

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 .....	ii
Introduction and Rule 35 Statement .....	1
Statement of the Case .....	3
Argument .....	8
I. This Case Presents an Issue of Exceptional Importance That Has Divided the Courts of Appeals .....	8
II. The Panel’s Decision Conflicts with the Supreme Court’s Decision in <i>Samantar</i> .....	14
Conclusion.....	17
Certificate of Compliance .....	i
Certificate of Service .....	ii

## TABLE OF AUTHORITIES

	Page(s)
<b>Cases</b>	
<i>Alicog v. Kingdom of Saudi Arabia</i> , 79 F.3d 1145 (5th Cir. 1996).....	8
<i>Alicog v. Kingdom of Saudi Arabia</i> , 860 F. Supp. 379 (S.D. Tex. 1994).....	8
<i>Belhas v. Ya’alon</i> , 515 F.3d 1279 (D.C. Cir. 2008).....	10
<i>Broidy Cap. Mgmt. LLC v. Muzin</i> , 12 F.4th 789 (D.C. Cir. 2021) .....	13
<i>Butters v. Vance Int’l, Inc.</i> , 225 F.3d 462 (4th Cir. 2000).....	8, 10, 12, 13
<i>Ivey ex rel. Carolina Golf Dev. Co. v. Lynch</i> , 2018 WL 3764264 (M.D.N.C. Aug. 8, 2018).....	9, 13
<i>Chuidian v. Philippine Nat’l Bank</i> , 912 F.2d 1095 (9th Cir. 1990).....	8
<i>Doğan v. Barak</i> , 932 F.3d 888 (9th Cir. 2019).....	8
<i>In re Estate of Ferdinand Marcos</i> , 25 F.3d 1467 (9th Cir. 1994).....	8
<i>Haig v. Agee</i> , 453 U.S. 280 (1981).....	11
<i>Matar v. Dichter</i> , 563 F.3d 9 (2d Cir. 2009) .....	8
<i>Mireskandari v. Mayne</i> , 800 F. App’x 519 (9th Cir. 2020) .....	8

<i>Moriah v. Bank of China</i> , 107 F. Supp. 3d 272 (S.D.N.Y. 2015).....	9, 13
<i>Rep. of Austria v. Altmann</i> , 541 U.S. 677 (2004) .....	9
<i>Samantar v. Yousuf</i> , 560 U.S. 305 (2010) .....	3, 14, 15, 16
<i>Siderman de Blake v. Rep. of Argentina</i> , 965 F.2d 699 (9th Cir. 1992).....	9
<i>Underhill v. Hernandez</i> , 168 U.S. 250 (1897) .....	8
<i>Yousuf v. Samantar</i> , 699 F.3d 763 (4th Cir. 2012).....	13
<b>Statutes and Rules</b>	
28 U.S.C. § 1603(a)–(b).....	14
Cir. R. 35-1 .....	14
Fed. R. App. P. 35(a)(2) .....	3
Fed. R. App. P. 35(b)(1)(A) .....	3, 16
Fed. R. Civ. P. 35(b)(1)(B) .....	14
<b>Other Authorities</b>	
Brief for the United States as Amicus Curiae, <i>CACI Premier Tech., Inc. v. Shimari</i> , No. 19-648 (U.S. Aug. 26, 2020).....	11
Brief for the United States as Amicus Curiae, <i>Mutond v. Lewis</i> , No. 19-185 (U.S. May 26, 2020) .....	10
Dan Sabbagh, <i>Call for Backdoor Access to WhatsApp as Five Eyes Nations Meet</i> , The Guardian (July 30, 2019, 3:32 p.m.) .....	5

Dipesh Gadher, *London Bridge Terror Attack Planned on WhatsApp*, Sunday Times (May 12, 2019, 12:01 a.m.)..... 5

Glenn J. Voelz, *Contractors and Intelligence: The Private Sector in the Intelligence Community*, 22 Int’l J. Intelligence & CounterIntelligence 586, 588–91 (2009)..... 10, 11

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.) ..... 5

Hazel Fox & Philippa Webb, *The Law of State Immunity* (3d ed. 2013) ..... 13

Hazel Fox, *The Law of State Immunity* (2d ed. 2008)..... 9

Lisa L. Turner & Lynn G. Norton, *Civilians at the Tip of the Spear*, 51 A.F. L. Rev. 1, 8 (2001)..... 11

National Intelligence, *The U.S. Intelligence Community’s Five Year Strategic Human Capital Plan* (June 2006) ..... 10

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.) ..... 6

Statement of Interest of the United States of America, *Matar v. Dichter*, No. 05-cv-10270 (S.D.N.Y. Nov. 17, 2006) ..... 8

Ved P. Nanda et al., 1 *Litigation of International Disputes in U.S.* (Dec. 2020 update) ..... 13

## 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*