

No. 25-7380

---

IN THE UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

---

WhatsApp, et al.,

*Plaintiff-Appellee,*

v.

NSO Group Technologies Limited, et al.

*Defendant-Appellant.*

---

ON APPEAL FROM THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

No. 4:19-cv-07123

The Honorable Phyllis Jean Hamilton

---

**BRIEF OF ACCESS NOW; AGORA INTERNATIONAL HUMAN RIGHTS  
GROUP; CENTER FOR DEMOCRACY & TECHNOLOGY; COMMITTEE  
TO PROTECT JOURNALISTS; CYBERPEACE INSTITUTE; DATA  
RIGHTS; ELECTRONIC FRONTIER FOUNDATION; INTERNATIONAL  
JUSTICE CLINIC AT THE UNIVERSITY OF CALIFORNIA, IRVINE,  
SCHOOL OF LAW; MEDIA DEFENCE; PRIVACY INTERNATIONAL;  
AND REPORTERS WITHOUT BORDERS AS *AMICI CURIAE* IN  
SUPPORT OF PLAINTIFF-APPELLEE**

---

Andreas T. Kaltsounis  
Jacob T. Wall  
King O. Xia  
Baker & Hostetler, LLP  
999 3rd Ave, Suite 3900  
Seattle, WA 98104  
(206) 566-7080  
akaltsounis@bakerlaw.com  
*Counsel for Amici Curiae*

## **CORPORATE DISCLOSURE STATEMENT**

Pursuant to Rules 26.1 and 29(a)(4)(A) of the Federal Rules of Appellate Procedure, *Amici Curiae* Access Now; Agora International Human Rights Group; Center for Democracy and Technology; Committee to Protect Journalists; CyberPeace Institute; Data Rights; Electronic Frontier Foundation; International Justice Clinic at the University of California, Irvine, School of Law; Media Defence; Privacy International; and Reporters Without Borders state that no party to this brief is a publicly held corporation, issues stock, or has a parent corporation.

Dated: May 20, 2026

Respectfully submitted,  
/s/Andreas T. Kaltsounis  
Andreas T. Kaltsounis, WSBA No. 29643  
*Counsel for Amici Curiae*

## TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT .....	ii
TABLE OF AUTHORITIES .....	iv
STATEMENT OF INTEREST .....	1
INTRODUCTION .....	5
ARGUMENT .....	6
I. THE PERMANENT INJUNCTION SERVES THE PUBLIC INTEREST ...	6
A. The Permanent Injunction is Necessary to Protect Journalists, Activists, and Human Rights Defenders .....	7
1. Journalists, activists, and human rights defenders need reliable access to secure, encrypted communications.....	8
2. Without the permanent injunction, NSO will continue enabling human rights violations.....	10
B. The Permanent Injunction Promotes National Security.....	17
1. Encryption is critical infrastructure and provides privacy and security benefits for the U.S. government. ....	20
2. U.S. law enforcement and intelligence agencies continue to demonstrate they are highly capable of lawfully gathering intelligence. ....	22
3. NSO is a known threat to U.S. national security. ....	23
4. Because NSO acts contrary to U.S. interests, any benefits it brings the U.S. government are incidental and unreliable.....	27
C. We All Benefit from Encryption.....	30
CONCLUSION.....	32
CERTIFICATE OF COMPLIANCE.....	33

## TABLE OF AUTHORITIES

	<b>Page(s)</b>
<b>Cases</b>	
<i>Carpenter v. United States</i> , 585 U.S. 296 (2017).....	23
<i>Doe v. Horne</i> , 115 F.4th 1083 (9th Cir. 2024).....	30
<i>Domain Name Comm’n Ltd. v. DomainTools, LLC.</i> , 781 F. App’x 604 (9th Cir. 2019).....	6
<i>E. Bay Sanctuary Covenant v. Biden</i> , 993 F.3d 640 (9th Cir. 2021) .....	8
<i>Francisco T. v. Bondi</i> , 797 F. Supp. 3d 970 (D. Minn. 2025).....	8
<i>HIAS, Inc. v. Trump</i> , 985 F.3d 309 (4th Cir. 2021) .....	8
<i>L.A. Press Club v. Noem</i> , 171 F.4th 1179 (9th Cir. 2026).....	7, 9, 30
<i>Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.</i> , 518 F. Supp. 2d 1197, 1221 (C.D. Cal. 2007).....	17
<i>Ramirez v. Collier</i> , 595 U.S. 411 (2022).....	7
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	23
<i>SEC v. Koracorp Indus., Inc.</i> , 575 F.2d 692 (9th Cir. 1978), cert. denied 439 U.S. 953 (1978) .....	17
<i>Shell Offshore, Inc. v. Greenpeace, Inc.</i> , 709 F.3d 1281 (9th Cir. 2013) .....	6
<i>Thalheimer v. City of San Diego</i> , 645 F.3d 1109 (9th Cir. 2011) .....	6

<i>United States v. Jones</i> , 565 U.S. 400 (2012).....	23
-------------------------------------------------------------	----

**Constitutional Provisions**

U.S. Const. amend. I .....	30, 31
U.S. Const. amend. IV .....	30
U.S. Const. amend. V.....	31

**Statutes**

50 U.S.C. § 3316a (2022) .....	26
--------------------------------	----

**Regulations**

12 C.F.R. § 364, appx. B, Section III(C)(1)(c).....	20
16 C.F.R. § 314.4(c)(3).....	20
201 Code Mass. Regs. § 17.04.....	21
Addition of Certain Entities to the Entity List, 86 Fed. Reg. 60,759 (Nov. 4, 2021).....	24
Cal. Code Regs. tit. 11, § 7123(c)(2) .....	21
Exec. Order No. 14028, Improving the Nation's Cybersecurity, 86 Fed. Reg. 26,633 (May 12, 2021).....	20
Exec. Order No. 14093, Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security, 88 Fed. Reg. 18,957-58 (Mar. 30, 2023).....	24
HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 898, 901 (proposed Jan. 6, 2025) (to be codified at 45 C.F.R. pts. 160, 164).....	20

**Other Authorities**

<i>2025 Round-Up</i> , Reps. Without Borders, 4 (Dec. 9, 2025), <a href="https://perma.cc/LMF9-DP4A">https://perma.cc/LMF9-DP4A</a> .....	8
----------------------------------------------------------------------------------------------------------------------------------------------	---

<i>Access Now and Russian civil society victims help take down Russian phishing infrastructure</i> , Access Now (Oct. 3, 2024), <a href="https://perma.cc/P38K-RXZB">https://perma.cc/P38K-RXZB</a> .....	14
Access Now et al., <i>NSO Group continues to fail in human rights compliance</i> , 4 (Apr. 27, 2021) <a href="https://perma.cc/HBW8-57D2">https://perma.cc/HBW8-57D2</a> .....	16
Agence France-Presse, <i>Discord to Bitchat, How Gen Z Protesters Used Tech During Nepal Protests</i> , NDTV World (Sept. 13, 2025), <a href="https://perma.cc/QPL9-EDB5">https://perma.cc/QPL9-EDB5</a> .....	10
<i>Amnesty International Among Targets of NSO-powered Campaign</i> , Amnesty Int'l (Aug. 1, 2018), <a href="https://perma.cc/D77A-G7JN">https://perma.cc/D77A-G7JN</a> .....	27
<i>Amnesty International staff targeted with malicious spyware</i> , Amnesty Int'l (July 25, 2018), <a href="https://perma.cc/YZH2-JMD9">https://perma.cc/YZH2-JMD9</a> .....	16
<i>Amnesty International uncovers new hacking campaign linked to mercenary spyware company</i> , Amnesty Int'l (Mar. 29, 2023), <a href="https://perma.cc/24NP-Z4UC">https://perma.cc/24NP-Z4UC</a> .....	14
Anthony Deutsch, <i>Russia-backed hackers breach Signal, WhatsApp accounts of officials, journalists, Netherlands warns</i> , Reuters (Mar. 9, 2026) .....	18
Ash Carter, Sec'y of Def., Remarks in a “Fireside” Chat with Ted Schlein in San Francisco, California (Mar. 2, 2016), <a href="https://perma.cc/4TEN-5PFW">https://perma.cc/4TEN-5PFW</a> .....	22
<i>Between a hack and a hard place: how Pegasus spyware crushes civic space in Jordan</i> , Access Now (Feb. 1, 2024), <a href="https://perma.cc/56YW-4TCN">https://perma.cc/56YW-4TCN</a> .....	15
Bill Marczak et al., <i>The Kingdom Came to Canada</i> , Citizen Lab (Oct. 1, 2018), <a href="https://perma.cc/ZN99-JH5A">https://perma.cc/ZN99-JH5A</a> .....	11
Bill Marczak et al., <i>Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries</i> , Citizen Lab (Sept. 18, 2018), <a href="https://perma.cc/6PBZ-D2HR">https://perma.cc/6PBZ-D2HR</a> .....	13
Bruce Schneier et al., <i>Don't Panic. Making Progress on the “Going Dark” Debate</i> , Berkman Ctr. for Internet & Soc., 10 (Feb. 1, 2016), <a href="https://perma.cc/4HSJ-MSGV">https://perma.cc/4HSJ-MSGV</a> .....	19, 22

Catherine Thorbecke, <i>How tech has fueled a “leaderless protest” in Hong Kong</i> , ABC News (Oct. 12, 2019), <a href="https://perma.cc/5P9W-PRXT">https://perma.cc/5P9W-PRXT</a> .....	9
Chris Jaikaran, Cong. Rsch. Serv., IF12798, <i>Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications</i> (updated Jan. 23, 2025), <a href="https://perma.cc/RP8R-W6G7">https://perma.cc/RP8R-W6G7</a> .....	21
Christopher Bing and Joseph Menn, <i>U.S. State Department phones hacked with Israeli company spyware</i> , Reuters (Dec. 4, 2021), <a href="https://perma.cc/B6QG-6RJL">https://perma.cc/B6QG-6RJL</a> .....	25
<i>Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware: Hearing Before the H. Permanent Select Comm. on Intel.</i> , 117th Cong. (2022) (written testimony of John Scott-Railton), <a href="https://perma.cc/4XLC-H6DU">https://perma.cc/4XLC-H6DU</a> .....	15
<i>Comments Submitted to the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression On the Use of Encryption and Anonymity in Digital Communications</i> , Hum. Rts. Watch, (Feb. 18, 2015), <a href="https://perma.cc/B68T-T7PT">https://perma.cc/B68T-T7PT</a> .....	10
Craig Timberg et al., <i>Key question for Americans overseas: Can their phones be hacked?</i> , Wash. Post (Jul. 19, 2021) .....	25
Craig Timberg et al., <i>Pegasus spyware used to hack U.S. diplomats working abroad</i> , Wash. Post (Dec. 31, 2021), <a href="https://perma.cc/3UAZ-T55Y">https://perma.cc/3UAZ-T55Y</a> .....	26
David Greene, <i>Deep Dive into First Unitarian Church v. NSA: Why Freedom of Association Matters</i> , Elec. Frontier Found. (Jan. 27, 2014), <a href="https://perma.cc/B3PV-58VB">https://perma.cc/B3PV-58VB</a> .....	31
<i>Digital Safety Kit</i> , Comm. to Protect Journalists (July 30, 2019), <a href="https://perma.cc/D4Z9-JSEE">https://perma.cc/D4Z9-JSEE</a> (last updated Feb. 20, 2026) .....	7
<i>Digital Security</i> , Glob. Investigative Journalism Network (Mar. 21, 2013), <a href="https://perma.cc/JJP2-NUN2">https://perma.cc/JJP2-NUN2</a> .....	7
<i>Digital Security Resource Hub for Civil Society</i> , Amnesty Int'l, <a href="https://perma.cc/L8MA-4V6D">https://perma.cc/L8MA-4V6D</a> (last visited May 17, 2020) .....	7

<i>Encryption</i> , Internet Soc’y (Oct. 2021), <a href="https://perma.cc/P7RJ-KKV7">https://perma.cc/P7RJ-KKV7</a> .....	9
<i>Enhanced Visibility and Hardening Guidance for Communications Infrastructure</i> , Cybersecurity & Infrastructure Sec. Agency, 2, 4 (Dec. 3, 2024), <a href="https://perma.cc/8VNK-MP8K">https://perma.cc/8VNK-MP8K</a> .....	21
Eur. Parl. Report, Sophie in 't Veld, <i>Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware</i> , 50 (May 22, 2023), <a href="https://perma.cc/WB4B-ARQP">https://perma.cc/WB4B-ARQP</a> .....	29
Gerardo Reyes, <i>Panama's ex-president wiretapped Americans, according to court documents</i> , Univision News (Jun. 24, 2017), <a href="https://perma.cc/MN3N-VNYW">https://perma.cc/MN3N-VNYW</a> .....	25
Hannar R. Garry, <i>Morocco v. Omar Radi II: Trialwatch Fairness Report</i> , Univ. of S. Cal. Gould Sch. of L. (July 2022), <a href="https://perma.cc/FN97-9KVU">https://perma.cc/FN97-9KVU</a> .....	12
International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), art. 19 (Dec. 16, 1966) .....	30, 31
Interview by Tom Ashbrook with Michael Hayden, Former Dir., NSA & CIA, <i>On Point</i> (WBUR radio broadcast Mar. 1, 2016), <a href="https://perma.cc/XL9U-4RFH">https://perma.cc/XL9U-4RFH</a> .....	18
<i>Israel: government has tried to suppress revelations in NSO spyware legal case</i> , Amnesty Int'l (July 25, 2024), <a href="https://perma.cc/S6CU-CRJ8">https://perma.cc/S6CU-CRJ8</a> .....	29
J.J. Gálvez, <i>Israel blocks Spain's judicial investigation into Pegasus spyware scandal</i> , El Pais (Jan. 22, 2026), <a href="https://perma.cc/D46W-4J4X">https://perma.cc/D46W-4J4X</a> .....	29
James Baker, former FBI General Counsel, <i>Rethinking Encryption</i> , Lawfare (Oct. 22, 2019), <a href="https://perma.cc/N8B6-JBX4">https://perma.cc/N8B6-JBX4</a> .....	20
James Comey, <i>Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy</i> 114th Cong. 69 (July 8, 2015), <a href="https://perma.cc/4MV7-SQG4">https://perma.cc/4MV7-SQG4</a> .....	19, 22, 30

John Scott-Railton et al., <i>Pegasus Spyware Used Against Thailand's Pro-Democracy Movement</i> , Citizen Lab (July 17, 2022), <a href="https://perma.cc/DV5S-6UZ9">https://perma.cc/DV5S-6UZ9</a> .....	15
John Scott-Railton et al., <i>Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware</i> , Citizen Lab (Aug. 3, 2020), <a href="https://perma.cc/8LUC-QQWP">https://perma.cc/8LUC-QQWP</a> .....	31
Jonathan Rozen, <i>How Nigeria's police used telecom surveillance to lure and arrest journalists</i> , Comm. to Protect Journalists (Feb. 13, 2020), <a href="https://perma.cc/RHD3-4WCX">https://perma.cc/RHD3-4WCX</a> .....	8
Lorenzo Franceschi-Bicchierai, <i>Spyware maker NSO Group confirms acquisition by US investors</i> , TechCrunch (Oct. 10, 2025), <a href="https://perma.cc/K3QE-7FF7">https://perma.cc/K3QE-7FF7</a> .....	28
Marco Rubio, Sec'y of State, Resources and Support for U.S. Citizens Overseas (Mar. 2, 2026), <a href="https://perma.cc/F999-MF7Q">https://perma.cc/F999-MF7Q</a> .....	18
<i>Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally</i> , Amnesty Int'l (July 19, 2021), <a href="https://perma.cc/8YU4-RKJF">https://perma.cc/8YU4-RKJF</a> .....	13
<i>Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally</i> , Amnesty Int'l (July 19, 2021), <a href="https://perma.cc/N3M9-TPLH">https://perma.cc/N3M9-TPLH</a> .....	11
<i>Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague</i> , Citizen Lab (Nov. 27, 2018), <a href="https://perma.cc/MXH6-SMR4">https://perma.cc/MXH6-SMR4</a> .....	11
<i>Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware</i> , Citizen Lab (June 19, 2017), <a href="https://perma.cc/SU55-M3WJ">https://perma.cc/SU55-M3WJ</a> .....	14
Michael De Dora, <i>New CPJ, Internet Society fact sheet on why journalists need encryption</i> , Comm. to Protect Journalists (Mar. 26, 2020), <a href="https://perma.cc/3KMZ-FJLB">https://perma.cc/3KMZ-FJLB</a> .....	9
Mike McConnell et al., former NSA director, <i>Why the Fear Over Ubiquitous Data Encryption is Overblown</i> , Wash. Post, July 28, 2015, <a href="https://perma.cc/D77C-B5DZ">https://perma.cc/D77C-B5DZ</a> .....	20

Mike Morrell et al., <i>Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies</i> (Dec. 12, 2013), <a href="https://perma.cc/TG3V-EZQP">https://perma.cc/TG3V-EZQP</a> .....	21
<i>Mobile Communications Best Practice Guidance</i> , Cybersecurity & Infrastructure Sec. Agency, 1–2 (Dec. 18, 2024), <a href="https://perma.cc/3BNA-2S89">https://perma.cc/3BNA-2S89</a> (last updated Nov. 24, 2025).....	18
Monique Beals, <i>FBI Says Pegasus spyware was tested, not used in any investigation</i> , The Hill (Feb. 2, 2022), <a href="https://perma.cc/7CVX-CGVF">https://perma.cc/7CVX-CGVF</a> .....	25
<i>Morocco: Human Rights Defenders Targeted with NSO Group's Spyware</i> , Amnesty Int'l (Oct. 10, 2019), <a href="https://perma.cc/ME6C-7LFY">https://perma.cc/ME6C-7LFY</a> .....	12
Natalia Krapiva, <i>Spyware in Serbia: Civil Society Under Attack</i> , Access Now (Nov. 28, 2023), <a href="https://perma.cc/84ZT-QWYR">https://perma.cc/84ZT-QWYR</a> .....	17
Orin Kerr, <i>An Equilibrium-Adjustment Theory of the Fourth Amendment</i> , 125 Harv. L. Rev. 476 (2011).....	23
<i>Pegasus Project: Rwandan authorities chose thousands of activists, journalists and politicians to target with NSO spyware</i> , Amnesty Int'l (July 19, 2021), <a href="https://perma.cc/5ALN-W7FE">https://perma.cc/5ALN-W7FE</a> .....	13
<i>Pegasus spyware maker rebuffed in efforts to get off trade blacklist</i> , Wash. Post (May 20, 2025), <a href="https://perma.cc/36MD-XXZ6">https://perma.cc/36MD-XXZ6</a> .....	24
<i>Pegasus: Spyware sold to government 'targets activists'</i> , BBC (July 19, 2021), <a href="https://perma.cc/9RHW-CJHN">https://perma.cc/9RHW-CJHN</a> .....	11
Rom Hendler, <i>Why Attorneys Need to Implement Email Encryption</i> , Am. Bar Ass'n (Mar. 7, 2023), <a href="https://perma.cc/L38Y-VL4K">https://perma.cc/L38Y-VL4K</a> .....	9
Ronan Farrow, <i>How Democracies Spy on their Citizens</i> , New Yorker (Apr. 18, 2022), <a href="https://perma.cc/4BMH-SDLS">https://perma.cc/4BMH-SDLS</a> .....	15, 16
Ronen Bergman and Mark Mazzetti, <i>Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia</i> , N.Y. Times (Mar. 23, 2022) .....	28

Ronen Bergman and Mark Mazzetti, <i>Israeli Companies Aided Saudi Spying Despite Khashoggi Killing</i> , N.Y. Times (July 17, 2021) .....	28
<i>Routine Message: Receive U.S. Embassy Messages via WhatsApp</i> , Virtual Embassy Tehran (Mar. 2, 2026), <a href="https://perma.cc/YD5R-MWDG">https://perma.cc/YD5R-MWDG</a> .....	18
<i>Ruling against NSO Group in Whatsapp case a “momentous win in fight against spyware abuse”</i> , Amnesty Int’l, May 7, 2025, <a href="https://perma.cc/N6ZV-CRDE">https://perma.cc/N6ZV-CRDE</a> .....	16
Ryan Naraine, <i>Google Catches Russian APT Reusing Exploits From Spyware Merchants NSO Group, Intellexa</i> , SecurityWeek (Aug. 29, 2024), <a href="https://perma.cc/47KL-ZKLH">https://perma.cc/47KL-ZKLH</a> .....	26
<i>Serbia: Technical Briefing: Journalists targeted with Pegasus Spyware</i> , Amnesty Int’l (Mar. 27, 2025), <a href="https://perma.cc/49SB-WNSA">https://perma.cc/49SB-WNSA</a> .....	17
Shalev Hulio, <i>Weaving a cyber web</i> , Ynet Glob. (Jan. 11, 2019), <a href="https://perma.cc/L2ZY-TDQS">https://perma.cc/L2ZY-TDQS</a> .....	16
<i>Start With Security: A Guide for Business</i> , Fed. Trade Comm’n (Aug. 2023), <a href="https://perma.cc/6FY9-74AZ">https://perma.cc/6FY9-74AZ</a> .....	21
Stephanie Kirchgaessner, <i>New evidence suggests spyware used to surveil Emirati activist Alaa Al-Siddiq</i> , Guardian (Sept. 24, 2021), <a href="https://perma.cc/9FXL-TKTV">https://perma.cc/9FXL-TKTV</a> .....	12, 13
<i>Stories of How Encryption Empowers and Protects People</i> , Glob. Encryption Coal., <a href="https://perma.cc/PGQ7-2E26">https://perma.cc/PGQ7-2E26</a> (last visited May 18, 2026) .....	31
Suzanne Smalley, <i>Former Mexican president investigated over allegedly taking bribes from spyware industry</i> , The Record (July 10, 2025), <a href="https://perma.cc/BE4G-5DQL">https://perma.cc/BE4G-5DQL</a> .....	29
Testimony of Christopher Wray, then FBI director, Oct. 21, 2022, <a href="https://perma.cc/83UC-E4FD">https://perma.cc/83UC-E4FD</a> .....	25
Tr. of Oral Arg. at 29, <i>Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.</i> , 545 U.S. 913 (2005) (No. 04-480) (Scalia, J.).....	16

<i>Transparency and Responsibility Report</i> , NSO Grp., 18 (June 30, 2021), <a href="https://perma.cc/72G3-HHXH">https://perma.cc/72G3-HHXH</a> .....	16
Vas Panagiotopoulos, <i>Will NSO's US Lobbying Pay Off Under Trump?</i> , Tech Pol'y Press (Mar. 4, 2026), <a href="https://perma.cc/QV6K-BT72">https://perma.cc/QV6K-BT72</a> .....	28
<i>Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware</i> , Citizen Lab (Mar. 20, 2019), <a href="https://perma.cc/4CT7-HF74">https://perma.cc/4CT7-HF74</a> .....	11

## STATEMENT OF INTEREST<sup>1</sup>

*Amici Curiae* are eleven international non-governmental organizations that endeavor to protect the rule of law and fundamental human rights, including the rights of civil society actors targeted with NSO's spyware. These actors must communicate safely and securely, without fear of reprisal by the governments that they seek to hold accountable. NSO's actions, which gave rise to the underlying lawsuit, undermine their ability to do so and put their lives at risk.

**Access Now** is an international non-governmental non-profit organization working to defend and extend the digital rights of people and communities at risk around the world, with particular focus on privacy and data protection, freedom of expression and assembly, digital security and connectivity. Access Now works to hold governments and companies accountable in courts around the globe.

**Agora International Human Rights Group** is an association of more than 100 lawyers and other legal professionals working on landmark human rights cases in Russia and internationally. Agora currently represents applicants in several hundred applications brought before the European Court of Human Rights. It also provides support to persons who have been forced to leave Russia due to persecution by the authorities.

---

<sup>1</sup> No party's counsel authored this brief in whole or in part. No party, counsel for a party, or any person or entity other than amici and their counsel made a monetary contribution intended to fund the preparation or submission of the brief.

The **Center for Democracy and Technology** (CDT) is a nonprofit, nonpartisan, public interest organization that, for over 30 years, has worked to promote the constitutional and democratic values of privacy, equality, free expression, and individual liberty in the digital age. CDT regularly advocates before courts, legislatures, and regulatory agencies for laws and policies that protect against invasive and unwarranted government surveillance. CDT was a founding member of and sits on the Steering Committee of the Global Encryption Coalition.

The **Committee to Protect Journalists** (CPJ) is an independent, nonprofit organization founded in 1981 to promote press freedom worldwide. It defends the right of journalists to report the news without fear of reprisal. CPJ's board of directors includes prominent journalists, media executives, and leaders from related professions.

The **CyberPeace Institute** protects the most vulnerable in cyberspace. It delivers cybersecurity assistance and holds all actors accountable for ensuring peace in cyberspace by exposing the human harm caused by cyberattacks and disinformation. It also advocates against the unacceptable use of AI to threaten international peace and security, while promoting its responsible development and use.

**Data Rights** is a French non-governmental non-profit that defends, enforces, and advances digital rights in Europe. It works to build an internet free from digital arms races and monopolistic control. Data Rights is a founding member of the PEGA Coalition and is also a member of the Global Encryption Coalition.

**Electronic Frontier Foundation (EFF)** is a nonprofit civil liberties organization that has worked for over 35 years to protect free speech, privacy, security, and innovation in the digital world. EFF has been a strong advocate for encryption and has litigated and otherwise advocated for it as an essential tool to advance human rights. EFF's technologists are also widely recognized as expert researchers on malware, leading investigations into misuse of surveillance technologies by governments to target citizens for human rights abuses.

The **International Justice Clinic at the University of California, Irvine School of Law (IJC)** advances international human rights law at the international, national, regional, and corporate levels, in the United States and globally. IJC is directed by David Kaye, who has written extensively on the protection of human rights in digital environments, including his landmark report on encryption and anonymity prepared during his tenure as Special Rapporteur (A/HRC/29/32). IJC has broad experience addressing threats to human rights in the digital realm, working alongside civil society organizations and other stakeholders worldwide.

**Media Defence** is an international human rights organization based in London, UK, that provides legal support to journalists, bloggers, and independent media facing legal threats to their work. It combines direct legal assistance with strategic litigation at regional and international courts to defend and advance press freedom globally. This includes cases involving spyware and other unlawful surveillance.

**Privacy International (PI)** is a London-based non-profit, non-governmental organization that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilizes allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

**Reporters Without Borders, Inc.** is a non-profit organization headquartered in Washington, D.C. It is the North American affiliate of Reporters Sans Frontières' (RSF), in that it operates as a branch of RSF for this region. RSF is an international non-profit, non-governmental organization dedicated to protecting the freedom, pluralism, and independence of journalism, and to defending those who embody these ideals, as well as promoting and defending the right of the public to access reliable and pluralistic information.

## INTRODUCTION

Encryption is a cornerstone of privacy and security that protects human rights and U.S. national security interests alike. The present injunction safeguards encryption and so serves public interests this Court has recognized. The injunction promotes the security and missions of journalists, activists, and human rights defenders in the U.S. and around the world; the constitutional and fundamental rights they exercise and protect; U.S. national security; and the security of global digital infrastructure that billions of people rely on.

When NSO exploits vulnerabilities to compromise the devices of WhatsApp users, circumventing the protections that end-to-end encryption provides, it undermines these public interests. While NSO warns that Pegasus is vital to avoid “Going Dark,” national security experts recognize not only that intelligence is richer and more broadly available than before, but also that strong encryption bolsters U.S. national security. Ultimately, Pegasus is not a boon to U.S. intelligence, but a mercenary tool that threatens U.S. public interests.

Accordingly, the Ninth Circuit should affirm the district court. The district court’s conclusion that the injunction benefits the public interest was not an abuse of discretion. Protecting encrypted communications benefits both security and privacy — the two do not trade-off as NSO claims.

## ARGUMENT

### I. THE PERMANENT INJUNCTION SERVES THE PUBLIC INTEREST

Encryption is critical to democracy in the digital age. Strong cryptography is a lifeline for civil society actors, including journalists, activists, and human rights defenders. It provides digital means for privacy and security, essential to hold power accountable when surveillance is wielded as a tool of political repression. Encryption thus furthers U.S. foreign policy interests to promote democracy and protect human rights. It protects domestic national security and is itself critical infrastructure. And, encryption is vital to protect individual liberties, serving as a technological backstop for the core values of liberal democracy.

We agree with the district court: the public interest weighs in favor of the injunction for many reasons. The district court's finding was not an abuse of discretion. "[A]s long as the district court got the law right," this Court should not reverse just because it "would have arrived at a different result." *Shell Offshore, Inc. v. Greenpeace, Inc.*, 709 F.3d 1281, 1286 (9th Cir. 2013) (citing *Thalheimer v. City of San Diego*, 645 F.3d 1109, 1115 (9th Cir. 2011)). The district court did not apply "an erroneous legal standard" or make "a factual finding that was illogical, implausible, or without support in inferences" from the record. *Domain Name Comm'n Ltd. v. DomainTools, LLC.*, 781 F. App'x 604, 606 (9th Cir. 2019)

(internal quotations omitted). It correctly identified that the “public interest tilt[s]” in WhatsApp’s favor. *Ramirez v. Collier*, 595 U.S. 411, 433 (2022).

**A. The Permanent Injunction is Necessary to Protect Journalists, Activists, and Human Rights Defenders**

The exclusion of journalists, activists, and human rights defenders “from public fora can have particularly deleterious effects on the public interest.” *L.A. Press Club v. Noem*, 171 F.4th 1179, 1190 (9th Cir. 2026). WhatsApp is a key tool that journalists, activists, and human rights defenders use to protect their causes, affiliates, and themselves from authoritarian regimes at scale. Amnesty International highlights that WhatsApp is “key to communications” for those “at heightened risk of digital surveillance” because it offers end-to-end encryption. *Digital Security Resource Hub for Civil Society*, Amnesty Int’l, <https://perma.cc/L8MA-4V6D> (last visited May 17, 2020). The Global Investigative Journalism Network states that journalists should “protect their communications and information from growing threats” through WhatsApp. *Digital Security*, Glob. Investigative Journalism Network (Mar. 21, 2013), <https://perma.cc/JJP2-NUN2>. And CPJ recommends WhatsApp for its end-to-end encrypted communications. *Digital Safety Kit*, Comm. to Protect Journalists (July 30, 2019), <https://perma.cc/D4Z9-JSEE> (last updated Feb. 20, 2026). If NSO is permitted to continue compromising user devices via Pegasus, it will harm

journalists, activists, and human rights defenders in the U.S. and throughout the world; their causes; and humanitarian and democratic U.S. foreign policy interests. *Cf. E. Bay Sanctuary Covenant v. Biden*, 993 F.3d 640, 678 (9th Cir. 2021) (noting that the public interest includes humanitarian causes, like “preventing the deaths and wrongful removal of asylum-seekers”); *HIAS, Inc. v. Trump*, 985 F.3d 309, 326 (4th Cir. 2021) (refugees); *cf. Francisco T. v. Bondi*, 797 F. Supp. 3d 970, 976 (D. Minn. 2025) (“[P]reventing unlawful detention is a compelling issue of public importance.”).

**1. Journalists, activists, and human rights defenders need reliable access to secure, encrypted communications.**

Secure, encrypted communications are critical for journalists, activists, and human rights defenders to do their jobs safely. In 2025, 67 journalists were killed, 503 detained, 20 held hostage, and 135 went missing, mainly in geographies in conflict with or governed by oppressive regimes. *2025 Round-Up*, Reps. Without Borders, 4 (Dec. 9, 2025), <https://perma.cc/LMF9-DP4A>. When civil society actors can protect their activity and conversations, they are better able to combat abuses of power. See Jonathan Rozen, *How Nigeria’s police used telecom surveillance to lure and arrest journalists*, Comm. to Protect Journalists (Feb. 13, 2020), <https://perma.cc/RHD3-4WCX>. Encryption helps journalists shield their sources and activists safeguard their supporters.

Encryption enables “[p]eaceful protests” and the “free press [that] sit at the core of our democracy.” *L.A. Press Club*, 171 F.4th at 1185. It prevents authoritarian regimes from intercepting, censoring, or modifying relevant communications. *Encryption*, Internet Soc’y (Oct. 2021), <https://perma.cc/P7RJ-KKV7>. Journalists are only able to conduct timely, high-quality reporting when they can promise their sources confidentiality, and can themselves communicate confidentially with editors at their publications. See Michael De Dora, *New CPJ, Internet Society fact sheet on why journalists need encryption*, Comm. to Protect Journalists (Mar. 26, 2020), <https://perma.cc/3KMZ-FJLB>; Catherine Thorbecke, *How tech has fueled a “leaderless protest” in Hong Kong*, ABC News (Oct. 12, 2019), <https://perma.cc/5P9W-PRXT> (protester-interviewee required anonymity). Encryption also protects confidential communications between individuals and their lawyers from unauthorized disclosure. Rom Hendler, *Why Attorneys Need to Implement Email Encryption*, Am. Bar Ass’n (Mar. 7, 2023), <https://perma.cc/L38Y-VL4K>.

Encryption further enables activists to securely associate and assemble. Community information, like police sightings, emboldened “not very brave protestor[s]” to participate in Hong Kong’s pro-democracy protests. *Thorbecke, supra*. Last year, Nepalese protesters used anonymous, end-to-end encrypted messaging to stay connected during government-imposed internet shutdowns.

Agence France-Presse, *Discord to Bitchat, How Gen Z Protesters Used Tech During Nepal Protests*, NDTV World (Sept. 13, 2025), <https://perma.cc/QPL9-EDB5>. This enabled them to securely coordinate protest activity and share police sightings. *Id.* They were ultimately successful in enacting change. *Id.* Contrast this with 2010, when the Tunisian government compromised protester Facebook accounts by intercepting unencrypted communications. The government used these accounts to undermine protest activities by poisoning communication channels and surveilling protesters. *Comments Submitted to the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression On the Use of Encryption and Anonymity in Digital Communications*, Hum. Rts. Watch, (Feb. 18, 2015), <https://perma.cc/B68T-T7PT>. The success of pro-democracy movements worldwide implicate U.S. foreign policy interests and hinge on the availability and reliability of end-to-end encrypted communications.

**2. Without the permanent injunction, NSO will continue enabling human rights violations.**

The trail of human rights violations that lay in NSO's wake demonstrate that NSO lacks either the ability or the willingness to control how its spyware is used. NSO's customers use Pegasus to spy on journalists and activists and potentially to plan their assassinations. These violations continue despite NSO's assurances since

2018 that it investigates and addresses these abuses. Despite its claims, NSO demonstrates little discernment about its customer base.

Authoritarian regimes routinely deploy Pegasus to silence journalists and activists who threaten their power. Just before and after the Saudi government assassinated journalist Jamal Khashoggi, Pegasus was deployed to surveil his family and associates. *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*, Amnesty Int'l (July 19, 2021), <https://perma.cc/N3M9-TPLH>; Bill Marczak et al., *The Kingdom Came to Canada*, Citizen Lab (Oct. 1, 2018), <https://perma.cc/ZN99-JH5A>. Just before and after the assassination of Javier Valdez Cárdenas, an independent Mexican journalist who investigated drug cartels and organized crime, Pegasus was deployed to surveil his wife and colleagues. *Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware*, Citizen Lab (Mar. 20, 2019), <https://perma.cc/4CT7-HF74>; *Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague*, Citizen Lab (Nov. 27, 2018), <https://perma.cc/MXH6-SMR4>. And following Cecilio Pineda Birto's murder, his phone number was discovered within a list of numbers of interest to NSO's clients. *Pegasus: Spyware sold to government 'targets activists'*, BBC (July 19, 2021), <https://perma.cc/9RHW-CJHN>.

Murder is not the only thing Pegasus surveillance targets worry about. Human rights defenders in Morocco, including Abdessadak El Bouchattaoui and Maati Monjib, experienced harassment and state action after being targeted by Pegasus. *Morocco: Human Rights Defenders Targeted with NSO Group's Spyware*, Amnesty Int'l (Oct. 10, 2019), <https://perma.cc/ME6C-7LFY>. Abdessadak El Bouchattaoui, lawyer and human rights defender, was sentenced to 20 months in prison by a Moroccan court for criticizing excessive use of state force. *Id.* Maati Monjib was charged with threatening state security for promoting privacy-protecting software for citizen journalists. *Id.* These account for only a portion of the harms that human rights defenders in Morocco, and all over the world in geographies with oppressive regimes, suffer, and that Pegasus enables. *See, e.g.*, Hannar R. Garry, *Morocco v. Omar Radi II: Trialwatch Fairness Report*, Univ. of S. Cal. Gould Sch. of L. (July 2022), <https://perma.cc/FN97-9KVU>.

Surveillance itself carries consequences. The late Alaa Al-Siddiq, former executive director of Saudi human rights group ALQST, is “one of the first known victims of targeting using Pegasus,” and was surveilled for six years. Stephanie Kirchgaessner, *New evidence suggests spyware used to surveil Emirati activist Alaa Al-Siddiq*, *Guardian* (Sept. 24, 2021), <https://perma.cc/9FXL-TKTV> (reporting on The Citizen Lab's research). Her phones were subject to persistent intrusion attempts. *Id.* Surveillance-induced fear caused behavioral changes — Al-

Siddiq would often change her subway routes, and tried “to not stand too close to the edge” “for fear she could be pushed on to the tracks.” *Id.*

Pegasus’s surveillance is widespread. In 2018, the Citizen Lab identified at least 45 countries where Pegasus spyware operators were likely conducting surveillance. Bill Marczak et al., *Tracking NSO Group’s Pegasus Spyware to Operations in 45 Countries*, Citizen Lab (Sept. 18, 2018), <https://perma.cc/6PBZ-D2HR>. In 2021, Forbidden Stories released the Pegasus Project, an exposé identifying 50,000 phone numbers, including those of thousands of activists, journalists, CEOs, and politicians, believed to be of interest to NSO’s clients. *Massive data leak reveals Israeli NSO Group’s spyware used to target activists, journalists, and political leaders globally*, Amnesty Int’l (July 19, 2021), <https://perma.cc/8YU4-RKJF>; *see also Pegasus Project: Rwandan authorities chose thousands of activists, journalists and politicians to target with NSO spyware*, Amnesty Int’l (July 19, 2021), <https://perma.cc/5ALN-W7FE>. These numbers only reflect potential targets of direct surveillance. They do not reflect other individuals whose conversations and other data were monitored and captured indirectly through surveillance directed at their friends, family, and colleagues.

Pegasus’s surveillance also reaches U.S. soil and citizens. Pegasus was used to surveil Carmen Aristegui, a reporter who spearheads critical investigations on the Mexican government. Efforts to surveil her dragged in her minor son, Emilio,

who was located in the U.S. *Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*, Citizen Lab (June 19, 2017), <https://perma.cc/SU55-M3WJ>. Both Carmen and Emilio received NSO exploit messages impersonating the U.S. embassy in Mexico. *Id.* And when Pegasus was deployed against Centro PRODH, a Mexican human rights group, it was also used to surveil American citizen Stephanie Brewer. *Id.*

These reports are highly reliable. Government authorities and major companies rely upon findings by organizations like Access Now, Amnesty International, and the Citizen Lab. Examples abound. Access Now's legal declaration before the U.S. District Court for the District of Columbia helped secure the seizure of 107 malicious domains used by Russian hacker group STAR BLIZZARD. *Access Now and Russian civil society victims help take down Russian phishing infrastructure*, Access Now (Oct. 3, 2024), <https://perma.cc/P38K-RXZB>. Vendors including Google and Samsung relied on Amnesty International's discovery, analysis, and report of a zero-day exploit chain to release security updates protecting billions of Android, Chrome, and Linux users from mercenary spyware. *Amnesty International uncovers new hacking campaign linked to mercenary spyware company*, Amnesty Int'l (Mar. 29, 2023), <https://perma.cc/24NP-Z4UC>. And the House of Representatives called for testimony from a senior researcher at the Citizen Lab to better understand national

security threats connected with foreign commercial spyware. *Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware: Hearing Before the H. Permanent Select Comm. on Intel.*, 117th Cong. (2022) (written testimony of John Scott-Railton), <https://perma.cc/4XLC-H6DU>.

Less reliable is NSO's claim that civil society actors are only incidentally surveilled, accidentally caught in the dragnet. The rate at which civil society actors are improperly surveilled, and the timing of that surveillance, betray this assertion. Among the thousands of improperly surveilled are thirty pro-democracy Thai protesters infected just before key political protests, John Scott-Railton et al., *Pegasus Spyware Used Against Thailand's Pro-Democracy Movement*, Citizen Lab (July 17, 2022), <https://perma.cc/DV5S-6UZ9>, thirty-five Jordanian journalists, activists, and human rights lawyers, *Between a hack and a hard place: how Pegasus spyware crushes civic space in Jordan*, Access Now (Feb. 1, 2024), <https://perma.cc/56YW-4TCN>, and sixty Catalanian politicians, lawyers and activists, Ronan Farrow, *How Democracies Spy on their Citizens*, New Yorker (Apr. 18, 2022), <https://perma.cc/4BMH-SDLS>. These people are journalists, activists, human rights defenders, and lawyers, not terrorists.

NSO's contradictory statements about its ability to screen for customer misuse show it cannot or will not control the danger to civil society actors. Sometimes, NSO claims it cannot get "sufficient data . . . to determine if there was

any misuse.” Access Now et al., *NSO Group continues to fail in human rights compliance*, 4 (Apr. 27, 2021) <https://perma.cc/HBW8-57D2>. At other times, NSO asserts it would be “impossible to act . . . without us being able to check” the activity. Shalev Hulio, *Weaving a cyber web*, Ynet Glob. (Jan. 11, 2019), <https://perma.cc/L2ZY-TDQS>. NSO employees report NSO can see every number Pegasus surveils: “We hear about every, every phone call that is being hacked over the globe, we get a report immediately.” Farrow, *supra*; see also *Ruling against NSO Group in Whatsapp case a “momentous win in fight against spyware abuse”*, Amnesty Int’l, May 7, 2025, <https://perma.cc/N6ZV-CRDE>.

In 2021, NSO admitted their insufficient screening “resulted in violations [of] fundamental human rights.” *Transparency and Responsibility Report*, NSO Grp., 18 (June 30, 2021), <https://perma.cc/72G3-HHXH>. Although NSO says that when a misuse allegation arises it “investigate[s] the issue and take[s] appropriate action,” violations continue. *Amnesty International staff targeted with malicious spyware*, Amnesty Int’l (July 25, 2018), <https://perma.cc/YZH2-JMD9>. This is unsurprising — NSO’s “past acts are what have developed [their] current clientele.” Tr. of Oral Arg. at 29, *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005) (No. 04-480) (Scalia, J.).

This Court should be skeptical of NSO’s claimed reform. Although NSO may point to deals it has declined, this Court should pause before “attaching any

significance to contrition under protest.” *SEC v. Koracorp Indus., Inc.*, 575 F.2d 692 (9th Cir. 1978), *cert. denied* 439 U.S. 953 (1978). It should be “inherently suspicious” of NSO’s “self-serving statements” “as it is entirely too easy for an adjudicated infringer to claim a reformation once the specter of a permanent injunction looms near.” *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 518 F. Supp. 2d 1197, 1221 (C.D. Cal. 2007). There are clear signs NSO continues to enable surveillance as usual. For example, in February 2025, two independent journalists were targeted with Pegasus. *Serbia: Technical Briefing: Journalists targeted with Pegasus Spyware*, Amnesty Int’l (Mar. 27, 2025), <https://perma.cc/49SB-WNSA>. This happened despite reports of misuse in Serbia just two years earlier. Natalia Krapiva, *Spyware in Serbia: Civil Society Under Attack*, Access Now (Nov. 28, 2023), <https://perma.cc/84ZT-QWYR>. And other abuses may yet be unknown: it took three years to establish a link between Pegasus and Khashoggi’s assassination, two for Cárdenas, and four for Birto. No doubt we will hear about new abuses for years to come.

## **B. The Permanent Injunction Promotes National Security**

Securing WhatsApp users from attacks by foreign intelligence also promotes U.S. national security. WhatsApp is widely selected as a secure channel for critical government communications. The Cybersecurity Infrastructure and Security Agency (CISA) lists WhatsApp as an example of a secure messaging service for

highly targeted individuals — officials in “senior government, military, or political positions.” *Mobile Communications Best Practice Guidance*, Cybersecurity & Infrastructure Sec. Agency, 1–2 (Dec. 18, 2024), <https://perma.cc/3BNA-2S89> (last updated Nov. 24, 2025). The State Department uses WhatsApp as a secure channel to provide security updates and alerts to U.S. citizens abroad. Marco Rubio, Sec’y of State, Resources and Support for U.S. Citizens Overseas (Mar. 2, 2026), <https://perma.cc/F999-MF7Q>; *Routine Message: Receive U.S. Embassy Messages via WhatsApp*, Virtual Embassy Tehran (Mar. 2, 2026), <https://perma.cc/YD5R-MWDG>. It is popular with U.S. government officials and their allies for sharing confidential and sensitive information. Anthony Deutsch, *Russia-backed hackers breach Signal, WhatsApp accounts of officials, journalists, Netherlands warns*, Reuters (Mar. 9, 2026), <https://perma.cc/5MBE-C6TJ>.

The U.S. recognizes the value of encryption beyond WhatsApp, too. It has codified mandates for encryption in federal statutes, state statutes, and agency materials. U.S. intelligence agency heads publicly attest to the merits of ubiquitous encryption, positing that “American security is better provided by not allowing” “exceptional or extraordinary access to otherwise unbreakable devices.” Interview by Tom Ashbrook with Michael Hayden, Former Dir., NSA & CIA, *On Point* (WBUR radio broadcast Mar. 1, 2016), <https://perma.cc/XL9U-4RFH>.

NSO claims Pegasus is necessary to avoid “Going Dark,” but both digital and national security experts agree that “Going Dark is the wrong metaphor. . . . Some areas are more illuminated now than in the past and others are brightening.” Bruce Schneier et al., *Don’t Panic. Making Progress on the “Going Dark” Debate*, Berkman Ctr. for Internet & Soc., 10 (Feb. 1, 2016), <https://perma.cc/4HSJ-MSGV> [hereinafter *Don’t Panic*]. Indeed, U.S. intelligence agencies have proven they remain capable of fulfilling their national security objectives. NSO raises the specter of end-to-end encryption’s threat to national security not only to argue the public interest favors overturning the injunction, but also to catastrophize the litigation as a whole. See James Comey, *Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy* 114th Cong. 69 (July 8, 2015), <https://perma.cc/4MV7-SQG4> (cautioning that others, “particularly those without our commitment to the rule of law[,] are using this debate as a cynical means to . . . undermine human rights”)

Yet, as the U.S. has recognized, NSO has continually proven that it itself is a threat to U.S. interests, both domestic and foreign. Pegasus has been used to surveil U.S. diplomats, in addition to an ever-growing number of journalists, activists, and other human rights defenders; NSO demonstrates little ability or willingness to control how Pegasus gets used; and Israel does its best to shield NSO from judicial inquiry and accountability, even when NSO comes under majority U.S. ownership.

**1. Encryption is critical infrastructure and provides privacy and security benefits for the U.S. government.**

“[I]n order to execute fully their responsibility to protect the nation from catastrophic attack and ensure the continuing operation of basic societal institutions, public safety officials should embrace encryption.” James Baker, former FBI General Counsel, *Rethinking Encryption*, Lawfare (Oct. 22, 2019), <https://perma.cc/N8B6-JBX4>. Indeed, “the greater public good is a secure communications infrastructure protected by ubiquitous encryption.” Mike McConnell et al., former NSA director, *Why the Fear Over Ubiquitous Data Encryption is Overblown*, Wash. Post, July 28, 2015, <https://perma.cc/D77C-B5DZ>.

U.S. national security and critical infrastructure relies on strong encryption. Statutes, guidance, and publications at federal and state levels require and promote encryption, including end-to-end encrypted communication, for critical infrastructure organizations, senior government officials, financial and healthcare systems, and military operations. *See supra* Section I.B. Further, federal agencies must encrypt data at rest and in transit. *See* Exec. Order No. 14028, Improving the Nation’s Cybersecurity, 86 Fed. Reg. 26,633 (May 12, 2021). And regulators across the country urge encryption across a variety of sectors. *See, e.g.*, 16 C.F.R. § 314.4(c)(3) (financial systems); 12 C.F.R. § 364, appx. B, Section III(C)(1)(c) (banking); HIPAA Security Rule To Strengthen the Cybersecurity of Electronic

Protected Health Information, 90 Fed. Reg. 898, 901 (proposed Jan. 6, 2025) (to be codified at 45 C.F.R. pts. 160, 164) (healthcare); *Start With Security: A Guide for Business*, Fed. Trade Comm’n (Aug. 2023), <https://perma.cc/6FY9-74AZ>; 201 Code Mass. Regs. § 17.04; Cal. Code Regs. tit. 11, § 7123(c)(2).

U.S. intelligence agencies also urge ubiquitous encryption adoption. Joint guidance from CISA, the NSA, and the FBI recommends that telecommunications and other critical infrastructure organizations “[e]nsure that traffic is end-to-end encrypted to the maximum extent possible” to “mitigate [threat] actors’ activity.” *Enhanced Visibility and Hardening Guidance for Communications Infrastructure*, Cybersecurity & Infrastructure Sec. Agency, 2, 4 (Dec. 3, 2024), <https://perma.cc/8VNK-MP8K>. This guidance followed Chinese espionage group Salt Typhoon’s surveillance campaigns across the U.S. communications sector. Chris Jaikaran, Cong. Rsch. Serv., IF12798, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications* (updated Jan. 23, 2025), <https://perma.cc/RP8R-W6G7>. Former CIA director Mike Morrell recommended the government “increase the use of encryption and urge U.S. companies to do so.” Mike Morrell et al., *Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies* (Dec. 12, 2013), <https://perma.cc/TG3V-EZQP>. Ash Carter, then Secretary of Defense, observed

that “data security including encryption is absolutely essential.” Ash Carter, Sec’y of Def., Remarks in a “Fireside” Chat with Ted Schlein in San Francisco, California (Mar. 2, 2016), <https://perma.cc/4TEN-5PFW>.

**2. U.S. law enforcement and intelligence agencies continue to demonstrate they are highly capable of lawfully gathering intelligence.**

The U.S. uses a potent combination of national security legislation and homegrown technological capabilities to fulfill its intelligence needs. In 2016, digital and national security experts met to discuss the “Going Dark” phenomena. *See Don’t Panic, supra*. These experts included Jack Goldsmith, former Assistant Attorney General to the Office of Legal Counsel and Special Counsel to the Department of Defense; Matthew Olsen, former NSA General Counsel and Director of the U.S. National Counterterrorism Center; and Anne Neuberger, then NSA’s Chief Risk Officer. *Id.* at 2. They agreed technological growth would “drastically change surveillance” and would offer “alternative vectors for information-gathering that could more than fill many of the gaps” left by encryption, to the point of “rais[ing] trouble questions about how exposed [] the general public is poised to become.” *Id.* at 12. These predictions have borne out as the U.S. has supercharged its surveillance authority and capabilities.

Congress has identified “how best to ensure that privacy and security can co-exist and reinforce each other.” Comey, *Going Dark, supra*. It has armed the

government with many legal avenues to assist law enforcement and intelligence agencies. The government routinely argues that CALEA, FISA courts, the Wiretap Act, and the traditional subpoena all empower it to acquire intelligence it seeks with legal basis. Surveillance technology is now so effective that the Supreme Court has fashioned legal constraints, *see, e.g., Carpenter v. United States*, 585 U.S. 296 (2017) (cell-site location information); *United States v. Jones*, 565 U.S. 400 (2012) (persistent vehicle tracking), recognizing the “vast quantities of personal information” cellphones hold also deserve “the protection for which the Founders fought,” *Riley v. California*, 573 U.S. 373, 386, 403 (2014). *See also* Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011).

### **3. NSO is a known threat to U.S. national security.**

NSO claims it is an essential provider to U.S. law enforcement and intelligence communities. But this is far from the truth. The U.S. government has designated NSO as a risk to U.S. national security and foreign policy interests. Foreign adversaries use Pegasus to surveil U.S. diplomats and allies, and leverage the same vulnerabilities that NSO exploits to the detriment of U.S. cybersecurity.

In 2021, the Department of Commerce’s Bureau of Industry and Security (BIS) identified reasonable cause to believe that NSO is “involved in activities that are contrary to the national security or foreign policy interests of the United

States.” 86 Fed. Reg. 60,759 (Nov. 4, 2021). It found NSO “supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers.” *Id.* For these reasons, the BIS added NSO to the Entity List. *Id.* NSO remains on the Entity List despite attempts to shake the designation loose. *See Pegasus spyware maker rebuffed in efforts to get off trade blacklist*, Wash. Post (May 20, 2025), <https://perma.cc/36MD-XXZ6>; *see also infra* Section I.B.4.

Executive Order 14093 also prohibits federal agencies from using NSO’s spyware. *See* Exec. Order No. 14093, Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security, 88 Fed. Reg. 18,957–58 (Mar. 30, 2023). Agencies may not use commercial spyware that any foreign entity has used “to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb dissent or political opposition; otherwise limit freedoms of expression, peaceful assembly, or association; or enable other forms of human rights abuses or suppression of civil liberties” or to compromise U.S. cybersecurity. *Id.*; *compare with supra* Section I.A.2.

NSO points at the FBI’s 2022 Pegasus license acquisition to claim it benefits U.S. national security. But Pegasus is good for U.S. national security in the same

way that studying virus samples is good for our health. The FBI purchased a “limited license” that allowed “product testing and evaluation only.” Monique Beals, *FBI Says Pegasus spyware was tested, not used in any investigation*, The Hill (Feb. 2, 2022), <https://perma.cc/7CVX-CGVF>. U.S. intelligence agencies “routinely identify, evaluate, and test” new technologies—not just for use, but to discern “operational and security concerns they might pose in the wrong hands.” *Id.*; *see also* Testimony of Christopher Wray, then FBI director, Oct. 21, 2022, <https://perma.cc/83UC-E4FD> (testifying the FBI has not used Pegasus for surveillance, and only to “figure out how bad guys could use it”). U.S. adversaries have used Pegasus against the devices of U.S. citizens and government officials on multiple occasions. *See, e.g.*, Christopher Bing and Joseph Menn, *U.S. State Department phones hacked with Israeli company spyware*, Reuters (Dec. 4, 2021), <https://perma.cc/B6QG-6RJL>; Gerardo Reyes, *Panama's ex-president wiretapped Americans, according to court documents*, Univision News (Jun. 24, 2017), <https://perma.cc/MN3N-VNYW>. Even if the injunction would impair the U.S. government, the U.S. technological environment is well-equipped to make up for the shortfall. *See supra* Section I.B.2.

NSO also claims its spyware cannot harm the U.S. After all, NSO says, Pegasus cannot surveil U.S. phone numbers. Even if true, U.S. citizens and officials using non-U.S. numbers remain unprotected. Craig Timberg et al., *Key*

*question for Americans overseas: Can their phones be hacked?*, Wash. Post (Jul. 19, 2021), <https://perma.cc/NZ8V-PD43>. After Pegasus was used to target eleven U.S. diplomats in Uganda, the U.S. National Security Council observed that “commercial spyware like NSO Group’s software poses a serious counterintelligence and security risk to U.S. personnel.” Craig Timberg et al., *Pegasus spyware used to hack U.S. diplomats working abroad*, Wash. Post (Dec. 31, 2021), <https://perma.cc/3UAZ-T55Y>.

And, NSO does not handle the vulnerabilities it discovers responsibly or in a way that furthers U.S. interests. The U.S. uses the Vulnerabilities Equities Process to balance immediate vulnerability disclosure against temporary national security use. 50 U.S.C. § 3316a (2022). The process evaluates risks, benefits, and competing considerations in a structured and holistic manner. *Id.* NSO engages in no such process. This results in foreign adversaries using the vulnerabilities NSO discovers and refashioning the exploits NSO develops. For example, Russian cyberespionage group APT29 leveraged CVE-2024-5274, a zero-day vulnerability first discovered from NSO use, against U.S. companies, including Google, Meta, and LinkedIn. Ryan Naraine, *Google Catches Russian APT Reusing Exploits From Spyware Merchants NSO Group*, *Intellexa*, SecurityWeek (Aug. 29, 2024), <https://perma.cc/47KL-ZKLH>.

**4. Because NSO acts contrary to U.S. interests, any benefits it brings the U.S. government are incidental and unreliable.**

Beyond greater ability to enforce injunctive relief, majority ownership by a U.S. investor is unlikely to improve NSO's behavior. Even when NSO has previously come under U.S. ownership, Pegasus has continued to be used to perpetuate human rights abuses against U.S. foreign policy interests. And when justice systems try to hold NSO accountable for degrading national security, Israel shields NSO from scrutiny and accountability.

U.S. ownership has not historically deterred NSO's misconduct or resulted in NSO's alignment with U.S. interests. NSO was owned by U.S. private equity firm Francisco Partners from 2014 to 2019. During this time, Pegasus surveillance targets included journalists in Mexico, human rights activists in the UAE, Amnesty International staff in Saudi Arabia, and the inner circle of noted journalist Jamal Khashoggi. *Amnesty International Among Targets of NSO-powered Campaign*, Amnesty Int'l (Aug. 1, 2018), <https://perma.cc/D77A-G7JN>; and *infra* Section I.A.2. This surveillance presaged the assassinations of Javier Valdez Cárdenas (2017), Cecilio Pineda Birto (2017), and Jamal Khashoggi (2018). *Id.* And just months after it was sold back to foreign owners, NSO engaged in the campaign against WhatsApp that gave rise to this litigation. NSO's most recent maneuvers to access U.S. markets include its sale to Hollywood producer Robert Simonds and the replacement of its executive chairman with former Trump administration

official David Friedman. Vas Panagiotopoulos, *Will NSO's US Lobbying Pay Off Under Trump?*, Tech Pol'y Press (Mar. 4, 2026), <https://perma.cc/QV6K-BT72>. So although yet another U.S. entity has very recently acquired a controlling stake in NSO, history suggests it will bring no improvement to NSO's behavior.

Despite this U.S. investment, NSO will remain a foreign company under “regulatory or operational control” by a foreign government. Lorenzo Franceschi-Bicchierai, *Spyware maker NSO Group confirms acquisition by US investors*, TechCrunch (Oct. 10, 2025) <https://perma.cc/K3QE-7FF7>. The company does not plan to move its headquarters or core operations to the U.S. *Id.* It will remain “fully supervised and regulated by the relevant Israeli authorities.” *Id.* Foreign government control over NSO is just another reason why the U.S. cannot rely on Pegasus. Israel has substantial ability to direct what deals NSO makes. When Ukraine and Estonia approached NSO to gain the ability to target Russian phone numbers for national defense, Israel reportedly blocked licensure. Ronen Bergman and Mark Mazzetti, *Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia*, N.Y. Times (Mar. 23, 2022), <https://perma.cc/K4CL-LBJE>. Israel has also allegedly encouraged its firms to do business with Saudi Arabia, even in the wake of Jamal Khashoggi's assassination. Ronen Bergman and Mark Mazzetti, *Israeli Companies Aided Saudi Spying Despite Khashoggi Killing*, N.Y. Times (July 17, 2021), <https://perma.cc/EGW8-7JEV>.

And, Israel has impeded legal inquiries throughout this case. It seized documents to stymie discovery, *Israel: government has tried to suppress revelations in NSO spyware legal case*, Amnesty Int'l (July 25, 2024), <https://perma.cc/S6CU-CRJ8>, and barred access to crucial computer code by making it “viewable only by Israeli citizens while in Israel,” 1-ER-60. Israel does this regularly with respect to Pegasus-related legal proceedings and legislative inquiries. Spanish Audiencia Nacional high court judge Calama says Israel ignores repeated “requests for cooperation,” forcing the high court to once again close its investigation into nine Pegasus attacks on Spain’s president and defense minister. J.J. Gálvez, *Israel blocks Spain’s judicial investigation into Pegasus spyware scandal*, El Pais (Jan. 22, 2026), <https://perma.cc/D46W-4J4X>. Israel has blocked the inquiries “for almost four years.” *Id.* The European Parliament notes that Israel provides no information about Pegasus licenses even though Pegasus is used “to violate the rights of European citizens and to undermine our democracy.” Eur. Parl. Report, Sophie in ‘t Veld, *Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware*, 50 (May 22, 2023), <https://perma.cc/WB4B-ARQP>. Mexico’s Attorney General says Israel has “historically been uncooperative” with investigations into Pegasus abuses. Suzanne Smalley, *Former*

*Mexican president investigated over allegedly taking bribes from spyware industry*, The Record (July 10, 2025), <https://perma.cc/BE4G-5DQL>.

### **C. We All Benefit from Encryption**

“[S]trong encryption is a key tool to secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cyber security.” Comey, *Going Dark*, *supra*.

Encryption improves peoples’ ability to exercise fundamental human rights, as embodied by the U.S. Constitution and human rights instruments worldwide. It is “always in the public interest” to uphold fundamental rights. *Doe v. Horne*, 115 F.4th 1083, 1098–99 (9th Cir. 2024). Further, the Ninth Circuit has “consistently recognized the significant public interest in upholding First Amendment principles.” *L.A. Press Club*, 171 F.4th at 1190 (internal citation omitted). Encryption directly protects the freedom of speech, the freedom of opinion and expression, and the right to hold opinions without interference. U.S. Const. amend. I; International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), art. 19 (Dec. 16, 1966) (ratified by U.S.). And encryption protects the right to secure one’s papers “against unreasonable searches,” U.S. Const. amend. IV, and from “arbitrary or unlawful interference” with one’s privacy or correspondence, International Covenant, *supra*, at art. 17.

Encryption has positive secondary effects for people's access to their fundamental rights, too. When correspondence is protected, people are better able to exercise their rights to freely assemble and associate. *Id.* at arts. 21–22; U.S. Const. amend. I; David Greene, *Deep Dive into First Unitarian Church v. NSA: Why Freedom of Association Matters*, Elec. Frontier Found. (Jan. 27, 2014), <https://perma.cc/B3PV-58VB>. It reinforces due process requirements, U.S. Const. amend. V, and so improves people's ability to avoid arbitrary arrest, International Covenant, *supra*, at art. 9.

Vulnerable groups who experience persecution for their identities or beliefs feel these benefits particularly sharply. Minority groups use encrypted channels to find each other, communicate, and build communities. *Stories of How Encryption Empowers and Protects People*, Glob. Encryption Coal., <https://perma.cc/PGQ7-2E26> (last visited May 18, 2026). In Togo, Pegasus was used to surveil opposition party figures and the Catholic Church of Togo, following their criticism of the current regime and efforts to support human rights and democracy. John Scott-Railton et al., *Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware*, Citizen Lab (Aug. 3, 2020), <https://perma.cc/8LUC-QQWP>. The surveillance targets believe this led to smear and disinformation campaigns against them. *Id.* Encryption gives people everywhere the peace of mind to express themselves and engage with the world.

## CONCLUSION

For the reasons above, *amici curiae* respectfully request that this Court affirm the district court's order granting plaintiff's motion for permanent injunction.

DATED this 20th day of May, 2026

Baker & Hostetler, LLP

/s/ Andreas T. Kaltsounis

Andreas T. Kaltsounis, WSBA No. 29643

Jacob T. Wall, WSBA No. 58844

King O. Xia, CSBA No. 339128

Baker & Hostetler, LLP

999 3rd Ave, Suite 3900

Seattle, WA 98104

(206) 566-7080

akaltsounis@bakerlaw.com

*Counsel for Amici Curiae*

UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

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

9th Cir. Case Number(s)

I am the attorney or self-represented party.

This brief contains  words, including  words

manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

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

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

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

Feedback or questions about this form? Email us at [forms@ca9.uscourts.gov](mailto:forms@ca9.uscourts.gov)