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

BRIEF FOR *AMICUS CURIAE* DAVID KAYE, FORMER SPECIAL RAPPORTEUR TO THE UNITED NATIONS ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION, IN SUPPORT OF APPELLEES (AFFIRMANCE)

David Kaye
401 E. Peltason Dr.
Irvine, California 92697
dkaye@law.uci.edu

Amicus Curiae

Elaine Goldenberg
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Avenue NW, Suite 500E
Washington, D.C. 20001-5369
202-220-1000
Elaine.Goldenberg@mto.com

Marianna Mao
MUNGER, TOLLES & OLSON LLP
560 Mission Street, 27th Floor
San Francisco, California 94105-2907
Marianna.Mao@mto.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

LEGAL AUTHORITIES

TABLE OF AUTHORITIES
(Continued)

Page(s)

OTHER AUTHORITIES

TABLE OF AUTHORITIES
(Continued)

Page(s)

TABLE OF AUTHORITIES
(Continued)

Page(s)

INTEREST OF THE *AMICUS CURIAE*

Amicus David Kaye served as the United Nations ("UN") Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression from August 2014 to July 2020.[1] In that role, through detailed research and official country missions, he monitored trends concerning the freedom of expression globally and reported on those trends to the UN General Assembly and Human Rights Council. He is a clinical professor of law at the University of California, Irvine, School of Law, where his teaching and research focus on international human rights law, technology and international law, and other subjects in public international law.

Amicus is an expert in the field of international human rights law, having published a book on technology and human rights, as well as numerous law review articles, book chapters, and opinion pieces on the topic. His reporting for the UN addressed, among other subjects concerning the impact of technology on the enjoyment of human rights, encryption and anonymity, the protection of whistleblowers and journalistic sources, the human rights obligations of

[1] Both parties have consented to the filing of this brief. Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), *amicus* states that (1) no "party's counsel authored the brief in whole or in part"; (2) no "party or a party's counsel contributed money that was intended to fund preparing or submitting the brief"; and (3) no "person—other than the amicus curiae, its members, or its counsel" has "contributed money that was intended to fund preparing or submitting the brief."

governments and responsibilities of companies in the Information and Communications Technology sector, the regulation of online content by social media and search companies, Artificial Intelligence technologies and human rights, and online hate speech.

A member of several boards dealing with freedom of expression in online and offline fora, since October 2020 *amicus* has been serving as the Independent Chair of the Board of the Global Network Initiative, a multi-stakeholder organization consisting of companies, academics, investors, and others. *Amicus* began his legal career with the U.S. State Department's Office of the Legal Adviser, is a life member of the Council on Foreign Relations, and is a former member of the Executive Council of the American Society of International Law.

Of special relevance to this case, *amicus* is highly familiar with the private cyber-surveillance industry, of which appellant NSO Group ("NSO") is a prominent member, through his experience as a professor of international law and his six-year tenure as Special Rapporteur. Most notably, in May 2019, in his capacity as Special Rapporteur, *amicus* submitted a report to the Human Rights Council of the United Nations regarding the private cyber-surveillance industry. *See Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/41/35 (May 28, 2019) ("Report"), https://www.undocs.org/A/HRC/41/35.

ARGUMENT

NSO develops and markets a spyware tool, known as Pegasus, that surreptitiously allows access to victims' mobile devices—including communications, documents, contacts, and data about online and offline activities. The use of Pegasus, and other spyware tools like it, constitutes a serious invasion of rights to privacy and free expression that are protected under international human rights law.

NSO argues that it should not be held accountable for its actions because, it alleges, it sells its tools only to governments, and only for the purpose of investigating terrorism and serious crime. That self-serving story is impossible to confirm, given the cloak of secrecy under which NSO and other businesses in the private spyware market operate. It is also contradicted by a growing body of evidence that spyware—including NSO's Pegasus tool—has repeatedly interfered with the human rights of activists, journalists, and others and has undermined democratic values globally. That evidence almost certainly reflects only a fraction of actual instances of abuse, as the private market for cyber-surveillance technology is largely unregulated and opaque to public scrutiny.

A viable remedy for that abuse is desperately needed and yet globally unavailable. Neither export controls nor voluntary due diligence programs have proven effective at preventing violations of human rights by repressive regimes

around the world, or at protecting American individuals or corporations from unlawful hacking. And the novel extension of legal immunity requested by NSO would effectively eliminate any remedy, allowing private companies to take with impunity whatever steps they deem appropriate to develop, improve, and market their spyware and to support their clients in deploying the spyware.

This Court should not endorse the elimination of the judicial remedy that WhatsApp seeks in this case. Such a step would exacerbate the serious problems to which NSO's actions and the actions of similar companies give rise. It also would contradict the United States's commitment, reflected in an international treaty that the United States has ratified, to "develop the possibilities of judicial remedy" with respect to the rights guaranteed by the International Covenant on Civil and Political Rights, which include the rights to privacy and freedom of expression. Those rights are threatened by NSO's unregulated marketing, sale, transfer, and support of spyware to target activists, journalists, and dissidents around the world.

I. THE PRIVATE CYBER-SURVEILLANCE INDUSTRY MARKETS SOPHISTICATED SPYWARE TO REPRESSIVE GOVERNMENTS

A. NSO and Other Private Companies Develop and Sell Comprehensive and Covert Cyber-Surveillance Technology

In the past decade, private companies like NSO have developed and offered for sale sophisticated spyware tools that surreptitiously hack into computers, mobile phones, and other devices and obtain unfettered access to an individual's

communications, documents, and data about online and offline activities. *See* Report ¶¶ 5–14. For example, NSO's Pegasus program can be used to extract encrypted messages, contact lists, calendar records, emails, and GPS locations from virtually any modern cell phone. *See* Nicole Perlroth, *How Spy Tech Firms Let Governments See Everything on a Smartphone*, N.Y. Times (Sept. 2, 2016), https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html. The program also can act as a wiretap by taking over a cell phone's microphone. *See id.*

NSO is far from the only private company involved in selling clandestine spyware tools. According to the UK-based organization Privacy International, as early as 2016, there were already well over five hundred companies known to be developing, marketing, and selling surveillance products, *see* Report ¶ 6, and still more such companies exist today. Those companies market products that include not only computer surveillance tools similar to the Pegasus program, *see* Report ¶ 8; Amnesty International, *German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed* (Sept. 25, 2020), https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/, but also (for example) hardware that enables surveillance of telecommunications networks and facial-recognition software that uses artificial intelligence to identify and surveil individuals offline, *see* Report

¶¶ 11-12; *see also* Human Rights in China, *Submission to the Special Rapporteur* 2-3 (Feb. 15, 2019), https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/HUMAN%20RIGHTS%20IN%20CHINA.pdf.

Cyber-surveillance companies like NSO are constantly developing new ways to enable invasive and surreptitious surveillance. Cyber-surveillance technology requires leveraging security vulnerabilities—for example, vulnerabilities in iOS or Android operating systems, or vulnerabilities in the design of applications for email and messaging. In the present case, for example, NSO is alleged to have spent over a year reverse-engineering the WhatsApp software to identify and test for vulnerabilities and to circumvent technical restrictions in WhatsApp's servers. *See* WhatsApp Br. 8. Once those vulnerabilities are discovered and patched, the spyware can continue to function only if it is installed on a target device through an alternate vulnerable pathway.

Cyber-surveillance companies also are known to purchase "zero-day exploits"—that is, vulnerabilities that can serve as entry points for electronic surveillance because the relevant software or hardware manufacturer does not know about them. *See* Report ¶ 17. A highly lucrative and unregulated market exists for the purchase and sale of zero-day exploits to potentially unscrupulous bidders.

NSO has been linked to multiple zero-day exploits of the iOS operating system, which is widely considered to be one of the most secure consumer programs

in the world. In 2016, the Toronto-based research institute Citizen Lab investigated an attempt to install Pegasus spyware on an iPhone belonging to well-known UAE human rights activist Ahmed Mansoor. The attempt involved three separate zero-day exploits, corresponding to previously unknown vulnerabilities in iOS, which Apple ultimately investigated and closed through a software update. *See* Bill Marczak & John Scott-Railton, Citizen Lab, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender* (Aug. 24, 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae.

B. NSO's Product and Tools Like It Are Marketed To Governments That Use Them For Severe and Dangerous Invasions Of Privacy

1. *NSO markets and sells its products to oppressive regimes.* As WhatsApp explains (WhatsApp Br. 49), companies like NSO market and sell their technologies widely to many government purchasers—and many of those customers are repressive regimes with a known record of human rights abuses.

One study concluded that nearly 30 percent of spyware export licenses granted by EU member states between 2014 and 2017 went to countries labeled "not free" by Freedom House, including the United Arab Emirates, Egypt, and Vietnam. *See* Sebastian Gjerding & Lasse Skou Anderson, de Correspondent, *How European spy technology falls into the wrong hands* (Feb. 23, 2017), https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-

51234153.[2] And as to NSO specifically, between 2016 and 2018, the Pegasus program appears to have been operated by at least 33 different customers against individuals in 45 different countries, including Bahrain, Saudi Arabia, and Togo. *See* Report ¶ 9; Bill Marczak *et al.*, Citizen Lab, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries* (Sept. 18, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/; *see also* Catalin Cimpanu, ZD Net, *New versions of FinFisher mobile spyware discovered in Myanmar* (July 10, 2019) (discussing wide use of program similar to Pegasus but created by a different company), https://www.zdnet.com/article/new-versions-of-finfisher-mobile-spyware-discovered-in-myanmar/.

Some cyber-surveillance companies claim, as NSO does here (NSO Br. 16), that they sell their spyware only to government actors seeking to halt or investigate serious crimes. But public reporting and digital forensic investigations have confirmed that technologies like Pegasus are regularly used to monitor and suppress the viewpoints of journalists, academics, students, opposition leaders, and others who are engaged in the exercise of fundamental rights to freedom of expression and

[2] Many EU member states simply refused to provide the requested information about export licenses—including "France and Italy, both home to some of the world's biggest spy-tech businesses." *Id.*

association—and clearly not in terrorist activities. *See* Report ¶¶ 8–14. As *amicus* concluded in his Report, "[c]redible allegations have shown that [cyber-surveillance] companies are selling their tools to Governments that use them to target journalists, activists, opposition figures and others who play critical roles in democratic society," and that activity amounts to "gross . . . abuse[]" of the targets' rights to privacy, freedom of expression, and freedom of association. Report ¶¶ 32, 48.

There is also more to NSO's *sale* of Pegasus than the mere transaction and transfer of the spyware. *See* WhatsApp Br. 6-7 (stating that NSO provides post-transaction support). As one report found, "NSO provides hacking as a streamlined service, which means . . . NSO can offer hands-on assistance to the government employees who use it." Lorenzo Fransechi-Bicchierai and Joseph Cox, Vice, *How NSO Group Helps Countries Hack Targets* (October 31, 2019), https://www.vice.com/en/article/gyznnq/how-nso-group-helps-countries-hack-targets. Not only does the company help set up Pegasus for a customer and troubleshoot it, but "NSO also helps some customers craft phishing messages that the target is more likely to click." *Id.* Public information thus suggests that NSO's claims that "[f]oreign states, not NSO, operate the technology" and that "NSO provides limited support," NSO Br. 2-3, may elide broader involvement in the deployment of Pegasus.

2. *The problem is severe and continuing.* It is difficult to quantify the full extent of the serious problem of human rights abuses using cyber-surveillance technologies, although it is likely even more widespread than has been confirmed. The misuse of such technologies is understudied and underreported because those tools are designed to operate in secrecy and without detection by the target of the surveillance. Nevertheless, five recent examples bolster the conclusions in *amicus*'s 2019 Report and illustrate the ways in which tools like NSO's continue to be regularly deployed to undermine human rights.

a. As noted above, in 2016, Ahmed Mansoor, an internationally recognized human rights activist from the UAE, discovered with the support of forensic experts at Citizen Lab that he had been targeted by a Pegasus attack that would have leveraged multiple zero-day exploits on Mansoor's iPhone. Mansoor had previously been the target of attacks using spyware and a surveillance tool sold by other companies. *See* Marczak, et al., *Million Dollar Dissident*, *supra* p.7.

Shortly after the Pegasus attack, UAE authorities arrested Mansoor. He was convicted and sentenced to 10 years in prison for offending the "status and prestige of the UAE and its symbols" through his human rights activism. *See* Human Rights Watch, *UAE: Free Unjustly Detained Rights Defender Ahmed Mansoor Ahead of His 50th birthday, Over 135 Groups Call for His Release* (Oct. 16, 2019),

https://www.hrw.org/news/2019/10/16/uae-free-unjustly-detained-rights-defender-ahmed-mansoor.

b. The New York Times, Citizen Lab, the Mexican organization R3D, and Amnesty International, among others, have reported on a sprawling surveillance campaign from 2016 to 2018 during which NSO's Pegasus spyware was used to target and surveil Mexican journalists, human rights activists, academics, and lawyers. *See, e.g.*, Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N.Y. Times (June 19, 2017), https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html. The persons targeted during that lengthy campaign included Mexican citizens—"some of the government's most outspoken critics and their families"—as well as international officials who were investigating the disappearance of 43 Mexican student protestors. *See id.*; *see also* Azam Ahmed, *Spyware in Mexico Targeted Investigators Seeking Students*, N.Y. Times (July 10, 2017), https://www.nytimes.com/2017/07/10/world/americas/mexico-missing-students-pegasus-spyware.html; John Scott-Railton *et al.*, Citizen Lab, *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware* (June 19, 2017), https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

c. In June 2018, an Amnesty International staff member received a WhatsApp message with a link that would have downloaded NSO's Pegasus spyware onto the

staff member's device. *See* Report ¶ 43. The WhatsApp message purported to provide the staff member with information about a protest outside the Saudi embassy in Washington, D.C., at a time when Amnesty International was actively involved in campaigning for the release of six women's rights activists detained in Saudi Arabia. Amnesty International, *The Surveillance Industry and Human Rights: Amnesty International Submission to United Nations Special Rapporteur* (Feb. 22, 2019), https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/AMNESTY%20INTERNATIONAL.pdf. The Pegasus attack would have allowed a hostile government to infiltrate, among other things, sensitive and encrypted communications internal to Amnesty International.

d. Saudi Arabia and the UAE have been credibly alleged to have used Pegasus as recently as the summer of 2020 to conduct invasive surveillance against dozens of journalists with the Al Jazeera network. Citizen Lab discovered that these governments deployed what is known as a "zero-click" attack, such that the spyware may be installed on the target's device surreptitiously without the target even clicking on a suspicious link or answering a call from an unknown number. *See, e.g.*, Bill Marczak *et al.*, Citizen Lab, *The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit* (Dec. 20, 2020), https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.

e. Like NSO's Pegasus product, spyware from a different company has been used to surveil pro-democracy activists. In 2012, emails purporting to contain documentation of regime abuses were sent to Bahraini pro-democracy activists and dissidents. The attached documentation, if clicked, would have covertly installed that spyware on recipients' computers. *See* Morgan Marquis-Boire & Bill Marczak, Citizen Lab, *From Bahrain With Love: FinFisher's Spy Kit Exposed?* (July 25, 2012), https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/.

3. *Surreptitious surveillance without any legal control violates fundamental rights enshrined in international law*. Regardless of whether the cyber-surveillance attempt is successful or the target is aware of it, unaccountable surveillance violates human rights that are protected by international law—including the International Covenant on Civil and Political Rights ("ICCPR"), which the United States ratified in 1992,[3] and the Universal Declaration of Human Rights, long considered the benchmark for the human rights that all people worldwide enjoy and that governments must promote and protect.[4]

---

[3] The ICCPR was adopted December 16, 1966; entered into force on March 23, 1976; and entered into force for the United States on September 8, 1992. *See* 999 U.N.T.S. 171.

[4] The Universal Declaration of Human Rights was adopted by the United Nations General Assembly in 1948. *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, arts. 12, 19, 20(1) (Dec. 10, 1948). The UN has specifically

Those instruments directly protect the rights to privacy and free expression with which cyber-surveillance interferes—particularly when it involves journalists or others to whom free expression is fundamental. *See* Report ¶¶ 23–25; *see also, e.g.*, ICCPR arts. 17 (freedom from interference with privacy), 19 (freedom of expression), 21 (freedom of assembly), 22 (freedom of association). Indeed, privacy and expression are intertwined in digital space, with online privacy serving as a gateway to secure exercise of the freedom of opinion and expression. *See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/29/32 (May 22, 2015), https://undocs.org/en/A/HRC/29/32; *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/23/40 ¶ 24 (April 17, 2013), https://undocs.org/en/A/HRC/23/40.

Article 17(1) of the ICCPR, echoing article 12 of the Universal Declaration, provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence." Report ¶ 23. Article 17 permits an interference with privacy only where "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant," is in pursuit of

---

recognized the threat posed by surveillance, with the UN General Assembly, for instance, condemning "unlawful or arbitrary surveillance" and communications interception as "highly intrusive acts" that interfere with fundamental human rights. A/RES/68/167 (Dec. 18, 2013); A/RES/71/199 (Dec. 19, 2016).

"a legitimate aim," and "meet[s] the tests of necessity and proportionality." *Report of the Special Rapporteur on the promotion and protection of fundamental human rights while countering terrorism* ¶ 30, A/69/397 (Sept. 23, 2014), https://undoc.org/en/A/63/397. Significant interference with privacy through unregulated spyware like Pegasus offers no assurance of even attempting to meet those basic standards.

Article 19 of both the ICCPR and the Universal Declaration "protects everyone's right to hold opinions without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media." Report ¶ 23. That basic provision of international law is a foundation of democratic societies. It may be subject to restriction only when meeting tests of legality, necessity and proportionality, and legitimacy of objective.

The ICCPR also imposes a duty on governments to protect individuals against third-party interference with those rights. In particular, Article 17(2) of the ICCPR "provides that everyone has the right to the protection of the law against unlawful interference with his or her privacy." Report ¶ 27. That obligation of protection against third parties echoes Article 2 of the ICCPR, which obligates States Parties not only to respect the rights in the ICCPR but to "ensure to all individuals within [their] territory and subject to [their] jurisdiction the rights" the ICCPR recognizes. ICCPR Art. 2(1).

The tools of the private surveillance industry are designed and used to evade exactly those fundamental human rights. To give one example of the impact of spyware like Pegasus, following a fact-finding mission to Mexico *amicus* found that targeted surveillance "create[d] incentives for self-censorship and directly undermine[d] the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information." Report ¶ 26 (citation omitted). Targeted surveillance may claim legitimate law enforcement and counter-terrorism purposes, when constrained by basic rule-of-law standards, practices, and enforcement, but it also poses undeniable risks to fundamental rights of expression, religion, association, privacy, and more.

II. A JUDICIAL REMEDY IS NECESSARY

In this case, WhatsApp seeks to enforce existing statutory and common-law duties against a private actor that has injured an American corporation. To avoid any such liability, NSO has attempted to cloak its own acts—including the steps that NSO takes to test, refine, and market its spyware before the point of sale and to provide service after sale—in immunity that is available only to sovereigns or (in limited circumstances) to natural persons acting on behalf of a sovereign. In support of that novel argument, NSO suggests as a policy matter that no liability is needed here to control its activities because its spyware sales are already subject to Israeli

export controls and NSO's own due diligence processes, which NSO says act as accountability mechanisms. *See* NSO Br. 16-17.

As an initial matter, *amicus* is aware of no support in international law for the novel extension of sovereign immunity principles that NSO proposes in this case. Providing NSO with immunity would mark an unprecedented extension of the limited immunity enjoyed by *states* and certain state actors in foreign courts and tribunals. *See* ICCPR art. 2(3)(a) (stating that "any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity").

Moreover, such a novel extension would directly contradict the trend in international law to hold private corporate actors responsible for the protection of human rights. In 2011, the UN Human Rights Council, the central human rights body of the UN system (of which the United States was an elected member at the time), endorsed the UN Guiding Principles on Business and Human Rights ("Guiding Principles"). *See* Human Rights Council Resolution 17/4, A/HRC/RES/17/4 (June 16, 2011). The Guiding Principles instrument, which is non-binding, reaffirms the obligations of states to ensure that business operations within their jurisdiction respect human rights and encourages businesses to "avoid infringing on the human rights of others" and to "address adverse human rights impacts with which they are involved." Office of the High Commissioner, Guiding

Principles, Principle 11, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf. As recently as September 2020, the U.S. State Department, in keeping with the Human Rights Council's endorsement of the Guiding Principles, issued guidance encouraging American businesses in the surveillance industry to meet their responsibilities "to respect human rights." U.S. Dep't of State, *Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities* (Sept. 30, 2020), https://www.state.gov/wp-content/uploads/2020/10/DRL-Industry-Guidance-Project-FINAL-1-pager-508-1.pdf.

NSO is also wrong to suggest that the existing mechanisms of export controls and self-regulatory commitments are sufficient as a practical matter to constrain the kinds of abuses described in this filing and in the reporting of international and non-governmental organizations. *See* pp. 7-13, *supra*. Export controls have not been an effective method of "reduc[ing] the risks caused by the private surveillance industry and the repressive use of its tools." Report ¶ 34 (concluding that the "effectiveness" of such controls is "limited"). A non-binding international arrangement in which the United States is a leading participant—the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies—exists to address export controls generally, but it is "ill-suited to addressing the threats that

targeted surveillance pose to human rights" because "it lacks guidelines or enforcement measures that would directly address human rights violations caused by surveillance tools." *Id*. Moreover, Israel, where NSO is headquartered, is not part of that arrangement. Israel has adopted its own export controls on "dual-use items regulated under the Wassenaar Arrangement," but its "enforcement of these controls is shrouded in secrecy." Report ¶ 38. For instance, after the Amnesty International incident described above, *see* p. 12, *supra*, Israel declined that organization's request that NSO's export license be revoked, and even refused to confirm or deny that such a license existed, *see* Report ¶ 43.

Similarly, NSO's own internal procedures evidently are far from effective to prevent abuses. *See* Letter of Special Rapporteur to Shalev Hulio, CEO, NSO Group Technologies (Feb. 20, 2020), https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25079. NSO is well aware of, and is alleged to provide support for, the malicious uses to which its technology is put. Still, as *amicus* explained in his Report, "[g]iven the nature of the industry and the widespread use of its products for purposes that are inconsistent with international human rights law, it is difficult to imagine" that NSO "do[es] in fact take such impacts into account." Report ¶ 29; *see id.* ("[G]iven the broad public knowledge of the repression practised by many of their clients, the companies cannot seriously claim to lack insight into the repressive uses of their tools."). There is no indication

that NSO (or any similar company) has taken "meaningful action," such as enacting *effective* "due diligence processes that identify and avoid causing or contributing to adverse human rights impacts through their own activities and that prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships." Report ¶ 32. To the contrary, NSO continues selling to—and then providing technical support to—repressive regimes. *See id.* ("mounting evidence of the industry's central role in facilitating gross human rights abuses, coupled with its steadfast refusal to explain its safeguards, makes it difficult to avoid the conclusion" that claims of "self-regulation lack[] substance").

Nor are there other governmental or private mechanisms, aside from bringing suits like the one before this Court, that are available to prevent or redress the serious violations of free speech, association, and privacy enabled by tools like NSO's. As *amicus* explained in his Report, "[a]lternatives to litigation, providing for remedies consistent with international human rights law, appear unavailable." Report ¶ 43; *see id.* ¶ 46 ("It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists."). That is particularly true given that entities like NSO sell their wares to, and operate across, many different countries across the world, making it unclear which of those countries could effectively regulate those entities. *See Report of the open-ended*

intergovernmental working group, A/HRC/22/41 at 3 (Dec. 24, 2012), https://undocs.org/en/A/HRC/22/41 (when "companies . . . operate transnationally," that operation presents special human rights challenges).

For those reasons, private liability like that sought in this case may well be the only currently viable way to hold NSO and similar entities accountable for their actions in infiltrating other companies' services and in assisting repressive regimes to commit human rights abuses. Extending common-law immunity to NSO in the United States thus would effectively *eliminate* the possibility of any redress for U.S. victims of NSO hacking and would ensure that private cyber-surveillance companies continue to inflict the many harms to which the design, maintenance, and sale of their products give rise. *See* WhatsApp Br. 48-51.

That result would be especially unwarranted given that NSO's proposed common-law immunity rule contradicts the United States's obligations under the ICCPR. The ICCPR requires ratifying nations not only "to give effect to the rights recognized" in the ICCPR, which include freedom of expression, association, assembly, and privacy, *see* pp. 14-16, *supra*, but also to "develop the possibilities of judicial remedy" and to "adopt such laws or other measures as may be necessary to give effect to the rights recognized" by the ICCPR, *id.* arts. 2(2), 2(3)(b).

NSO's proposed immunity rule cannot be squared with the United States's commitment to promote fundamental human rights through "develop[ing] the

possibilities of judicial remedy." *See* Report ¶ 39 ("The duty to provide effective remedies also entails an obligation to protect individuals from acts by private sector entities that cause infringements, by exercising due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities."); *see also id.* ¶ 55 ("States that are serious about the abuse of surveillance technologies should take steps to enable individual claims."). Interference with fundamental human rights is the unavoidable outcome of NSO's practices and its argument in this Court. But in NSO's view, neither it nor any other cyber-surveillance company has any enforceable obligations or duties towards any American corporation or citizen, so long as cyber-surveillance companies sell their spyware to governments rather than directly to private actors. That cannot be the law.

CONCLUSION

The decision of the district court should be affirmed.

Respectfully submitted,

s/Elaine J. Goldenberg

Elaine J. Goldenberg
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Avenue NW
Suite 500E
Washington, D.C. 20001-5369
202-220-1000
Elaine.Goldenberg@mto.com

Marianna Mao
MUNGER, TOLLES & OLSON LLP
560 Mission Street, 27th Floor
San Francisco, California 94105-2907
Marianna.Mao@mto.com

Counsel for Amicus Curiae

David Kaye
401 E. Peltason Dr.
Irvine, California 92697
dkaye@law.uci.edu

Amicus Curiae

DATED: December 23, 2020

CERTIFICATE OF COMPLIANCE

Form 8. Certificate of Compliance for Briefs

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

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

I am the attorney or self-represented party.

This brief contains 4,704 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

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

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[x] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
- [ ] it is a joint brief submitted by separately represented parties;
- [ ] a party or parties are filing a single brief in response to multiple briefs; or
- [ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/Elaine J. Goldenberg **Date** 12/23/20
(use "s/[typed name]" *to sign electronically-filed documents)*

CERTIFICATE OF SERVICE

I hereby certify that on December 23, 2020, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

DATED: December 23, 2020

Respectfully submitted,

MUNGER, TOLLES & OLSON LLP

By: s/Elaine J. Goldenberg
ELAINE J. GOLDENBERG