took as the agent of a German official. *Id.* at *6–7. The court approved the defendant's argument that "'foreign official immunity extends to the private, domestic agents of foreign officials.'" *Id.*

4. Extending conduct-based immunity to the agents of foreign states also accords with the "law of nations," which "is part of federal common law." *Estate of Ferdinand Marcos*, 25 F.3d at 1473.

a. "[C]ustomary international law" has long granted immunity to "individuals acting as an agent for the government." *Moriah*, 107 F. Supp. 3d at 277; *see* Office of the Legal Adviser, U.S. Dep't of State, *Digest*

of United States Practice in International Law, Ch. 10, § B(3), at 426 (CarrieLyn D. Guymon, ed. 2015); Curtis A. Bradley & Jack L. Goldsmith, *Foreign Sovereign Immunity, Individual Officers, and Human Rights Litigation*, 13 Green Bag 2d 9, 14–15 (2009). The House of Lords, for instance, has held that a "foreign state's right to immunity cannot be circumvented by suing its servants or agents." *Jones v. Ministry of Interior*, UKHL 26 ¶ 10 (House of Lords, U.K. 2006). A Canadian appellate court has approved "the common law principle that, when acting in pursuit of their duties, officials or employees of foreign states enjoy the benefits of sovereign immunity." *Jaffe v. Miller*, 95 ILR 446, 460 (Ontario Ct. App., Canada 1993). And Germany's Federal Supreme Court has held that "[t]he acts of [government] agents constitute direct State conduct and cannot be attributed as private activities to the person authorized to perform them." *Church of Scientology Case*, 65 ILR 193, 198 (Fed. Supreme Ct., Fed. Rep. of Germany 1978). That is true even when the agent would be a private actor under the foreign state's laws. *Id.* at 197. As long as the agent's challenged acts are not "entirely unrelated to the official activities of the

agency concerned," they "must be placed within the ambit of State conduct." *Id.* at 198.

The international community has codified this consensus about the scope of conduct-based foreign sovereign immunity in the United Nations Convention on Jurisdictional Immunities of States and their Property. U.N. Doc. A/RES/59/38 (Dec. 16, 2004), *available at* https://treaties.un.org/doc/source/RecentTexts/English_3_13.pdf. The Convention, which has been signed or ratified by thirty-six nations,[3] grants "State" immunity to "representatives of the State acting in that capacity." *Id.* Art. 2, ¶ 1(b)(4). "Actions against such representatives or agents of a foreign Government in respect of their official acts are essentially proceedings against the State they represent." Report of the International Law Commission to the General Assembly on the Work of Its Forty-Third Session at 18, U.N. Doc. A/46/10 (Jul. 19, 1991), *available at* https://legal.un.org/ilc/documentation/english/reports/a_46_10.pdf. While the United States has not signed the Convention, it views its

[3] *See* U.N. Treaty Collection, Status of Treaties: United Nations Convention on Jurisdictional Immunities of States and Their Properties, *available at* https://bit.ly/3iYy8Zv.

treatment of conduct-based immunity "as consistent with customary international law." *Matar* Statement at 21.

b. As with much of international law, common-law immunity is "a matter of comity." *Rep. of Austria v. Altmann*, 541 U.S. 677, 688 (2004); *see Hilton v. Guyot*, 159 U.S. 113, 228 (1895) ("[I]nternational law is founded upon mutuality and reciprocity."); *Siderman de Blake v. Rep. of Argentina*, 965 F.2d 699, 718 (9th Cir. 1992) ("[F]oreign sovereign immunity 'is rooted in two bases of international law, the notion of sovereignty and the notion of the equality of sovereigns.'"); *Jones*, UKHL 26 ¶ 1 ("[S]tates must treat each other as equals not to be subjected to each other's jurisdiction.").

For one nation's courts to exercise jurisdiction over the official acts of another nation's agents "would destroy, not enhance that comity." *Belhas*, 515 F.3d at 1286. The United States has warned that "personal damages actions against foreign officials could . . . trigger concerns about the treatment of United States officials abroad, and interfere with the Executive's conduct of foreign affairs." *Mutond* Amicus Br. at 16; *cf. Sabbatino*, 376 U.S. at 423 ("[T]he Judicial Branch['s] . . . passing on the validity of foreign acts of state may hinder rather than further this

country's pursuit of goals both for itself and for the community of nations as a whole in the international sphere.").

B. Factual Background

1. NSO is an Israeli company that designs a highly regulated technology for use by governments to investigate terrorism, child exploitation, and other serious crimes. ER 52–53 ¶¶ 5–9, 63 ¶ 5. One of NSO's products—a data program called "Pegasus"—"enables law enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device." ER 107. Governments can use Pegasus to intercept messages, take screenshots, or exfiltrate a device's contacts or history. ER 67 ¶ 27, 70 ¶ 41.

Pegasus is marketed only to and used only by sovereign governments. ER 53 ¶ 9, 96. NSO licenses Pegasus to law enforcement and intelligence agencies, and those government agencies choose whether and how to use Pegasus. ER 54–55 ¶ 14. NSO's foreign-state customers—not NSO—determine whether to install Pegasus on a mobile device, and then the government customers install Pegasus and monitor the device. *See* ER 55 ¶ 15.

Because of Pegasus's effectiveness, it is subject to strict regulation. Export of Pegasus is regulated under Israel's Defense Export Control Law, which authorizes Israel's Ministry of Defense to grant or deny any license between NSO and its foreign-sovereign customers. ER 52 ¶¶ 5, 6. In addition, the Ministry of Defense mandates that NSO require its users to certify that Pegasus "will be used only for prevention and investigation of terrorism and criminal activity." ER 53 ¶ 8. And the Ministry of Defense may itself deny or revoke export licenses if it determines that a foreign country has used Pegasus for an unauthorized reason, such as to violate human rights. ER 54 ¶ 12. Pegasus is also designed with technical safeguards, including general and customer-specific geographic restrictions that prevent it from accessing any device with a U.S. phone number or any device within the geographic bounds of the United States. ER 54 ¶ 13.

WhatsApp, owned by Facebook, is a popular communication service. *See* ER 65 ¶ 17. WhatsApp, together with Facebook Messenger and Instagram, are used by 1.5 billion people in 180 countries. *Id.* Some WhatsApp users are violent criminals and terrorists who exploit the software's encryption to avoid detection. Terrorists have used WhatsApp

to plan and execute attacks, while WhatsApp disclaims responsibility and resists efforts to use its technology and data to prevent the attacks or investigate the perpetrators. Because WhatsApp takes the position that preventing criminals and terrorists from using its platform is not its job, governments understandably hire third parties such as NSO to provide the tools they need to protect citizens from violent attacks facilitated by encrypted communications. *See* Lieber, et al., *supra*.

For instance, the Islamic State terrorist who attacked London's Westminster Bridge in 2017 used WhatsApp two minutes before killing five innocent civilians. Three months later, terrorists used WhatsApp to plan a knife rampage on London Bridge. Following both attacks, WhatsApp refused to turn over the terrorists' messages or to assist in apprehending them. *E.g.*, Dipesh Gadher, *London Bridge Terror Attack Planned on WhatsApp*, Sunday Times (May 12, 2019, 12:01 a.m.), https://bit.ly/38xG2Uy; Gordon Rayner, *WhatsApp Accused of Giving Terrorists "A Secret Place to Hide" as It Refuses to Hand Over London Attacker's Messages*, Telegraph (Mar. 27, 2017, 1:54 p.m.), https://bit.ly/38uHkjl; Dan Sabbagh, *Call for Backdoor Access to WhatsApp as Five Eyes Nations Meet*, The Guardian (July 30, 2019, 3:32

p.m.), https://bit.ly/2InSNpZ; Ryan Sabey, *Tool of Terror: Social Media Giants Will Be Made to Hand over Encrypted WhatsApp Messages in Fight Against Terrorism*, The Sun (Sept. 29, 2019, 7:45 a.m.), https://bit.ly/2TuLNhK.

Technology like Pegasus enables sovereign governments to prevent terrorism and violent crime while exposing how WhatsApp is used as a safe space by terrorists and other criminals. WhatsApp and Facebook don't like that, so they take steps to prevent law enforcement and intelligence agencies from investigating users.

In May 2019, WhatsApp notified 1,400 users that their WhatsApp accounts may have been compromised by government actors using NSO's technology. ER 71 ¶ 44. WhatsApp's notification "killed" a significant government investigation into an Islamic State terrorist who had been using WhatsApp to plan an attack. Lieber et al., *supra*.

2. WhatsApp filed this suit in October 2019, claiming that its servers were used in the process of installing Pegasus on the devices of 1,400 users in violation of WhatsApp's terms of service. ER 63 ¶ 1. It sought injunctive relief and damages for violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and state law.

NSO moved to dismiss. *See* ER 1. Among other defenses, NSO challenged the district court's subject-matter jurisdiction on the ground that it was immune from this suit as an agent of foreign sovereigns. *See* ER 11. In support, NSO filed a declaration from its CEO, which discussed its technology, Pegasus's exclusive use by sovereign governments, and the regulations constraining NSO. ER 51–56. NSO also filed a report from its independent auditor about its compliance with Israel's export controls. ER 57–61.

By submitting this evidence, NSO raised a "factual" challenge to the district court's subject-matter jurisdiction. ER 9. NSO's declarations showed, as a matter of fact, that "NSO markets and licenses its Pegasus technology exclusively to sovereign governments and authorized agencies for national security and law enforcement purposes." ER 53 ¶ 9. NSO's "sovereign customers . . . operate the technology themselves, to advance their own sovereign interests of fighting terrorism and serious crime." ER 54–55 ¶ 14. NSO's "role is limited to . . . providing advice and technical support to assist customers in setting up—not operating—the Pegasus technology." *Id.* NSO "provide[s] these support services . . . entirely at the direction of [its] government customers." *Id.*

The district court recognized that NSO's evidence shifted the burden to WhatsApp to "furnish affidavits or other evidence necessary to satisfy its burden of establishing subject matter jurisdiction." ER 5 (quoting *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004) (internal quotation marks omitted)). WhatsApp, however, did not submit any evidence to contradict NSO's evidence. As a result, the district court found NSO's evidence related to subject-matter jurisdiction to be undisputed. *E.g.*, ER 11.

3. The district court dismissed one state-law claim but otherwise denied NSO's motion. *See* ER 1–45. In particular, it declined to dismiss the suit as barred by foreign sovereign immunity. Although NSO argued that its immunity was "grounded in the common law of foreign sovereign immunity," the district court treated its immunity claim as implicating "two distinct doctrines, foreign official immunity and derivative sovereign immunity." ER 11 n.1.

The district court found, based on NSO's undisputed evidence, that NSO was an agent of foreign governments and that NSO's alleged conduct fell within its "official capacity" as a foreign agent. ER 11. Nonetheless, the court ruled that NSO did not qualify for conduct-based

foreign official immunity because a judgment against NSO would not bind any foreign sovereign. As the court put it, NSO's "foreign sovereign customers would [not] be forced to pay a judgment against defendants if plaintiffs were to prevail," and "the court can craft injunctive relief that does not require a foreign sovereign to take an affirmative action." ER 12. As for derivative sovereign immunity, the court reasoned that if that species of immunity were valid, it would apply only to American companies. ER 13–14.

NSO timely appealed. ER 46. WhatsApp moved to dismiss the appeal for lack of appellate jurisdiction, and a motions panel denied that motion. CA9 Dkt. No. 18.

SUMMARY OF THE ARGUMENT

WhatsApp seeks to hold NSO liable for actions it allegedly performed as an agent of foreign governments. Under the common law, NSO is immune from claims based on that official conduct. The district court's holding otherwise conflicts with the common law as developed by the controlling cases and the United States' longstanding approach to conduct-based immunity. This Court should reverse.

I. As a preliminary matter, WhatsApp may renew its argument that this Court lacks appellate jurisdiction. A motions panel already rejected that argument, and for good reason. This Court has held that a denial of foreign sovereign immunity is immediately appealable. *Compania Mexicana de Aviacion, S.A. v. U.S. Dist. Ct.*, 859 F.2d 1354, 1356 (9th Cir. 1988). This appeal falls squarely within that rule. *See Doğan v. Barak*, 932 F.3d 888, 895 (9th Cir. 2019); *Farhang v. Indian Inst. of Tech.*, 655 F. App'x 569, 571 (9th Cir. 2016). WhatsApp's contrary arguments go to the merits of the appeal—*i.e.*, whether NSO is in fact entitled to foreign sovereign immunity—not to this Court's jurisdiction to decide that question. *Del Campo v. Kennedy*, 517 F.3d 1070, 1072 (9th Cir. 2008).

II. The district court's factual findings, which were undisputed below and thus not subject to challenge on appeal, confirm that NSO is entitled to common-law foreign sovereign immunity. The district court found, based on NSO's undisputed evidence, that NSO is an "agent[] of foreign governments" and that it performed the conduct WhatsApp challenges in its "official capacity" as a foreign agent. ER 11. Those findings satisfy the requirements for conduct-based immunity.

III. Despite finding that NSO was a foreign agent acting in its official capacity, the district court denied NSO immunity based on two holdings with no basis in the common law. First, the court held that NSO could not receive conduct-based immunity unless a foreign sovereign would be bound by a judgment against NSO. Second, the court held that "derivative sovereign immunity," which it treated as distinct from conduct-based immunity, cannot protect foreign entities. Both holdings were incorrect.

A. The Supreme Court and this Court have both already rejected the district court's holding that conduct-based immunity cannot exist when a plaintiff sues a foreign agent in its individual capacity. *Samantar v. Yousuf*, 560 U.S. 305, 325 (2010); *Mireskandari v. Mayne*, 800 F. App'x 519, 519 (9th Cir. 2020); *Doğan*, 932 F.3d at 894. The United States' longstanding practice, which provides the basis for common-law immunity, similarly forecloses the district court's approach. *Mutond* Amicus Br. at 8–10.

The district court held otherwise based on the D.C. Circuit's decision in *Lewis v. Mutond*, 918 F.3d 142 (D.C. Cir. 2019), which interpreted Section 66 of the Second Restatement of Foreign Relations

Law to bar conduct-based immunity in individual-capacity suits. But the D.C. Circuit doubted that Section 66 accurately reflects the common law, and it misread Section 66's test for immunity in any event. The governing cases—including this Court's decision in *Doğan*—and the United States' practice confirm that common-law conduct-based immunity applies in individual-capacity suits.

Any other rule would undermine the FSIA and endanger U.S. officials. If litigants can avoid foreign sovereign immunity merely by suing foreign officials or agents instead, they could easily "accomplish indirectly what the [FSIA] bar[s] them from doing directly." *Chuidian v. Philippine Nat'l Bank*, 912 F.2d 1095, 1102 (9th Cir. 1990). And that rule would also open foreign courts to retributive lawsuits or prosecutions against U.S. officials.

B. The district court's holding that "derivative sovereign immunity" does not protect foreign entities rests on two mistakes.

The court's first mistake was treating derivative foreign sovereign immunity as distinct from conduct-based foreign sovereign immunity. There is no such distinction. Derivative sovereign immunity and conduct-based immunity are two names for the same common-law rule: foreign

sovereigns' agents are immune from suit for actions they take in their capacity as agents.

The court's second mistake was excluding foreign entities from the scope of immunity. There is no good reason why a doctrine designed to protect *foreign* sovereigns and *foreign* officials should exclude *foreign* entities. Indeed, limiting immunity to American entities disrespects the equal sovereignty of foreign states and threatens the United States' ability to conduct important intelligence and military operations. The United States relies extensively on private contractors for such operations. But if U.S. courts can entertain suits against foreign states' foreign agents, then foreign courts can entertain similar suits against the United States' domestic agents.

For all these reasons, this Court should reverse the district court's decision and hold that NSO is entitled to conduct-based immunity.

STANDARD OF REVIEW

This Court reviews the district court's denial of NSO's motion to dismiss de novo. *Fed. Home Loan Mortg. Corp. v. SFR Invs. Pool 1, LLC*, 893 F.3d 1136, 1144 (9th Cir. 2018). It reviews the district court's factual findings for clear error. *Will v. United States*, 60 F.3d 656, 658 (9th Cir.

1995). It reviews questions of its own jurisdiction de novo. *Hunt v. Imperial Merchant Servs., Inc.*, 560 F.3d 1137, 1140 (9th Cir. 2009).

ARGUMENT

I. This Court Has Appellate Jurisdiction Over the District Court's Denial of NSO's Claim to Conduct-Based Immunity

WhatsApp has argued that this Court lacks jurisdiction over NSO's appeal, and it may renew that argument in its answering brief. As NSO argued in its opposition to WhatsApp's motion to dismiss the appeal, which a motions panel denied, WhatsApp is wrong. A denial of foreign sovereign immunity is immediately appealable under the collateral order doctrine. *See generally* CA9 Dkt. No. 14. WhatsApp's arguments otherwise are foreclosed by this Court's precedent.

A. This Court has already held that a denial of foreign sovereign immunity is appealable as a collateral order. *Compania Mexicana de Aviacion*, 859 F.2d at 1356. That is because foreign sovereign immunity confers "an immunity from suit rather than a mere defense to liability; it is effectively lost if a case is erroneously permitted to go to trial." *Id.* at 1358.

The same is true for the conduct-based foreign sovereign immunity enjoyed by agents of foreign states. In *Doğan*, this Court held that conduct-based "common law foreign official immunity" is "an immunity

from *suit* rather than a mere defense to *liability*." 932 F.3d at 895 (internal quotation marks omitted). Confirming what it explained in *Doğan*, this Court has considered an interlocutory appeal from the denial of a motion to dismiss based on common-law foreign sovereign immunity. *Farhang*, 655 F. App'x at 571. In that case, this Court held that it had jurisdiction over an individual's appeal of the district court's denial of common-law foreign official immunity. *Id.*; *see also Yousuf*, 699 F.3d at 768 n.1 (holding that denial of common-law foreign sovereign immunity "is immediately appealable under the collateral-order exception").

Like the defendants in *Doğan* and *Farhang*, NSO appeals the denial of its claim to common-law foreign sovereign immunity. That denial, as this Court's cases dictate, is immediately appealable as a collateral order. It is conclusive and resolved an important question: whether NSO is entitled to immunity as the agent of a foreign sovereign. It is also effectively unreviewable on appeal from a final judgment: "Because the whole point of [foreign official] immunity is to enjoy 'an immunity from suit rather than a mere defense to liability,'" NSO will have been deprived of its immunity if forced to go through discovery and

litigate all the way to final judgment in the district court. *Doğan*, 932 F.3d at 895.[4]

B. WhatsApp has never cited a single case, from any court, holding that a denial of foreign sovereign immunity, including conduct-based immunity, is not immediately appealable. Instead, WhatsApp has disputed the merits of NSO's claim, arguing that it is not entitled to immunity as the agent of foreign sovereigns. *See* CA9 Dkt. No. 13 at 12–13, 17–19. These merits issues have no bearing on the Court's jurisdiction.

This Court rejected an argument indistinguishable from WhatsApp's in *Del Campo*. There, a private company claimed Eleventh Amendment sovereign immunity for acts it took as an agent for a state government. 517 F.3d at 1072. The plaintiff argued that the state's immunity did not extend to private entities, so the Court lacked jurisdiction to hear the appeal. The Court disagreed, holding that it had jurisdiction over "[a]ppeals from denial of sovereign immunity," even if raised by a private party. *Id.* at 1074. The plaintiff's argument conflated

[4] Indeed, after NSO filed its appeal, the district court held that the immunity claimed by NSO is an immunity from suit, not merely from liability, and therefore stayed proceedings pending this Court's resolution of NSO's appeal. *See* CA9 Dkt. No. 16.

the issue on appeal—whether the contractor had a *meritorious* claim to sovereign immunity—with whether the Court had jurisdiction to decide that question. As the Court put it, "[w]hether the immunity reaches beyond 'states and state entities' is the substantive issue we face, which we may not prejudge by denying jurisdiction to decide it." *Id.*

As in *Del Campo*, WhatsApp disputes whether foreign sovereign immunity "reaches beyond [foreign] 'states and state entities'" to agents of foreign states like NSO, but that is "the substantive issue" on appeal. *Id.* This Court has jurisdiction to decide that merits question, which it should not "prejudge" by "denying jurisdiction." *Id.*

II. NSO Is Entitled to Conduct-Based Immunity Because It Acted as an Agent of Foreign Sovereigns

Under the common law, a defendant is entitled to foreign sovereign immunity if it (1) is an agent of a foreign sovereign and (2) is being sued for acts it took in its capacity as an agent. *Supra* at 5–16. As the district court found, the undisputed evidence shows that NSO satisfies both of these requirements. ER 11. It is entitled to conduct-based immunity.

A. The district court found that NSO is an "agent[] of foreign governments." ER 11. That finding was undisputed. *Id.* The complaint alleges that NSO's customers include the Kingdom of Bahrain, the

United Arab Emirates, and Mexico. *Id.*; ER 70 ¶ 43. And NSO's evidence shows that NSO acts *exclusively* as an agent of foreign sovereigns. ER 53 ¶ 9. WhatsApp did not contradict this evidence.[5]

B. The district court similarly found that, with respect to the conduct at issue in this lawsuit, NSO acted in its "official capacity" as an agent of foreign states. ER 11. That finding was also undisputed. *Id*. NSO provides its technology to foreign states "to fight terrorism and serious crime, which are official public acts." *Id.*; *see* ER 53 ¶ 9. Under NSO's contracts, its foreign state customers make every decision about whether and how to use NSO's technology, and the foreign states operate the technology themselves. ER 54–55 ¶ 14. NSO's role is limited to providing occasional technical support, which it does entirely at the direction of foreign states. *Id.* As the district court found, WhatsApp did not argue "that [NSO] w[as] acting outside the scope of [its] contracts" or that NSO

[5] The complaint alleges, based on three articles, that NSO has private customers. ER 70 ¶ 43 & n.2. None of the articles supports that claim; to the contrary, they show that NSO's customers are foreign states. And NSO's evidence confirms that NSO has no private customers. ER 53 ¶ 9. Because WhatsApp introduced no evidence to the contrary, its allegations are not assumed to be true. *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004).

"operated outside [its] official capacity." ER 11. Based on these undisputed facts, NSO is entitled to conduct-based immunity.

Although WhatsApp did not raise this argument in its opposition to NSO's motion to dismiss, it has argued in subsequent filings that NSO cannot seek conduct-based immunity from claims based on its design and marketing of technology. This is wrong because none of WhatsApp's claims can be divorced from NSO's foreign state customers' use of its technology, which are undisputedly "official public acts." ER 11. All of WhatsApp's claims require proof of injury. *See* 18 U.S.C. § 1030(g) (limiting cause of action to "[a]ny person who suffers damage or loss"); Cal. Penal Code § 502(e)(1) (limiting cause of action to person "who suffers damage or loss"); *Behnke v. State Farm Gen. Ins. Co.*, 196 Cal. App. 4th 1443, 1468 (2011) ("Damages are an essential element of a breach of contract claim."). WhatsApp only alleges injury caused by NSO's customers' use of NSO's technology, not by any of NSO's other alleged conduct. ER 72–74 ¶¶ 57, 64, 73. The alleged use of NSO's technology is thus an essential part of every claim. Because NSO's conduct-based immunity applies to an essential element of every claim, it bars WhatsApp's entire suit.

In addition, because NSO exclusively designs its technology for, and exclusively markets it to, governments, ER 53 ¶ 9, all of that conduct serves its role as a government agent. Whether foreign states *direct* NSO's design or marketing of its technology is of no moment, since it is still "on behalf of" NSO's "foreign state" customers. *Rishikof*, 70 F. Supp. 3d at 13. At a minimum, it is not "entirely unrelated to the official activities" of NSO's customers and thus "must be placed within the ambit of State conduct." *Church of Scientology Case*, 65 ILR at 198.

III. The District Court Erred in Denying NSO Foreign Sovereign Immunity

Although the district court recognized that NSO is being sued for its conduct as an agent of foreign sovereigns, the court nonetheless denied NSO immunity. The court gave two reasons for this conclusion. First, it held that NSO could not receive conduct-based foreign sovereign immunity unless a judgment against it would bind a foreign sovereign. ER 12. Second, it held that "derivative sovereign immunity," if treated as a distinct basis for immunity, is available only to American entities. ER 14–15.

Both of these holdings are erroneous. They are inconsistent with the common law as articulated by the Supreme Court, this Court, and

the Executive Branch. And they would impair the United States' foreign relations by exposing U.S. officials and agents to retributive lawsuits and prosecutions in foreign tribunals. This Court should reverse.

A. Conduct-Based Immunity Does Not Require That a Foreign Sovereign Be Bound by the Judgment

1. Conduct-Based Immunity Protects Foreign Agents in Individual-Capacity Suits

The common law does not support the district court's restriction of conduct-based immunity to cases in which a foreign sovereign "would be forced to pay a judgment" or "to take an affirmative action." ER 12. That holding categorically excludes "individual capacit[y]" suits from the scope of conduct-based immunity. *Id.* But the common law, as discussed above, immunizes foreign officials and agents for their conduct on behalf of foreign states. *Supra* at 5–16. That immunity would be illusory if it did not apply where it was most needed—*i.e.*, in cases brought against foreign officials and agents. After all, if a suit is brought against a foreign state itself rather than its agent, it does not matter whether the agent is immune. Saying that foreign agents are immune except in cases brought against foreign agents makes no sense. *Mutond* Amicus Br. at 9-10 ("Indeed, the question of conduct-based immunity logically arises when

the defendant is not sued in his official capacity—*i.e.*, when the foreign government is *not* the real party in interest.").

The Supreme Court and this Court have already held that foreign officials and agents are immune for their conduct on behalf of foreign states. The plaintiffs in *Samantar* sued the defendant "in his personal capacity" and "s[ought] damages from his own pockets." *Samantar*, 560 U.S. at 325. Yet the Supreme Court held that the case was "properly governed by the common law." *Id.*[6] Similarly, the plaintiffs in *Doğan* sought damages solely from a foreign official, not a foreign state. *See* Complaint at 30, *Doğan v. Barak*, No. 2:15-cv-08130 (C.D. Cal. Oct. 16, 2015), ECF No. 1. Yet this Court granted conduct-based immunity because holding the official liable for acts he performed on behalf of a foreign state "would be to enforce a rule of law against the sovereign state." *Doğan*, 932 F.3d at 894. In *Mireskandari* this Court also granted conduct-based immunity to defendants who "acted to further the

[6] The Fourth Circuit eventually denied immunity on the grounds that officials cannot be immune for *jus cogens* violations and that the United States had not officially recognized the defendant's government. *Yousuf*, 699 F.3d at 777–78. This reasoning would have been unnecessary if the defendant were categorically ineligible for immunity when sued "in his personal capacity." *Samantar*, 560 U.S. at 325.

objectives of foreign government entities," 800 F. App'x at 519, even though the plaintiffs sought a judgment "payable not by the sovereign but the defendants themselves," Pet. for a Writ of Certiorari at 28–29, *Mireskandari v. Mayne*, No. 20-307 (U.S. Sept. 3, 2020), *cert. denied*, 2020 WL 6551910 (U.S. Nov. 9, 2020). All of these decisions are inconsistent with the district court's holding that a foreign agent may not receive conduct-based immunity unless the foreign sovereign would be bound by the judgment.

The district court's holding also "contradicts the principles of foreign official immunity long advanced by the Executive Branch," which rejects the proposition that "conduct-based immunity has no application to suits against foreign officials in their personal capacities." *Mutond* Amicus Br. at 8–9. Because conduct-based immunity "turns on whether the challenged *action* was taken in an official capacity," the "Executive Branch has repeatedly suggested immunity in suits filed against foreign officials in their personal capacities." *Id.* at 9–10. This clear "State Department policy" must inform courts' application of common-law immunity. *Jam*, 139 S. Ct. at 765–66; *see Doğan*, 932 F.3d at 893. And it compels a rejection of the district court's contrary holding.

2. The District Court Erroneously Relied on the D.C. Circuit's Interpretation of the Second Restatement to Hold That Conduct-Based Immunity Does Not Apply to Individual-Capacity Suits

Despite the controlling cases and Executive Branch practice applying conduct-based immunity in individual-capacity suits, the district court based its contrary rule on the D.C. Circuit's decision in *Lewis*, 918 F.3d 142. *See* ER 12. In *Lewis*, the D.C. Circuit assumed without deciding that Section 66 of the Second Restatement of Foreign Relations Law "accurately sets out the scope of common-law immunity." 918 F.3d at 146. Under Section 66(f), an "agent of the state" is immune "if the effect of exercising jurisdiction would be to enforce a rule of law against the state." Restatement (Second) of Foreign Relations Law § 66(f) (1965). The D.C. Circuit interpreted that principle to defeat conduct-based immunity any time "the plaintiff pursues an individual-capacity claim seeking relief against an official in a personal capacity." *Lewis*, 918 F.3d at 147.

The district's court's reliance on *Lewis* was mistaken for a number of reasons, the most fundamental of which is that it conflicts with the controlling law. As explained, the Supreme Court's and this Court's cases hold that conduct-based immunity applies in individual-capacity suits.

Supra at 34–36; *Samantar*, 560 U.S. at 325; *Mireskandari*, 800 F. App'x at 519; *Doğan*, 932 F.3d at 894. No other federal court of appeals has ever endorsed the D.C. Circuit's approach. *Mutond* Amicus Br. at 17. And the United States rejects it as "contrary to the long-stated views and practice of the Executive Branch." *Id.* at 8–14.

Even if *Lewis* were not inconsistent with the governing law, it is essentially an advisory opinion on this issue, with little precedential value. The D.C. Circuit relied on the Second Restatement only because "both parties assume[d] § 66 accurately sets out the scope of common-law immunity." *Lewis*, 918 F.3d at 146. The court acknowledged that Section 66 might not reflect the common law, *id.*, and one judge wrote separately to argue that it doesn't, *id.* at 148–49 (Randolph, J., concurring in the judgment). More importantly, the D.C. Circuit misinterpreted Section 66. This Court's decision in *Doğan* rejects the D.C. Circuit's false assumption that a lawsuit can "enforce a rule of law against the foreign state" *only if* the judgment "would bind (or be enforceable against) the foreign state." *Lewis*, 918 F.3d at 146. As explained above, the plaintiff in *Doğan* did not seek a judgment against a foreign state. *Supra* at 35. But because the defendant acted "under actual or apparent authority, or color of law," of

a foreign state, this Court held that declaring his conduct to be unlawful would "enforce a rule of law against the sovereign state" under Section 66. *Doğan*, 932 F.3d at 894. Similarly, this Court held in *Mireskandari* that the defendants were "entitled to common-law foreign sovereign immunity" entirely because they "performed the alleged conduct in their official capacities," 800 F. App'x at 519, even though the suit was against the defendants in their individual capacity and did not seek a judgment against the foreign state. And in this case, a judgment against NSO, even if its sovereign customers would not be bound to pay it, would effectively invalidate foreign states' official decisions about how to conduct their national-security and law-enforcement operations.

Other courts have likewise held that immunity exists under Section 66 when a plaintiff's lawsuit—though brought against officials or agents of a foreign state rather than the state itself—would require a court to hold unlawful conduct committed by a foreign state's agent on behalf of the state. *E.g.*, *Ivey*, 2018 WL 3764264, at *7; *Moriah*, 107 F. Supp. 3d at 278; *Ghana Commercial Bank*, 2012 WL 2930462, at *9; *see also Underhill*, 65 F. at 579 (holding that when a foreign agent acts within the scope of its agency, its acts "are those of the state itself"). Consistent

with these cases, the Second Restatement should not be interpreted to exclude conduct-based immunity in individual-capacity suits.

In short, if Section 66 meant what the D.C. Circuit believed, it would not accurately state U.S. law; but *Doğan* makes clear as a matter of binding precedent that Section 66 looks to whether the agent's acts at issue were under authority of the foreign state, not—as the D.C. Circuit erroneously believed—to whether the suit seeks a judgment that would bind the foreign state.

3. Rejecting Conduct-Based Immunity in Individual-Capacity Suits Undermines the FSIA and Exposes U.S. Officials to Retribution

The district court's holding that conduct-based immunity does not apply to individual-capacity suits will have several negative consequences. First, it gives plaintiffs an obvious end-run around the FSIA's protections for foreign states. Second, it creates a risk that foreign courts will entertain lawsuits against U.S. officials and government agents.

Allowing litigants to sue a foreign agent for its official acts merely by naming the agent in its individual capacity would "accomplish indirectly what the [FSIA] bar[s] them from doing directly." *Chuidian*,

912 F.2d at 1102. The FSIA bars suit when a foreign state is a party or "the real party in interest." *Samantar*, 560 U.S. at 325. But conduct-based immunity "logically arises when the defendant is not sued in his official capacity—*i.e*, when the foreign government is *not* the real party in interest." *Mutond* Amicus Br. at 9–10. If the named defendant is a foreign state or an agency or instrumentality of a foreign state, then it is immune under the FSIA based on its status as such; it would make no sense to apply *conduct-based common-law* immunity only to suits against defendants whose immunity is based on their *status* and governed by *the FSIA*. *Id.* Under the district court's holding, a plaintiff who wants to challenge a foreign state's conduct could easily circumvent the FSIA by filing an individual-capacity suit against the relevant foreign officials or agents. This would "frustrat[e] the important purposes served by the statute." *Matar* Statement at 4.

The district court's holding also "trigger[s] concerns about the treatment of United States officials abroad." *Mutond* Amicus Br. at 16. The United States has previously warned that its "officials are at special risk of being made the targets of politically driven lawsuits abroad," including prosecutions in "foreign criminal courts." *Matar* Statement at

22 & n.20. But if U.S. courts begin exercising jurisdiction over individual-capacity suits against foreign officials and agents, then principles of "mutuality and reciprocity" will empower foreign courts to entertain similar suits against U.S. officials and agents. *Hilton*, 159 U.S. at 228. This "threaten[s] serious harm to U.S. interests." *Matar* Statement at 22.

B. The District Court Erred by Categorically Denying Immunity to Foreign Entities

1. So-Called "Derivative Sovereign Immunity" for Private Agents Is Not Distinct from Conduct-Based Immunity

The district court treated NSO as raising a second ground for immunity in addition to conduct-based immunity, namely "derivative sovereign immunity, as discussed in [the Fourth Circuit's decision in] *Butters*." ER 11 n.1. The court expressed reluctance to adopt this supposedly distinct form of immunity, stating that this Court has not recognized it. ER 13–14. And the court ultimately held that, even if derivative sovereign immunity exists as a distinct form of immunity, it protects only entities incorporated in the United States. ER 14–15. Because NSO is an Israeli corporation, the court denied it immunity. *Id.*

This line of reasoning, however, was mistaken from the first step. "Derivative sovereign immunity" is not, as the district court believed, a

distinct theory of immunity. It is merely another name for conduct-based immunity, which protects agents of foreign states—including private agents—for actions they take in their capacity as agents. *Supra* at 5–16. Such agents' immunity could be described as "derivative," in the sense that private agents of foreign states are immune because they are acting on behalf of immune foreign states; but the immunity is nonetheless conduct-based, in that it applies only where the private, non-sovereign actor is acting in its capacity as an agent of a foreign state. *Ivey*, 2018 WL 3764264, at *6.

Contrary to the district court's reading of *Butters*, ER 12–13, that case did not present derivative sovereign immunity as distinct from conduct-based immunity. *Butters*, 225 F.3d at 466. Instead, the Fourth Circuit primarily relied on *Alicog*, *id.*, which cited common law and the FSIA to hold that foreign "governmental agents" are immune for actions "within the scope of their employment." *Alicog*, 860 F. Supp. at 382, 384–85. While the Fourth Circuit also found support in U.S. contractors' domestic derivative immunity, it did so mostly by analogy. *Butters*, 225 F.3d at 466. It left no doubt that the ultimate basis for its holding was the law of *foreign*, not domestic, sovereign immunity. *See id.* (awarding

"derivative immunity under the FSIA"). That holding, as with other pre-*Samantar* decisions applying the FSIA, remains "instructive for post-*Samantar* questions of common law immunity." *Yousuf*, 699 F.3d at 774. While those pre-*Samantar* courts erred to the extent they relied on the FSIA as a positive-law grant of immunity to private actors, the Supreme Court made clear that the pre-FSIA common law of foreign sovereign immunity continues to apply to actors whose immunity is not governed by the FSIA. *Samantar*, 560 U.S. at 324–25.

Indeed, later decisions that follow *Butters* to immunize private foreign agents do so explicitly based on common-law conduct-based immunity. *See Ivey*, 2018 WL 3764264, at *2, 6–7 (holding, based on *Butters*, that private foreign agent was "protected by foreign official immunity"); *Moriah*, 107 F. Supp. 3d at 277 & n.35 (holding, based on *Butters*, that "conduct-based immunity . . . extends beyond current and former government officials to individuals acting as an agent for the government"). The district court here disregarded *Moriah*'s reliance on *Butters* because *Moriah* "applied the 'two-step procedure to assess common-law claims of foreign sovereign immunity.'" ER 15 n.3 (internal quotation marks omitted); *see supra* at 5–6 (explaining that two-step

procedure). But that is precisely the point. *Moriah*'s reliance on common-law immunity does not reflect a failure to "discuss the distinction between derivative foreign sovereign immunity and foreign official immunity." ER 15 n.3. It confirms that there *is no such distinction*. "Derivative sovereign immunity" and "conduct-based immunity" are just two labels for the same common-law doctrine.

2. Conduct-Based Immunity Protects Both Foreign and American Entities

Without its mistaken distinction between conduct-based immunity and derivative sovereign immunity, the district court's reasons for rejecting derivative sovereign immunity evaporate. It doesn't matter whether this Court has recognized "the doctrine of derivative sovereign immunity," ER 13, because it *has* recognized the identical doctrine of "conduct-based immunity." *Doğan*, 932 F.3d at 893–94. And because the district court did not dispute that conduct-based immunity protects private foreign agents, *see* ER 11, its exclusion of foreign entities from "derivative sovereign immunity," ER 14–15, makes no difference to this case. As explained above, NSO is entitled to conduct-based immunity notwithstanding its status as an Israeli corporation. *Supra* at 30–33.

Beyond that, there is no good reason to approve the district court's denial of immunity, however labeled, to foreign entities. While the agents in *Alicog*, *Butters*, and *Ivey* happened to be U.S. residents, the agent in *Moriah* was Israeli. None of these cases held that the agent's nationality was relevant to the existence of immunity. To the contrary, they recognize that foreign sovereigns "need flexibility to hire private agents to aid them in conducting their government functions." *Butters*, 225 F.3d at 466. Conditioning immunity on whether a foreign state hired an American or foreign agent would limit that flexibility. And it would be quite odd for an immunity doctrine that protects *foreign* states and *foreign* officials to somehow exclude *foreign* entities.

If anything, American entities should be *less* entitled to foreign sovereign immunity than foreign entities. The United States has treated a defendant's U.S. residency as a reason to deny conduct-based immunity because "U.S. residents . . . who enjoy the protections of U.S. law ordinarily should be subject to the jurisdiction of our courts." *Samantar II* Amicus Br. at 5; *Yousuf*, 699 F.3d at 767; *see Broidy Cap. Mgmt LLC v. Muzin*, 2020 WL 1536350, at *6–7 (D.D.C. Mar. 31, 2020) (denying "derivative sovereign immunity" to U.S. defendants because State

Department "would not recognize immunity" for "U.S. citizen[s] who reside[] in the United States"). That is all the more true of American corporations, which are not just protected by domestic law, but owe their very existence to it. *CTS Corp. v. Dynamics Corp. of Am.*, 481 U.S. 69, 94 (1987). This rationale for exercising jurisdiction over U.S. residents does not apply to foreign corporations like NSO, which is a creature of Israeli law subject to extensive regulation in Israel. ER 52–55 ¶¶ 4–9, 12, 14.

The district court flipped this reasoning on its head, suggesting that immunity should uniquely encourage the use of American corporations to perform foreign contracts. ER 15. But this protectionist "Buy American" rationale contradicts the "principles of comity between nations" that ground conduct-based immunity. *Chuidian*, 912 F.2d at 1104. Just like the United States, foreign states employ private contractors to assist intelligence operations, investigate terrorism, and "learn details of criminal plots." Lieber et al., *supra*. Extending immunity to the American entities while withholding it from foreign entities hardly treats these foreign states "as equals." *Jones*, UKHL 26 ¶ 1.

Such unequal treatment of foreign and domestic entities could seriously interfere with the United States' foreign policy. Since the

Revolutionary War, the United States has relied on private agents to support its intelligence and military operations. Glenn J. Voelz, *Contractors and Intelligence: The Private Sector in the Intelligence Community*, 22 Int'l J. Intelligence & CounterIntelligence 586, 588–91 (2009). Today, the United States often has "no choice but to use contractors for work that may be borderline 'inherently governmental.'" Office of the Director of National Intelligence, *The U.S. Intelligence Community's Five Year Strategic Human Capital Plan* 6 (June 2006). Some 70,000 private contractors support U.S. intelligence operations, with a quarter of those contractors "directly involved in core intelligence mission functions." Voelz, *supra*, at 587. And "as many as sixty private firms provide[] various security and intelligence-related services in Iraq and Afghanistan," *id.* at 588, performing "tasks once performed only by military members" in locations "closer to the battlespace than ever before," Lisa L. Turner & Lynn G. Norton, *Civilians at the Tip of the Spear*, 51 A.F. L. Rev. 1, 8 (2001).

If U.S. courts deny immunity to foreign states' foreign agents, then those states may retaliate by exercising jurisdiction over lawsuits against the United States' many private contractors. Such lawsuits would

implicate "[m]atters intimately related to foreign policy and national security," which "are rarely proper subjects for judicial intervention." *Haig v. Agee*, 453 U.S. 280, 292 (1981); *see Carmichael v. Kellogg, Brown & Root Servs., Inc.*, 572 F.3d 1271, 1275 (11th Cir. 2009) (noting that claim against military contractor "would require extensive reexamination and second-guessing of many sensitive judgments surrounding the conduct of a military convoy"). The United States' international rivals could, therefore, turn to their courts to disrupt the United States' military and intelligence operations through lawsuits against U.S. contractors.

That is, in fact, what WhatsApp seeks to do to foreign states in this case. It wants to prevent foreign states from using NSO's technology to advance their sovereign interests in crime prevention and national security. Conduct-based immunity exists to prevent such meddling in foreign states' affairs. The district court erred in holding otherwise. This Court should reverse.

CONCLUSION

The Court should reverse the district court's denial of NSO's motion to dismiss and hold that NSO is entitled to foreign sovereign immunity.

Respectfully submitted,

/s/ Joseph N. Akrotirianakis
Joseph N. Akrotirianakis
KING & SPALDING LLP
633 W. 5th Street
Suite 1600
Los Angeles, CA 90071
jakro@kslaw.com

Counsel for Appellants NSO Group Tech. Ltd. et al.

November 16, 2020

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify that:

1. This document complies with the type-volume limitation of Circuit Rule 32-1 because it contains 9,864 words, excluding the parts exempted by Fed. R. App. P. 32(f).

2. This document complies with the typeface and type-style requirements of Fed. R. App. P. 32(a)(5) because it has been prepared in a proportionally spaced typeface using Century Schoolbook size 14-point font with Microsoft Word.

Date: November 16, 2020

/s/ Joseph N. Akrotirianakis
Joseph N. Akrotirianakis

Counsel for Appellants

CERTIFICATE OF SERVICE

I hereby certify that on November 16, 2020, I caused the foregoing to be electronically filed with the Clerk of the Court for the United States 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.

/s/ Joseph N. Akrotirianakis
Joseph N. Akrotirianakis

Counsel for Appellants