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' PETITION FOR REHEARING OR REHEARING EN BANC

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 22, 2021

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

Other Authorities

INTRODUCTION AND RULE 35 STATEMENT

Appellees Facebook and WhatsApp (collectively "WhatsApp") brought this lawsuit to restrict how foreign countries may conduct their law-enforcement, intelligence, and national-security operations. Appellant NSO Group Technologies Ltd. designs technology and licenses it to foreign nations for use to investigate criminals who rely on encrypted messaging to plan acts of terrorism, child exploitation, bank robbery, weapons trafficking, and other serious crimes. WhatsApp does not like that. It has told this Court that governments should not be allowed to use surveillance software developed by private companies.

That is why WhatsApp brought this lawsuit against NSO. WhatsApp knows it cannot directly sue the foreign states and officials who conduct investigations using NSO's technology. So it chose 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 NSO's business. These undisputed facts establish that NSO acts entirely in an "official capacity" as an "agent[] of foreign governments." ER 11.

NSO therefore moved to dismiss WhatsApp's complaint, arguing that it is immune from suit under the common-law doctrine—known as "conduct-based immunity"—that protects foreign agents from suit. It is undisputed that conduct-based immunity protects the private agents of foreign states for actions they take in their official capacity as agents. The question in this appeal is whether conduct-based immunity protects only private *individuals*, or whether, under appropriate circumstances, it also protects private *entities*.

The correct answer to that question is that conduct-based immunity covers private entities. But the district court denied NSO immunity, and a three-judge panel of this Court affirmed in a published opinion. In doing so, however, the panel endorsed none of the district court's reasoning. Op. 5. Instead, the panel adopted a novel and sweeping position that no other court has adopted: that private entities are *categorically* ineligible for conduct-based immunity because the Foreign Sovereign Immunities Act ("FSIA") entirely supplants common-law immunity for entities. Op. 14.

If the panel does not grant rehearing, the full Court should grant rehearing en banc and review the panel's decision. First, whether private entities may receive conduct-based immunity is "a question of exceptional importance" that affects the ability of sovereign nations—including the United States—to conduct core sovereign activities without interference from foreign courts. Fed. R. App. P. 35(a)(2). The question has divided the federal Courts of Appeals, with three Circuits (including this one) taking different approaches. Second, the panel's novel holding—that the FSIA entirely displaces the common law as applied to entities—"conflicts with" the Supreme Court's decision in *Samantar v. Yousuf*, 560 U.S. 305 (2010). Fed. R. App. P. 35(b)(1)(A). Rehearing en banc is warranted for these reasons.

STATEMENT OF THE CASE

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 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 abilities, 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 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. Some WhatsApp users are violent criminals and terrorists who exploit WhatsApp's encryption to avoid detection. 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 thus enables sovereign governments to prevent terrorism and violent crime when WhatsApp is unwilling to do so itself.

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 and state law.

NSO moved to dismiss. 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. ER 11. In support, NSO submitted evidence—including a declaration from its CEO—proving that its "sovereign customers . . . operate the technology themselves, to advance their own sovereign interests," while NSO provides only limited "advice and technical support," "entirely at

the direction of [its] government customers." ER 54–55 ¶ 14. WhatsApp did not submit any contrary evidence. ER 11.

The district court nonetheless rejected NSO's immunity defense. 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. The court ruled, however, that NSO did not qualify for conduct-based foreign official immunity because a judgment against NSO would not bind any foreign sovereign. ER 12. The district court also held that so-called "derivative sovereign immunity," which it treated as a separate theory of immunity, protects only American companies. ER 13–14.

3. NSO timely appealed, ER 46, and a panel of this Court affirmed. The panel did not, however, endorse either of the grounds relied on by the district court. Op. 5. Instead, it adopted a novel argument that WhatsApp raised for the first time on appeal: that private entities are categorically ineligible for conduct-based immunity because the FSIA entirely displaces the common law as applied to entities. Op. 14–18.

ARGUMENT

I. This Case Presents an Issue of Exceptional Importance That Has Divided the Courts of Appeals.

A. It is undisputed that, for more than 200 years, the common law has afforded conduct-based immunity to foreign officials and other agents acting on a foreign state's behalf. Statement of Interest of the United States of America at 6–10, *Matar v. Dichter*, No. 05-cv-10270 (S.D.N.Y. Nov. 17, 2006) ("*Matar* Statement"); *see, e.g.*, *Underhill v. Hernandez*, 168 U.S. 250, 252 (1897); *Mireskandari v. Mayne*, 800 F. App'x 519, 519 (9th Cir. 2020); *Doğan v. Barak*, 932 F.3d 888, 893–94 (9th Cir. 2019); *Matar v. Dichter*, 563 F.3d 9, 14 (2d Cir. 2009); *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).

It is similarly undisputed that conduct-based immunity extends to *private* individuals when they act in their capacity as foreign agents. Although private agents seek immunity somewhat less often than foreign officials, courts have uniformly held that private individuals may assert conduct-based immunity. *See Butters v. Vance Int'l, Inc.*, 225 F.3d 462, 466 (4th Cir. 2000); *Alicog v. Kingdom of Saudi Arabia*, 79 F.3d 1145 (5th Cir. 1996) (table), *affirming Alicog v. Kingdom of Saudi Arabia*, 860 F.

Supp. 379, 384–85 (S.D. Tex. 1994); *Ivey ex rel. Carolina Golf Dev. Co. v. Lynch*, 2018 WL 3764264, at *6–7 (M.D.N.C. Aug. 8, 2018); *Moriah v. Bank of China*, 107 F. Supp. 3d 272, 277–78 (S.D.N.Y. 2015). Whether the agent is public or private, "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).

B. The question in this appeal is whether the conduct-based immunity that undisputedly protects private *individuals* can also protect private *entities*. The panel held that private entities can never, under any circumstances, claim conduct-based immunity under the common law. Op. 18. That sweeping holding has exceptionally important implications for how the United States and other nations conduct core sovereign activities.

Common-law immunity is "a matter of comity." *Rep. of Austria v. Altmann*, 541 U.S. 677, 688 (2004); *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.'"). For one nation's courts to exercise jurisdiction over the official acts of another

nation's agents "would destroy, not enhance that comity." *Belhas v. Ya'alon*, 515 F.3d 1279, 1286 (D.C. Cir. 2008). The United States has thus 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." Brief for the United States as Amicus Curiae at 16, *Mutond v. Lewis*, No. 19-185 (U.S. May 26, 2020).

This concern extends to private entities. "All sovereigns need flexibility to hire private agents to aid them in conducting governmental functions," which includes hiring private entities when appropriate. *Butters*, 225 F.3d at 466. Indeed, the United States has relied on private agents to support its intelligence and military operations since the Revolutionary War. 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[d] 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 categorically deny immunity to foreign states' private entity agents, then those states can retaliate by exercising jurisdiction over lawsuits against the United States' many 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). That is why the United States has reserved the right to argue that its entity "contractor[s] should be sheltered by . . . sovereign immunity in an adjudication in a foreign or international court." Brief for the United States as Amicus Curiae at 10 n.1, *CACI Premier Tech., Inc. v. Shimari*, No. 19-648 (U.S. Aug. 26, 2020). The panel decision takes that important argument away from the United States, exposing U.S. contractors to

foreign suits designed to interfere with sovereign U.S. military and intelligence operations.

C. The important question of whether conduct-based immunity can protect private entities has divided the federal Courts of Appeals. The Fourth Circuit has granted conduct-based immunity to a private entity, and the D.C. Circuit has allowed private entities to *seek* conduct-based immunity. The panel decision here is the only one to ever hold that private entities are categorically excluded from conduct-based immunity.

First, the Fourth Circuit held in *Butters v. Vance Int'l, Inc.*, 225 F.3d 462, 466 (4th Cir. 2000), that a private entity was immune for providing security services to Saudi Arabia. Although the Fourth Circuit arguably described that immunity as deriving from the FSIA, it applied the test for conduct-based immunity, holding that private agents are immune "when following the commands of a foreign sovereign employer." *Id.* And it held that private entities could receive that immunity because "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.* This holding, even if phrased in terms of FSIA immunity, is "instructive for . . . questions of common law immunity."

Yousuf v. Samantar, 699 F.3d 763, 774 (4th Cir. 2012); *see Ivey*, 2018 WL 3764264, at *2, 6–7 (interpreting *Butters* as granting conduct-based immunity); *Moriah*, 107 F. Supp. 3d at 277 & n.34 (same); Ved P. Nanda et al., 1 *Litigation of International Disputes in U.S. Courts* § 3:59 n.132 (Dec. 2020 update) (same); Hazel Fox & Philippa Webb, *The Law of State Immunity* 444, 453 (3d ed. 2013) (same).

More recently, the D.C. Circuit treated conduct-based immunity as available to private entities. *Broidy Cap. Mgmt. LLC v. Muzin*, 12 F.4th 789 (D.C. Cir. 2021). In that case, private entities sought immunity for work they allegedly performed for Qatar. The D.C. Circuit rejected immunity for factual reasons, holding that the entities had not introduced the necessary evidence to show that they "act[ed] as [Qatar's] agents to carry out any sovereign functions" or that "Qatar requested, approved, or even knew of the unlawful conduct." *Id.* at 800. But the court treated entities as eligible for common-law immunity, *id.* at 802 (stating that common-law immunity applies to "private entities or individuals"), and the panel here criticized the D.C. Circuit for its "summary assertion that a private *entity* can seek immunity under the common law despite the FSIA." Op. 16 n.5.

The panel decision here took a completely different approach, holding that private entities can *never* seek conduct-based immunity. These conflicting approaches to an exceptionally important question of law justify en banc review. Fed. R. Civ. P. 35(b)(1)(B); Cir. R. 35-1.

II. The Panel's Decision Conflicts with the Supreme Court's Decision in *Samantar*.

The panel here did not deny that, under the common law, private individuals could claim conduct-based immunity. But it held that the FSIA entirely displaces that common law with respect to entities, categorically excluding entities from conduct-based immunity. That holding is incorrect and inconsistent with the Supreme Court's decision in *Samantar*.

Congress passed the FSIA to codify only *some* aspects of common-law foreign sovereign immunity. It is a specific and narrow statute that governs only "whether a *foreign state* is entitled to sovereign immunity." *Samantar*, 560 U.S. at 313 (emphasis added). Its definition of "foreign state" thus incorporates entities that, because they are state-owned "agenc[ies] or instrumentalit[ies]," are equivalent to foreign states. *Id.* at 314; 28 U.S.C. § 1603(a)–(b). But that definition limits only which entities possess immunity *as foreign states* under the FSIA. *Samantar* held that

when a plaintiff sues a defendant that is not "a foreign state as the [FSIA] defines that term," the FSIA has no force. *Samantar*, 560 U.S. at 325. Those suits are "governed by the common law." *Id.*

Private entities are not "foreign state[s] as the [FSIA] defines that term." *Id.* Under *Samantar*, therefore, the FSIA has nothing to say about whether private entities may receive conduct-based immunity. That depends entirely on the common law, which Congress did not "intend[] the FSIA to supersede." *Id.* at 320.

The panel's response to these points departed from how *Samantar* described both the FSIA and the common law. The panel reasoned that the FSIA does not extend foreign sovereign immunity to "actors that are neither sovereigns themselves nor . . . acting on behalf of a sovereign." Op. 15. True enough, but that does not support the panel's conclusion. Under *Samantar*, the FSIA addresses only entities that, because of their relationship to a foreign state, *are* "sovereigns themselves." *Id.*; *see Samantar*, 560 U.S. at 314. The FSIA does not address entities or individuals that seek immunity because they "act[ed] on behalf of a sovereign." Op. 15. Those claims for immunity are covered by the common law, which the FSIA did not disturb. *Samantar*, 560 U.S. at 320.

Because of the FSIA's limited focus on "foreign state[s]," *Samantar*, 560 U.S. at 325, the panel's invocation of the *expressio unius exclusio alterius* canon is beside the point, Op. 15. It is no doubt correct that the FSIA "create[ed] a 'comprehensive set of legal standards governing claims of immunity . . . *against a foreign state or its political subdivisions, agencies or instrumentalities*.'" Op. 15–16 (quoting *Verlinden B.V. v. Cent. Bank of Nigeria*, 461 U.S. 480, 487 (1983)) (emphasis added). That is why NSO has never claimed immunity *under the FSIA*. But the panel did not and could not deny that conduct-based immunity protects more than "foreign state[s] or [their] political subdivisions." *Id.* And *Samantar* could not have been clearer that the FSIA simply does not apply to defendants that are not "foreign state[s] as the [FSIA] defines that term." *Samantar*, 560 U.S. at 325. If the FSIA does not apply, it cannot bar NSO's claim of immunity.

Because NSO is not a "foreign state" under the FSIA, *Samantar* forecloses the panel's holding that the FSIA supersedes conduct-based immunity under the common law. That "conflict[] with a decision of the United States Supreme Court" supports en banc review. Fed. R. App. P. 35(b)(1)(A).

CONCLUSION

The Court should grant rehearing or rehearing en banc.

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 22, 2021

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g) and Cir. R. 40-1(a), I certify that:

1. This document complies with the type-volume limitation of Circuit Rule 40-1(a) because it contains 3,160 words.

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 22, 2021

/s/ Joseph N. Akrotirianakis
Joseph N. Akrotirianakis

Counsel for Appellants

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

WHATSAPP INC., a Delaware corporation; FACEBOOK, INC., a Delaware corporation, *Plaintiffs-Appellees*, v. NSO GROUP TECHNOLOGIES LIMITED; Q CYBER TECHNOLOGIES LIMITED, *Defendants-Appellants*.	No. 20-16408 D.C. No. 4:19-cv-07123-PJH OPINION

Appeal from the United States District Court
for the Northern District of California
Phyllis J. Hamilton, District Judge, Presiding

Argued and Submitted April 12, 2021
San Francisco, California

Filed November 8, 2021

Before: Mary H. Murguia, Ryan D. Nelson, and Danielle J. Forrest, Circuit Judges.

Opinion by Judge Forrest

SUMMARY*

Foreign Sovereign Immunity

The panel affirmed the district court's order denying a private Israeli corporation's motion to dismiss, based on foreign sovereign immunity, an action brought under the Computer Fraud and Abuse Act and California state law.

WhatsApp Inc. and Facebook, Inc., alleged that defendant, a privately owned and operated Israeli corporation, sent malware through WhatsApp's server system to mobile devices.

The panel held that it had jurisdiction under the collateral order doctrine to review the district court's order denying defendant's motion to dismiss based on a claim of immunity from suit.

The panel held that the Foreign Sovereign Immunity Act occupies the field of foreign sovereign immunity and categorically forecloses extending immunity to any entity that falls outside the Act's broad definition of "foreign state." The panel rejected defendant's argument that it could claim foreign sovereign immunity under common-law immunity doctrines that apply to foreign officials. The panel stated that there was no indication that the Supreme Court in *Samantar v. Yousuf*, 560 U.S. 305 (2010), intended to extend foreign official immunity to entities. Moreover, the FSIA's text, purpose, and history demonstrate that Congress

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

displaced common-law sovereign immunity as it relates to entities. The panel therefore affirmed the district court's order.

COUNSEL

Jeffrey S. Bucholtz (argued), King and Spalding LLP, Washington, D.C.; Matthew V.H. Noller, King and Spalding LLP, Sacramento, California; Joseph N. Akrotirianakis, King and Spalding LLP, Los Angeles, California; for Defendants-Appellants.

Michael R. Dreeben (argued), O'Melveny & Myers LLP, Washington, D.C.; Yaira Dubin, O'Melveny & Myers LLP, New York, New York; for Plaintiffs-Appellees.

Mark Parris, Carolyn Frantz, Paul Rugani, and Alyssa Barnard-Yanni, Orrick Herrington & Sutcliffe LLP, Seattle, Washington; for Amici Curiae Microsoft Corp., Cicsco Systems Inc., Github Inc., LinkedIn Corporation, VMWare Inc., and Internet Association.

Michael Trinh, Google LLC, Mountain View, California, for Amicus Curiae Google LLC.

Sophia Cope and Andrew Crocker, Electronic Frontier Foundation, San Francisco, California, for Amicus Curiae Electronic Frontier Foundation.

Elaine Goldenberg, Munger Tolles & Olson LLP, Washington, D.C.; Marianna Mao, Munger Tolles & Olson LLP, San Francisco, California; David Kaye, Irvine, California; for Amicus Curiae David Kaye.

Kyle A. McLorg, Stephanie Skaff, and Deepak Gupta, Farella Braun & Martel LLP, San Francisco, California, for Amici Curiae Access Now, Amnesty International, Committee to Protect Journalists, Internet Freedom Foundation, Paradigm Initiative, Privacy International, Red en Defensa de los Derechos Digitales, and Reporters Without Borders.

Geoffrey M. Klineberg and Bethan R. Jones, Kellogg Hansen Todd Figel & Frederick PLLC, Washington, D.C., for Amicus Curiae Foreign Sovereign Immunity Scholars.

OPINION

FORREST, Circuit Judge:

The question presented is whether foreign sovereign immunity protects private companies. The law governing this question has roots extending back to our earliest history as a nation, and it leads to a simple answer—no. Indeed, the title of the legal doctrine itself—*foreign sovereign* immunity—suggests the outcome.

Plaintiffs-Appellees WhatsApp Inc. and Facebook, Inc. (collectively WhatsApp) sued Defendants-Appellants NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. (collectively NSO), alleging that NSO, a privately owned and operated Israeli corporation, sent malware through WhatsApp's server system to approximately 1,400 mobile devices, breaking both state and federal law. NSO argues foreign sovereign immunity protects it from suit and, therefore, the court lacks subject matter jurisdiction. Specifically, NSO contends that even if WhatsApp's allegations are true, NSO was acting as an agent of a foreign

state, entitling it to "conduct-based immunity"—a common-law doctrine that protects foreign officials acting in their official capacity.

The district court rejected NSO's argument, concluding that common-law foreign official immunity does not protect NSO from suit in this case. We agree that NSO is not entitled to immunity in this case, but we reach this conclusion for a different reason than did the district court. We hold that the Foreign Sovereign Immunity Act (FSIA or Act) occupies the field of foreign sovereign immunity as applied to *entities* and categorically forecloses extending immunity to any entity that falls outside the FSIA's broad definition of "foreign state." And we reject NSO's argument that it can claim foreign sovereign immunity under common-law immunity doctrines that apply to foreign officials—i.e., natural persons. *See Samantar v. Yousuf*, 560 U.S. 305, 315–16 (2010). There is no indication that the Supreme Court intended to extend foreign *official* immunity to entities. Moreover, the FSIA's text, purpose, and history demonstrate that Congress displaced common-law sovereign immunity doctrine as it relates to entities. *See Native Vill. of Kivalina v. ExxonMobile Corp.*, 696 F.3d 849, 856 (9th Cir. 2012) ("Federal common law is subject to the paramount authority of Congress.").

I. BACKGROUND

NSO is an Israeli company that designs and licenses surveillance technology to governments and government agencies for national security and law enforcement purposes. One of NSO's products—a program named Pegasus—"enables law enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device." Pegasus users may intercept messages, take screenshots, or exfiltrate a device's contacts

or history. NSO claims that it markets and licenses Pegasus to its customers,[1] which then operate the technology themselves. According to NSO, its role "is limited to . . . providing advice and technical support to assist customers in setting up—not operating—the Pegasus technology."

WhatsApp provides an encrypted communication service to the users of its application. Because of its encryption technology, every type of communication (telephone calls, video calls, chats, group chats, images, videos, voice messages, and file transfers) sent using WhatsApp on a mobile device can be viewed only by the intended recipient. WhatsApp asserts that NSO used WhatsApp's servers without authorization to send "malicious code" to approximately 1,400 WhatsApp users. The malicious code was allegedly designed to infect the targeted devices for the purpose of surveilling the device users.

In October 2019, WhatsApp sued NSO in federal district court. 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. WhatsApp alleged that NSO intentionally accessed WhatsApp servers without authorization to figure out how to place Pegasus on WhatsApp users' devices without detection. WhatsApp sought an injunction restraining NSO from accessing WhatsApp's servers, violating WhatsApp's terms, and

[1] WhatsApp contends that NSO's customers are not limited to foreign governments. Whether this is true or not is immaterial to the outcome of this case.

impairing WhatsApp's service. WhatsApp also sought compensatory, statutory, and punitive damages.

NSO moved to dismiss the complaint. As relevant here, NSO asserted that the court lacked subject matter jurisdiction because NSO was acting at the direction of its foreign government customers and is protected from suit under foreign sovereign immunity. The district court denied NSO's motion. Relying on the Restatement (Second) of Foreign Relations Law § 66, the district court concluded that NSO was not entitled to common-law conduct-based foreign sovereign immunity because it failed to show that exercising jurisdiction over NSO would serve to enforce a rule of law against a foreign state. This interlocutory appeal followed.

II. DISCUSSION

A. Interlocutory Jurisdiction

As a threshold matter, WhatsApp argues that we lack jurisdiction over this interlocutory appeal because the district court's order is not a final appealable order. "We review questions of our own jurisdiction *de novo*." *Hunt v. Imperial Merch. Servs., Inc.*, 560 F.3d 1137, 1140 (9th Cir. 2009) (citation omitted).

We have jurisdiction over "final decisions of the district courts." 28 U.S.C. § 1291. Under the collateral-order doctrine, a small class of interlocutory orders qualifies as "final decisions." *See Cohen v. Beneficial Indus. Loan Corp.*, 337 U.S. 541, 545–46 (1949). To be an appealable collateral order, the decision must "[1] conclusively determine the disputed question, [2] resolve an important issue completely separate from the merits of the action, and [3] be effectively unreviewable on appeal from a final judgment." *P.R. Aqueduct & Sewer Auth. v. Metcalf & Eddy,*

Inc., 506 U.S. 139, 144 (1993) (citation omitted). WhatsApp contests only the third element—that the order is effectively unreviewable after final judgment.

A common example of an immediately appealable collateral order that is effectively unreviewable after final judgment is an interlocutory denial of certain immunities from suit. *SolarCity Corp. v. Salt River Project Agric. Improvement & Power Dist.*, 859 F.3d 720, 725 (9th Cir. 2017) (noting that the "Supreme Court has allowed immediate appeals from" interlocutory denials of Eleventh Amendment immunity, absolute and qualified immunity, foreign sovereign immunity, and tribal sovereign immunity). In contrast, denials of a "defense to liability" are not immediately appealable final orders. *Id.* at 725–26 (explaining that "[u]nlike immunity from suit, immunity from liability can be protected by a post-judgment appeal" and "therefore do[es] not meet the requirements for immediate appeal under the collateral-order doctrine").

The parties dispute whether common-law conduct-based foreign official immunity is an immunity from suit, entitling it to an interlocutory appeal, or a defense to liability that can only be appealed post-judgment. But all agree that foreign state sovereign immunity, now codified in the FSIA, is an immunity from suit and that an order denying a foreign state's claim of sovereign immunity is immediately appealable. *Compania Mexicana de Aviacion, S.A. v. U.S. Dist. Ct.*, 859 F.2d 1354, 1358 (9th Cir. 1988). Because we conclude that the FSIA governs NSO's claim of immunity, we have jurisdiction over this appeal under the collateral-order doctrine.

B. Foreign Sovereign Immunity

1. Origins of the Doctrine

Chief Justice John Marshall's opinion in *Schooner Exchange v. McFadden*, 7 Cranch 116; 3 L. Ed. 287 (1812), is credited with establishing foreign sovereign immunity in American law. *See Opati v. Republic of Sudan*, 140 S. Ct. 1601, 1605 (2020); *see also Schooner Exchange*, 7 Cranch at 136 (noting the Court was "exploring an unbeaten path, with few, if any, aids from precedents or written law"). Writing for the Court, he reasoned that a nation's jurisdiction within its own boundaries is "exclusive and absolute" and any limitations on such jurisdiction "must be traced up to the consent of the nation itself. They can flow from no other legitimate source." *Schooner Exchange*, 7 Cranch at 136. Chief Justice Marshall further explained that respecting, and claiming, the "perfect equality and absolute independence of sovereigns," the nations of the world have "wave[d] the exercise of a part of that complete exclusive territorial jurisdiction" in cases brought within their jurisdiction against a foreign sovereign and ministers of a foreign sovereign. *Id.* at 137–39; *Republic of Austria v. Altmann*, 541 U.S. 677, 688 & n.9 (2004).

From this origin—described as "the classical or virtually absolute theory of sovereign immunity," *Permanent Mission of India to the U.N. v. City of New York*, 551 U.S. 193, 199 (2007) (internal quotation marks and citation omitted)—"[t]he doctrine of foreign sovereign immunity developed as a matter of common law." *Samantar*, 560 U.S. at 311. During our early years as a country, the State Department took the lead in applying foreign sovereign immunity. *Id.*; *see also* Br. of Foreign Sovereign Immunity Scholars, 4–7, No. 20-16408. Essentially, when faced with an immunity claim brought by a foreign state or official, if the State

Department suggested immunity, a court would acquiesce. *Samantar*, 560 U.S. at 311–12. And if the State Department did not suggest immunity, the court's inquiry consisted of asking whether the State Department had a policy for recognizing sovereign immunity in similar circumstances. *Id.* So, the State Department, not the courts, was the primary arbiter of foreign sovereign immunity. And the State Department's general practice was to suggest immunity "in all actions against friendly sovereigns." *Id.* at 312.

2. The Foreign Sovereign Immunity Act

In the early 1950s, the State Department abandoned the absolute theory of foreign sovereign immunity and "join[ed] the majority of other countries by adopting the 'restrictive theory' of sovereign immunity." *Permanent Mission of India to the U.N.*, 551 U.S. at 199. Under this theory, foreign sovereign "'immunity is confined to suits involving the foreign sovereign's public acts, and does not extend to cases arising out of a foreign state's strictly commercial acts.'" *Samantar*, 560 U.S. at 312 (quoting *Verlinden B.V. v. Cent. Bank of Nigeria*, 461 U.S. 480, 487 (1983)). Congress recognized that "[u]nder international law, states are not immune from the jurisdiction of foreign courts insofar as their commercial activities are concerned." 28 U.S.C. § 1602. Unsurprisingly, the politics of international diplomacy, at times, caused the State Department to suggest granting immunity in cases where its new, restrictive theory would have dictated denial. *Samantar*, 560 U.S. at 312; *Verlinden B.V.*, 461 U.S. at 487. Inconsistent outcomes also occurred depending on whether an immunity claim was presented to the State Department or a court. *Verlinden B.V.*, 461 U.S. at 487–88.

Congress disapproved of this inconsistency and enacted the FSIA to promote uniformity. *Samantar*, 560 U.S. at 313.

As the Act explains, its purpose was twofold: (1) "endorse and codify the restrictive theory of sovereign immunity" that existed under international law, and (2) "transfer primary responsibility for deciding claims of foreign states to immunity from the State Department to the courts." *Id.* (internal quotation marks omitted); 28 U.S.C. § 1602. In Congress's view, placing the responsibility for deciding foreign sovereign immunity claims with courts "would serve the interests of justice and would protect the rights of both foreign states and litigants in the United States courts." 28 U.S.C. § 1602. And so, immunity determinations were no longer made in the Secretary's office but a courtroom.

The Supreme Court has addressed the purpose and scope of the FSIA on multiple occasions. In *Verlinden B.V.*, the Court addressed whether the FSIA exceeded the scope of Article III of the Constitution and concluded that the FSIA "contains a comprehensive set of legal standards governing claims of immunity in every civil action against a foreign state or its political subdivisions, agencies or instrumentalities." 461 U.S. at 488. Likewise, in *Republic of Austria*, the Court considered whether the FSIA governed pre-enactment conduct and stated that the FSIA "established a comprehensive framework for resolving *any* claim of sovereign immunity." 541 U.S. at 699 (emphasis added). Six years later, the Court addressed whether a foreign *official* comes within the FSIA's definition of "foreign state" and is, therefore, subject to the Act. *Samantar*, 560 U.S. at 313–14. Backing away from its prior expansive pronouncements concerning the scope of the FSIA, the Court interpreted the Act's definition of "foreign state" as not including *individual foreign officials* seeking immunity. *Id.* at 315–20. But the Court reiterated that the FSIA does govern the immunity of foreign state entities: "The FSIA was adopted . . . to address a modern world where foreign state enterprises are every day

participants in commercial activities, and to assure litigants that decisions regarding claims against states *and their enterprises* are made purely on legal grounds." *Id.* at 323 (emphasis added) (internal quotation marks and citation omitted). Considering that foreign sovereign immunity cases involving foreign officials were "few and far between" prior to the FSIA's enactment, the Court's initial expansive pronouncements concerning the scope of the Act are not surprising. *Id.*

For purposes of resolving the present case, it is worth retracing the Court's interpretative analysis in *Samantar*. The FSIA established that "'a foreign state shall be immune from the jurisdiction of the courts of the United States and of the States' except as provided in the Act." *Id.* at 313 (quoting 28 U.S.C. § 1604). Where it applies, the FSIA takes the entire field regarding application of immunity. If a party seeking immunity is a "foreign state," as defined in the Act, the FSIA "is the sole basis for obtaining jurisdiction" over that party. *Id.* at 314 (internal quotation marks and citation omitted). In such a case, it is improper for courts to consider common-law principles. *Native Vill. of Kivalina*, 696 F.3d at 856 ("[W]hen federal statutes directly answer the federal question, federal common law does not provide a remedy because legislative action has displaced the common law."). While "foreign state" could be defined as including only "a body politic that governs a particular territory," Congress defined it more broadly. *Samantar*, 560 U.S. at 314. Under the FSIA, "foreign state" includes a body politic, as well as its "political subdivisions, agencies, and instrumentalities." *Id.*; 28 U.S.C. § 1603(a). And "agency or instrumentality" is defined to include "*any entity* [that] is a separate legal person, corporate or otherwise and . . . which is an organ of a foreign state or political subdivision thereof, or a majority of whose shares or other ownership interest is owned by a

foreign state or political subdivision thereof." 28 U.S.C. § 1603(b) (emphasis added); *Samantar*, 560 U.S. at 316 ("Congress had corporate formalities in mind."); *see also EIE Guam Corp. v. Long Term Credit Bank of Japan, Ltd.*, 322 F.3d 635, 640 (9th Cir. 2003) (noting that an entity can be an organ of a foreign state even if it is involved in some commercial affairs). Given these defined terms, and the absence of *any* reference to individual foreign officials,[2] the Supreme Court held that Congress did not intend for the FSIA to govern immunity of foreign officials in part because "the types of defendants listed [in the FSIA] are *all entities*." *Samantar*, 560 U.S. at 317 (emphasis added).

3. Foreign Sovereign Immunity & Private Entities

Neither the Supreme Court nor this Court has answered whether an entity that does not qualify as a "foreign state" can claim foreign sovereign immunity under the common law. It is clear under existing precedent that such an entity cannot seek immunity under the FSIA. Whether such entity can sidestep the FSIA hinges on whether the Act took the entire field of foreign sovereign immunity as applied *to entities*, or whether it took the field only as applied to foreign *state* entities, as NSO suggests. The answer lies in the question. The idea that foreign sovereign immunity could

[2] We recognize that the FSIA literally includes "person" in the definition of "agency or instrumentality," but as the Supreme Court has explained, the phrase "separate legal person, corporate or otherwise" in § 1603(b)(1) "typically refers to the legal fiction that allows an entity to hold personhood separate from the natural persons who are its shareholders or officers." *Samantar*, 560 U.S. at 315. "It is similarly awkward to refer to a person as an 'organ' of the foreign state . . . . [And] the terms Congress chose simply do not evidence the intent to include individual officials within the meaning of 'agency or instrumentality.'" *Id.* at 315–16.

apply to non-state entities is contrary to the originating and foundational premise of this immunity doctrine. Moreover, there is no indication that Congress, in codifying the restrictive theory of foreign sovereign immunity to promote uniformity and ensure that immunity decisions are based on law rather than politics, intended to exempt an entire category of entities from its "comprehensive" regime. *See* 28 U.S.C. § 1603(b); *Republic of Austria*, 541 U.S. at 699. While the FSIA was silent about immunity for individual officials, that is not true for entities—quite the opposite. Thus, we hold that an entity is entitled to foreign sovereign immunity, if at all, only under the FSIA. If an entity does not fall within the Act's definition of "foreign state," it cannot claim foreign sovereign immunity. Period.

Before diving into the details, we go back to the beginning. Chief Justice Marshall explained that foreign sovereign immunity arises from the recognition of the "perfect equality and absolute independence of sovereigns." *Schooner Exchange*, 7 Cranch at 137. We give sovereign immunity to other nations as an act of "grace and comity," *Verlinden B.V.*, 461 U.S. at 486, so they will do the same for us. This cooperative acknowledgement that each nation has equal autonomy and authority promotes exchange and good relationships between nations. *See Schooner Exchange*, 7 Cranch at 137; *see also Siderman de Blake v. Republic of Argentina*, 965 F.2d 699, 718 (9th Cir. 1992) (quoting Chief Justice Marshall's discussion of the origins of sovereign immunity); *Butters v. Vance Int'l, Inc.*, 225 F.3d 462, 465 (4th Cir. 2000) ("[Sovereign] acts often have political, cultural, and religious components. Judicial interference with them would have serious foreign policy ramifications for the United States."). None of the purposes for recognizing foreign sovereign immunity are served by granting immunity to entities and actors that are neither

sovereigns themselves nor are not acting on behalf of a sovereign. Again, the very name of the doctrine—*foreign sovereign* immunity—reflects this truth. Congress did not displace this foundational premise when it enacted the FSIA. *See Samantar*, 560 U.S. at 320 n.13 ("Congress is understood to legislate against a background of common-law . . . principles" (omission in original) (internal quotation marks and citation omitted)).

As noted above, Congress could have limited the FSIA's reach to only "a body politic that governs a particular territory." *Id.* at 314. It did not. It expanded the FSIA's reach to "*any entity* [that] is a separate legal person, corporate or otherwise and . . . which is an organ of a foreign state or political subdivision thereof, or a majority of whose shares or other ownership interest is owned by a foreign state of political subdivision thereof." 28 U.S.C. § 1603(b) (emphasis added). In defining what qualifies as a "foreign state," the FSIA necessarily defines the scope of foreign sovereign immunity. An entity must be a sovereign or must have a sufficient relationship to a sovereign to claim sovereign-based immunity. Without such status or relationship, there is no justification for granting sovereign immunity. It is odd indeed to think that by not including a category of entity within its definition of "foreign state," Congress intended for such entities to have the ability to seek immunity outside its "comprehensive" statutory scheme. *See Republic of Austria*, 541 U.S. at 699.

This reasoning is supported by the *expressio unius exclusio alterius*[3] interpretive canon. In creating a "comprehensive set of legal standards governing claims of immunity . . . against a foreign state or its political

[3] The expression of one thing implies the exclusion of another.

subdivisions, agencies or instrumentalities," *Verlinden B.V.*, 461 U.S. at 488, Congress defined the types of foreign entities—including, specifically, foreign corporate entities[4]—that may claim immunity. 28 U.S.C. § 1603(b). The most reasonable interpretation then is that the definition of "foreign state" forecloses immunity for any entity falling outside such definition, particularly where "foreign state" is defined broadly.[5] *See Pfizer, Inc. v. Gov't of India*, 434 U.S. 308, 312–13 (1978) (noting that expansive statutory language matched the underlying statute's comprehensive nature); *Ingersoll-Rand Co. v. McClendon*, 498 U.S. 133, 138–39 (1990) (explaining that defining a term broadly underscored Congress's intent that the underlying statutory term be expansively applied). And the Supreme Court's holding in *Samantar* that individual foreign officials are not subject to the FSIA does not defeat this interpretation because, as the Court explained, the FSIA did not address, *at*

[4] The Supreme Court has recognized that in enacting the FSIA, "Congress was aware of settled principles of corporate law and legislated within that context." *Dole Food Co. v. Patrickson*, 538 U.S. 468, 474 (2003).

[5] The D.C. Circuit recently relied on the common law in denying foreign sovereign immunity to three United States citizens and a United States limited liability corporation. *Broidy Cap. Mgmt. LLC v. Muzin*, 12 F.4th 789, 798 (D.C. Cir. 2021). When summarizing *Samantar*, the court presumed without explanation that the common law applied to "private entities or individuals." *Id.* at 802. Unlike here, the parties in *Broidy* agreed that the FSIA did not apply; the defendants made only common-law arguments, and the defendant-entity was domestic, not foreign. *Id.* at 792; *see also NML Cap., Ltd.*, 573 U.S. at 142. The D.C. Circuit did not make an explicit finding that foreign sovereign immunity claims from foreign private entities should be analyzed under the common law, and it did not explain its summary assertion that a private *entity* can seek immunity under the common law despite the FSIA. *See Broidy*, 12 F.4th at 802.

all, immunity for individuals or natural persons. 560 U.S. at 319 ("Reading the FSIA as a whole, there is nothing to suggest we should read 'foreign state' in § 1603(a) to include an official acting on behalf of the foreign state, and much to indicate that this meaning was not what Congress enacted.").

Moreover, the Act's definition of "foreign state" cannot be divorced from the context that "[t]he FSIA was adopted . . . to address a modern world where foreign state enterprises are every day participants in commercial activities." *Id.* at 323 (emphasis added) (internal quotation marks and citation omitted). Congress prohibited applying foreign sovereign immunity to "strictly commercial acts." *Id.* at 312. So, a plaintiff who can show that a foreign entity—even a direct sovereign like the Welsh Government—was engaged in "a regular course of commercial conduct or a particular commercial transaction or act," 28 U.S.C. § 1603(d), may defeat a claim of immunity, *see Pablo Star Ltd. v. Welsh Gov't*, 961 F.3d 555, 560 (2d Cir. 2020), *cert. denied*, 141 S. Ct. 1069 (2021); 28 U.S.C. § 1605(a)(2). It makes little sense to conclude that the FSIA leaves open the possibility that a corporate entity *less* connected to a sovereign than those meeting the statutory definition of "foreign state" could seek immunity for commercial conduct under a different immunity doctrine while entities *more* connected to a sovereign—even a body politic itself—could not. Especially where the other immunity doctrine proffered, *foreign official* immunity, is as narrowly focused on natural persons as the FSIA is broadly focused on entities. *See Samantar*, 560 U.S. at 323 (finding "no reason to believe that Congress saw as a problem, or wanted to eliminate, the State Department's role in determinations regarding individual official immunity."). Instead, the omission of entities like NSO from the FSIA's definition of foreign states and their "political subdivisions,

agencies, and instrumentalities" reflects a threshold determination about the availability of foreign sovereign immunity for such entities: they never qualify.[6]

4. NSO's Foreign Sovereign Immunity Claim

Concluding that the FSIA governs all foreign sovereign immunity claims brought by entities, as opposed to individuals, makes this an easy case. NSO is a private corporation that designs spyware technology used by governments for law enforcement purposes. According to NSO, its Pegasus technology is a program that was "marketed only to and used only by sovereign governments" and it allowed those governments "to intercept messages, take screenshots, or exfiltrate a device's contacts or history."[7] NSO's clients choose how and when to use Pegasus, not NSO. NSO simply licenses the technology and provides "advice and technical support" at its customers' direction.

NSO does not contend that it meets the FSIA's definition of "foreign state," and, of course, it cannot. It is not itself a sovereign. 28 U.S.C. § 1603(a). It is not "an organ . . . or

[6] In *Butters*, the Fourth Circuit extended the doctrine of domestic derivative sovereign immunity, applicable to United States contractors, to a United States corporation acting as an agent of a foreign state. 225 F.3d at 466. *Butters* did not discuss whether this common-law doctrine also extends to *foreign* contractors acting on behalf of foreign states. In any event, it is unclear what remains of such reasoning where the Supreme Court has instructed that "any sort of immunity defense made by a foreign sovereign in an American court must stand on the Act's text. Or it must fall." *Republic of Argentina v. NML Cap., Ltd.*, 573 U.S. 134, 142 (2014).

[7] NSO alleges that its customers include the Kingdom of Bahrain, the United Arab Emirates, and Mexico.

political subdivision" of a sovereign. *Id.* § 1603(b)(2). Nor is a foreign sovereign its majority owner. *Id.* NSO is a private corporation that provides products and services to sovereigns—several of them. NSO claims that it should enjoy the immunity extended to sovereigns because it provides technology used for law-enforcement purposes and law enforcement is an inherently sovereign function. Whatever NSO's government customers do with its technology and services does not render NSO an "agency or instrumentality of a foreign state," as Congress has defined that term. Thus, NSO is not entitled to the protection of foreign sovereign immunity. And that is the end of our task. There is no need to analyze whether NSO is entitled to immunity under the common law and inquire how the State Department would resolve this case. *See WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 665 (N.D. Cal. 2020). Nor is it necessary to explain that neither the State Department nor any court has ever applied foreign official immunity to a foreign private corporation under the common law, although this is a compelling fact indeed.[8] The proper analysis begins and ends with the FSIA, the comprehensive framework Congress enacted for resolving any entity's

[8] There is not a single documented instance of the State Department recommending conduct-based immunity for a foreign private corporation. *See, e.g.*, Digest of U.S. Practice in International Law 2020, at 403–09 (CarrieLyn D. Guymon, ed.); Digest of U.S. Practice in International Law 2019, at 344–55 (CarrieLyn D. Guymon, ed.); Digest of U.S. Practice in International Law 2018, at 410–13 (CarrieLyn D. Guymon, ed.); Digest of U.S. Practice in International Law 2017, at 444–55 (CarrieLyn D. Guymon, ed.); Digest of U.S. Practice in International Law 2016, at 450–61 (CarrieLyn D. Guymon, ed.). Nor have we found any case contemplating the same.

claim of foreign sovereign immunity. *See Republic of Austria*, 541 U.S. at 699; *Samantar*, 560 U.S. at 319.

AFFIRMED.