CASE 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,
Northern District of California, Case No. 4:19-cv-07123-PJH

BRIEF OF ACCESS NOW, AMNESTY INTERNATIONAL, COMMITTEE TO PROTECT JOURNALISTS, INTERNET FREEDOM FOUNDATION, PARADIGM INITIATIVE, PRIVACY INTERNATIONAL, RED EN DEFENSA DE LOS DERECHOS DIGITALES, AND REPORTERS WITHOUT BORDERS AS *AMICI CURIAE* IN SUPPORT OF APPELLEES' REQUEST FOR AFFIRMANCE

Stephanie Skaff (SBN 183119)
Deepak Gupta (SBN 226991)
Kyle A. McLorg (SBN 332136)
FARELLA BRAUN + MARTEL LLP
235 Montgomery Street, 17th Floor
San Francisco, California 94104
(415) 954-4400 Telephone
(415) 954-4480 Facsimile
Attorneys 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, Amnesty International, Committee to Protect Journalists, Internet Freedom Foundation, Paradigm Initiative, Privacy International, Red en Defensa de los Derechos Digitales, and Reporters Without Borders make the following disclosures:

1) For non-governmental corporate parties please list all parent corporations: None.

2) For non-governmental corporate parties please list all publicly held companies that hold 10% or more of the party's stock: None.

Dated: December 23, 2020

Respectfully submitted,

FARELLA BRAUN + MARTEL LLP

By: */s/ Kyle A. McLorg*
Kyle A. McLorg

Attorneys for Amici Curiae Access Now, Amnesty International, Committee to Protect Journalists, Internet Freedom Foundation, Paradigm Initiative, Privacy International, Red en Defensa de los Derechas Digitales, and Reporters Without Borders

TABLE OF CONTENTS

Page

I. IDENTITY AND INTEREST OF *AMICI CURIAE* 1

II. FACTUAL BACKGROUND 6

A. WhatsApp is an international communications platform with end-to-end encryption, which is essential for protecting civil society workers around the globe. 6

B. NSO's powerful spyware can take control of a target's mobile device with a single missed call. 7

C. Amici advocate in support of many of the civil society members who were targeted as a result of the 2019 WhatsApp attack 9

1. Placide Kayumba – In exile from Rwanda 10

2. Father Pierre Marie-Chanel Affognon – Togo 12

3. Fouad Abdelmoumni and Aboubakr Jamaï – Morocco 15

4. Bela Bhatia – India 21

III. ARGUMENT 25

A. NSO's government clients use Pegasus to violate international laws that protect the right to privacy and free expression 25

B. NSO continues to supply surveillance technology to its clients while knowing they use it to violate international law, failing to fulfill its responsibility to respect human rights 29

C. Without hope for accountability in their countries, this suit provides many of NSO's victims their only avenue for justice. 32

IV. CONCLUSION 35

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

Carpenter v. United States,
585 U.S. __, 138 S.Ct. 2206 (2018) (Roberts, C.J.) 26

OTHER AUTHORITIES

Alok Putul, *Indian gov't report: 17 Adivasi falsely dubbed Maoists, shot dead*, Al Jazeera (Dec. 4 2019), https://www.aljazeera.com/news/2019/12/4/indian-govt-report-17-adivasi-falsely-dubbed-maoists-shot-dead 21, 22

Awards 2003 – Jamai, Committee to Protect Journalists (2003), https://cpj.org/awards/jamai/ 19, 20

Ben Hubbard, *Someone Tried to Hack My Phone. Technology Researchers Accused Saudi Arabia*, New York Times (Jan. 28, 2020), https://www.nytimes.com/2020/01/28/reader-center/phone-hacking-saudi-arabia.html 9

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, & Ron Deibert, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, Citizen Lab (Sept. 18, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ 8, 11, 12

Chaim Levinson, *With Israel's Encouragement, NSO Sold Spyware to UAE and Other Gulf States*, Haaretz (Aug. 25, 2020), https://www.haaretz.com/middle-east-news/.premium-with-israel-s-encouragement-nso-sold-spyware-to-uae-and-other-gulf-states-1.9093465 8

David Kaye, *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools*, OHCHR (June 25, 2019), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736 29

David Kirkpatrick & Azam Ahmed, *Hacking a Prince, an Emir and a Journalist to Impress a Client*, New York Times (Aug. 31, 2018), https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html 7

Deborah Amos, *In Morocco, The Arab Spring's Mixed Bounty*, NPR (Feb. 7, 2012), https://www.npr.org/2012/02/07/146526685/in-morocco-the-arab-springs-mixed-bounty 16

E. Tendayi Achiume, *UN expert joins call for immediate moratorium on sale, transfer and use of surveillance tech*, OHCHR (July 15, 2020), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26098&LangID=E 30

Freedom Around The World 2020: Rwanda, Freedom House, https://freedomhouse.org/country/rwanda/freedom-world/2020 .....10, 33

Freedom Around the World: Togo, Freedom House, https://freedomhouse.org/country/togo/freedom-world/2020 .....13, 33

Freedom In The World 2020: Morocco, Freedom House, https://freedomhouse.org/country/morocco/freedom-world/2020 .....*passim*

From India to Rwanda, the victims of NSO Group's WhatsApp hacking speak out, Access Now (Dec. 17, 2020), https://www.accessnow.org/nso-whatsapp-hacking-victims-stories/ .....*passim*

Front Line Defenders, *Bela Bhatia – HRD*, https://www.frontlinedefenders.org/en/profile/bela-bhatia/ 23

Front Line Defenders, *Take Action for Bela Bhatia*, https://www.frontlinedefenders.org/en/action/take-action-bela-bhatia 23

Guiding Principles on Business and Human Rights, UN Human Rights OHCHR (2011), https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf 30, 31, 32

Jambo-asbl, http://www.jamboasbl.com/ 10

Indian Constitution, Fifth Schedule, https://www.mea.gov.in/Images/pdf1/S5.pdf 22

International Covenant on Civil and Political Rights (ICCPR) Article 17, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx 27

International Principles of the Application of Human Rights to Communications Surveillance, Electronic Frontier Foundation (May 2014), https://www.eff.org/files/necessaryandproportionatefinal.pdf 26

Jane Kramer, *The Crusader*, The New Yorker (Oct. 9, 2006), https://www.newyorker.com/magazine/2006/10/16/the-crusader-2 .....19, 20

Jimmy Carter, *U.S. Finally Ratifies Human Rights Covenant*, The Carter Center (June 28, 1992), https://www.cartercenter.org/news/documents/doc1369.html 27

John Scott-Railton, Siena Anstis, Sharly Chan, Bill Marczak, & Ron Deibert, *Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware*, Citizen Lab (Aug. 3, 2020), https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/ 12, 13, 15

Lewis Mudge, *Another Mysterious Opposition Death in Rwanda*, Human Rights Watch (Mar. 12, 2019), https://www.hrw.org/news/2019/03/12/another-mysterious-opposition-death-rwanda 11

Lorenzo Franceschi-Bicchierai & Joseph Cox, *They Got "Everything": Inside a Demo of NSO Group's Powerful iPhone Malware*, Vice (Sept. 20, 2018), https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo 7

Malini Subramaniam, *No change in Chhattisgarh yet, but I hope Congress will correct past wrongs: Activist Bela Bhatia*, Scroll.in (Jan. 13, 2019), https://scroll.in/article/909221/no-change-in-chhattisgarh-yet-but-i-hope-congress-will-correct-past-wrongs-activist-bela-bhatia 22

Mehul Srivastava & Robert Smith, *Israel's NSO: the business of spying on your phone*, Financial Times (May 13, 2019), https://www.ft.com/content/7f2f39b2-733e-11e9-bf5c-6eeb837566c5 .....7, 9

Mehul Srivastava & Tom Wilson, *Inside the WhatsApp hack: how an Israeli technology was used to spy*, Financial Times (Oct. 29, 2019), https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229.....10

Michelle Bachelet, *Human rights in the digital age*, keynote speech (Oct. 17 2019), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E 26

The Mobile Economy 2020, GSMA (March 5, 2020), https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf 26

Morgan Ortagus, Department Spokesperson, *Release of U.S. Department of State Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities*, U.S. Department of State (Sept. 30, 2020), https://www.state.gov/release-of-u-s-department-of-state-guidance-on-implementing-the-un-guiding-principles-for-transactions-linked-to-foreign-government-end-users-for-products-or-services-with-surveillance-capabilities/ 31, 32

Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools, Amnesty International (June 22 2020), https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/ 31

Morocco: Human Rights Defenders Targeted with NSO Group's Spyware, Amnesty International (Oct. 10 2019), https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/ 20

NSO Group / Q Cyber Technologies – Over One Hundred New Abuse Cases, Citizen Lab (Oct. 29, 2019), https://citizenlb.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/ 7

NSO Group responds to human rights violations, but comes up short, Access Now (Aug. 11, 2017), https://www.accessnow.org/nso-group-responds-human-rights-violations-comes-short/ 30

NSO Group's Website, https://www.nsogroup.com/ 8

NSO Group spyware used against Moroccan journalist days after company pledged to respect human rights, Amnesty International (June 22, 2020), https://www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist/ 31

OECD Guidelines for Multinational Enterprises, OECD (2011), http://dx.doi.org/10.1787/9789264115415-en 32

The Panchayats (Extension to the Scheduled Areas) Act, 1996, http://legislative.gov.in/sites/default/files/A1996-40.pdf 22

Patrick Howell O'Neill, *Inside NSO, Israel's billion-dollar spyware giant*, MIT Technology Review (Aug. 19, 2020), https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/ 17, 31

Patrick Howell O'Neill, *The man who built a spyware empire says it's time to come out of the shadows*, MIT Technology Review (Aug. 19, 2020), https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/ 8

Raksha Kumar, *As Bastar mob hounds researcher Bela Bhatia out of her home, little has changed for activists here*, Scroll.in (Jan. 24, 2017), https://scroll.in/article/827500/as-bastar-mob-hounds-researcher-bela-bhatia-out-of-her-home-little-has-changed-for-activists-here 22

Raluca Besliu, *Togo Rallies for Change After 50 Years of Rule by One Family*, New York Times (Nov. 4, 2017), https://www.nytimes.com/2017/11/04/world/africa/togo-protests-faure-gnassingbe.html 13

Ruth Michaelson, *Moroccan journalist jailed for abortion that she says never happened*, The Guardian (Sept. 30, 2019), https://www.theguardian.com/world/2019/sep/30/moroccan-journalist-hajar-raissouni-jailed-abortion 19

Rwanda: Repression Across Borders, Human Rights Watch (Jan. 28, 2014), https://www.hrw.org/news/2014/01/28/rwanda-repression-across-borders# 12

Security Forces in Chhattisgarh Burn Effigies of Petitioners, Journalist, Activists, The Wire (Oct. 25, 2016), https://thewire.in/rights/security-forces-chhattisgarh-burn-effigies-petitioners-journalists-activists 23

Sushovan Sircar, *Pegasus Spying Row: Ex-RSS Leader Withdraws Petition Seeking Probe*, The Quint (Dec. 2, 2019), https://www.thequint.com/news/india/govindacharya-withdraws-pil-supreme-court-whatsapp-pegasus-spyware-bobde#read-more 33

Togo—Shadow Report to the African Commission on Human and Peoples' Rights, Amnesty International (2018) at 14, https://www.amnesty.org/download/Documents/AFR5782022018ENGLISH.pdf 13

Togo: Spiraling violence and repressive cybersecurity law hit the country ahead of contested parliamentary elections, Amnesty International, (Dec. 13, 2018), https://www.amnesty.org/en/latest/news/2018/12/togo-spiraling-violence-and-repressive-cybersecurity-law/ 13

UN General Assembly, Human Rights Committee, *Concluding observations on the fourth periodic report of the United States of America*, ¶ 22 (Apr. 23, 2014), https://undocs.org/CCPR/C/USA/CO/4 29

UN General Assembly, Human Rights Committee, *General Comment No. 34*, ¶ 22 (Sept. 12, 2011), https://undocs.org/CCPR/C/GC/34 27

UN General Assembly, Human Rights Council, *Report of the Office of the United Nations High Commissioner for Human Rights*, ¶ 14 (June 30, 2014), https://undocs.org/A/HRC/27/37 .....26, 28, 34

UN General Assembly, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, at ¶ 21 (May 28, 2019), https://undocs.org/A/HRC/41/35 25

UN General Assembly, Human Rights Council, *The right to privacy in the digital age*, ¶ 23 (June 30, 2014), https://undocs.org/A/HRC/27/37 27

UN General Assembly, *Resolution 73/179*, *"The right to privacy in the digital age,"* (Jan. 21 2019), https://undocs.org/en/A/RES/73/179 28

The United Nations Guiding Principles on Business and Human Rights (UNGPs) Section II, https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.....29

Universal Declaration of Human Rights (UDHR) Article 12, https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf.....26

WhatsApp, *WhatsApp Security*, https://www.whatsapp.com/security/?lang=en#:~:text=WhatsApp's%20end%2Dto%2Dend%20encryption,in%20between%2C%20not%20even%20WhatsApp 6

I. IDENTITY AND INTEREST OF *AMICI CURIAE*[1]

The question in this appeal is straightforward: Can Appellant NSO Group ("NSO"), a privately-owned company, piggyback on the immunity of sovereign governments, simply because its clients are governmental entities? As is clear from the parties' briefing, and as the court below recognized, it cannot. Holding otherwise would break with decades of foreign sovereign immunity law. And because NSO is a private company, unbound by traditional notions of intergovernmental fair play and reciprocity, immunity invites it to continue assaulting American technology companies and their customers for the sole purpose of generating profit.

But the implications of this Court's holdings reach further than that and, indeed, to the very core of the principles that America represents and international law protects. NSO's Pegasus is an insidious spyware product, and many of NSO's customers are repressive regimes that use Pegasus for insidious ends. For those regimes, the concern is not terrorism or criminal activity, but rather the threat posed by the work of activists, journalists, and lawyers to advance human rights, press freedom, and justice. Granting NSO immunity would not just undermine

[1] Pursuant to FEDERAL RULE OF APPELLATE PROCEDURE 29(a)(4)(e), Amici certify that no party's counsel authored this brief in whole or in part, and no person or entity other than Amici, its members, or its counsel contributed money that was intended to fund preparing or submitting of this brief. Websites cited in this brief were last visited December 20, 2020.

fundamental international legal protections for privacy, free expression, and association, it would seriously undermine civil society.

Amici Curiae Access Now, Amnesty International, Committee to Protect Journalists, Internet Freedom Foundation, Paradigm Initiative, Privacy International, Red en Defensa de los Derechos Digitales, and Reporters Without Borders, are eight international non-governmental organizations that advocate for and endeavor to protect fundamental human rights and rule of law. These amici work alongside the civil society actors targeted with NSO's spyware, including many of the more than 100 people targeted as a result of the WhatsApp breach. 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 and this appeal, 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 users around the world, with particular focus on privacy and data protection, freedom of expression and assembly, digital security and connectivity. It began as an emergency response team of technologists working to help people get back online and ensure safe communications after the Iranian government blocked internet access and censored content during the 2009 Iranian election. It now has a team of more than 80 people

across 15 countries. Recognizing that in the 21st century, the threat of digital rights violations compound where they intersect with human rights abuses, Access Now works to hold governments and companies accountable for such violations and abuses in courts around the globe.

Amnesty International is a worldwide movement of more than seven million people working for the respect, protection, and fulfillment of internationally recognized human rights. The movement has members and supporters in more than 150 countries and territories, and is independent of any government, political ideology, economic interest, or religion. Amnesty International bases its work on international human rights instruments adopted by the United Nations and regional bodies, and has intervened and filed amicus briefs in many cases involving human rights issues before national and international courts.

Committee to Protect Journalists (CPJ) is an independent, nonprofit organization that promotes press freedom worldwide. It defends the rights of journalists to report the news safely and without fear of reprisal, including targeting by surveillance systems like the technology that NSO deployed in the incident that gave rise to this case. When press freedom violations occur, CPJ mobilizes a network of correspondents who report and take action on behalf of

those targeted, regardless of whether those violations occur in repressive countries, conflict zones, or established democracies.

Internet Freedom Foundation (IFF) is a digital rights organization in India. Its work includes surveillance reforms, and it is a petitioner in a case before the Supreme Court of India challenging the constitutionality of India's electronic surveillance law, which allows the government to intercept, monitor, and decrypt information from targets without independent judicial oversight. As an organization, it has supported NSO's victims with advice about obtaining remedies, including providing an initial statement, making representations to the State Governments of Maharashtra and Chhattisgarh, and engaging on the issue with the Standing Committees of Parliament.

Paradigm Initiative (PIN) builds ICT-enabled support systems and advocates for digital rights in order to improve the livelihoods of underserved young Africans. PIN's digital rights advocacy program is focused on the promotion of a positive rights environment and support of public policy toward internet freedom in various regions of Africa, including Nigeria, Ghana, Kenya, Zambia, Zimbabwe, and Cameroon. PIN has led efforts to promote freedom of expression and privacy by challenging surveillance regimes, strategizing on navigating oppressive environments where freedom of expression is under threat, challenging government-implemented internet shutdowns around elections, and

developing frameworks for rights-respecting legislation. Much of this work has been undertaken in the very countries that have been listed as NSO's clients.

Privacy International exists to protect people's privacy, dignity, and freedoms from abuses at the hands of both private companies and governments. It recognizes that safeguards are essential to combat the growing embrace of intrusive technological surveillance around the world. Through research, investigation, and advocacy, Privacy International seeks to build a better future where technologies, laws, and policies contain modern safeguards to protect people and their data from exploitation.

Red en Defensa de los Derechos Digitales (R3D) is a Mexican organization dedicated to defending human rights in the digital environment. It uses various legal and communication tools for policy research, strategic litigation, advocacy, and campaigns to defend digital rights, including the right to privacy, freedom of expression, and access to knowledge. In addition to this work, R3D maintains a permanent investigation into the technological capability of Mexico's federal and local authorities to intervene on communications and invade individuals' privacy.

Reporters without Borders, also known under its French name Reporters Sans Frontières (RSF), is an international non-governmental organization defending freedom, independence, and pluralism of journalism. RSF advocates against surveillance of journalists and their sources to protect the safety of

journalists around the world and prevent censorship of a free press, both of which are endangered by NSO's technology and activities.

Amici's interest in the outcome of this appeal is substantial. They have filed this brief in order to draw this Court's attention to the grave human rights and international law concerns that weigh heavily against granting NSO's unprecedented immunity demand in this case.

II. FACTUAL BACKGROUND

A. WhatsApp is an international communications platform with end-to-end encryption, which is essential for protecting civil society workers around the globe.

WhatsApp is an international communications platform that allows users to send messages, make voice calls, and host video chats on computers and cellphones. Dkt. 1 ¶¶ 17-18. 1.5 billion people use WhatsApp, both because of its worldwide connectivity and its robust privacy protections. *Id*. at ¶ 15. WhatsApp's end-to-end encryption acts as a digital lock on communications, ensuring that only the sender and recipient can read or listen to what is sent.[2]

This privacy is important for all users, but especially for civil society actors, whose work invites attack from powerful governments. Whether planning a peaceful protest, speaking to a source for investigative reporting, or making

[2] WhatsApp, *WhatsApp Security*, https://www.whatsapp.com/security/?lang=en#:~:text=WhatsApp's%20end%2Dto%2Dend%20encryption,in%20between%2C%20not%20even%20WhatsApp.

privileged communications with a client, these actors choose encrypted technologies like WhatsApp to prevent those governments from intercepting communications and conducting intrusive surveillance.

B. NSO's powerful spyware can take control of a target's mobile device with a single missed call.

Between April and May 2019, NSO's Pegasus surveillance technology was used to exploit previously-unknown vulnerabilities in WhatsApp's servers against over 1,400 individuals across the globe. Dkt. 1, ¶ 1. Widespread media reports describe the ease with which Pegasus achieves its ends. "[J]ust one simple missed call on WhatsApp" allows Pegasus to "drop its payload" and access everything, from email and messages to the phone's microphone, camera, and GPS coordinates.[3] Using WhatsApp as a vector, NSO's spyware can take control of a cellphone and extract boundless information about a target in real time.

[3] Mehul Srivastava & Robert Smith, *Israel's NSO: the business of spying on your iPhone*, Financial Times (May 13, 2019), https://www.ft.com/content/7f2f39b2-733e-11e9-bf5c-6eeb837566c5; *see also* Lorenzo Franceschi-Bicchierai & Joseph Cox, *They Got "Everything": Inside a Demo of NSO Group's Powerful iPhone Malware*, Vice (Sept. 20, 2018), https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo; David Kirkpatrick & Azam Ahmed, *Hacking a Prince, an Emir and a Journalist to Impress a Client*, New York Times (Aug. 31, 2018), https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html; *NSO Group / Q Cyber Technologies – Over One Hundred New Abuse Cases*, Citizen Lab (Oct. 29, 2019), https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/.

NSO markets Pegasus as a tool for fighting crime and terrorism.[4] It has told this Court that it is "subject to strict regulation" by the Israeli Ministry of Defense, which "mandate[s] that NSO require its users to certify that Pegasus 'will be used only for prevention and investigation of terrorism and criminal activity.'" *See* Appellant's Br. 16. But these claims are disingenuous. The Israeli Ministry of Defense has reportedly never denied NSO an export license.[5] And the loophole in this policy speaks for itself: many of the countries on NSO's rolodex criminalize dissent and human rights defense work.[6]

Investigations by The Citizen Lab at the University of Toronto reveal NSO's disingenuity. Between 2016 and 2018, it found that Pegasus had proliferated into 45 countries, including several that had either "previously been linked to abusive use of spyware to target civil society" or had "dubious human rights records and histories of abusive behaviour by state security services."[7] And after investigating

---

[4] *See, e.g.*, NSO Group's Website, https://www.nsogroup.com/.

[5] Patrick Howell O'Neill, *The man who built a spyware empire says it's time to come out of the shadows*, MIT Technology Review (Aug. 19, 2020), https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/.

[6] Chaim Levinson, *With Israel's Encouragement, NSO Sold Spyware to UAE and Other Gulf States*, Haaretz (Aug. 25, 2020), https://www.haaretz.com/middle-east-news/.premium-with-israel-s-encouragement-nso-sold-spyware-to-uae-and-other-gulf-states-1.9093465.

[7] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, & Ron Deibert, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, Citizen Lab (Sept. 18, 2018), https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

the 2019 WhatsApp incident, it identified over 100 cases of abusive targeting of human rights defenders, journalists, lawyers, international investigators, political opposition groups, and other civil society actors, both American and foreign, in 20 different countries.[8]

C. Amici advocate in support of many of the civil society members who were targeted as a result of the 2019 WhatsApp attack.

Amici stand alongside many of these individuals, who work to advance human rights around the globe. Some are forced into exile under threat of interminable prison sentences or execution.[9] Others remain within their home countries' borders, although the threat of retribution for their work is the same. All understand the danger they face when speaking truth to immense power. Some of these victims' stories, told below, shed crucial light on the devastating impact of NSO's invasive spyware and the danger it will continue to pose to human rights pioneers if NSO is not held accountable.

[8] Citizen Lab, *supra* note 3; *see also* Ben Hubbard, *Someone Tried to Hack My Phone. Technology Researchers Accused Saudi Arabia*, New York Times (Jan. 28, 2020), https://www.nytimes.com/2020/01/28/reader-center/phone-hacking-saudi-arabia.html.

[9] *See infra*, Section II.C.1.

1. Placide Kayumba – In exile from Rwanda

The Rwandan Patriotic Front (RPF), led by President Paul Kagame, has ruled Rwanda for 19 years.[10] Although the regime has brought stability and economic growth to Rwanda, it has also suppressed political opposition through surveillance, intimidation, and violence, both within Rwanda's borders and abroad.[11] And with Pegasus, the RPF now has a dangerous arrow in its quiver, allowing it to more precisely surveil its targets, who increasingly work in exile out of fear of assassination.

One such target is Placide Kayumba. Kayumba fled Rwanda in 1994,[12] and in 2008, while studying in Belgium, he co-founded and served as the first president of Jambo-asbl, a non-profit organization seeking to raise awareness regarding human rights in Rwanda.[13] He later joined Victoire Ingabire in the FDU-Inkingi opposition party.[14]

---

[10] *Freedom Around The World 2020: Rwanda*, Freedom House, https://freedomhouse.org/country/rwanda/freedom-world/2020.
[11] *Id.*; *see also* Mehul Srivastava & Tom Wilson, *Inside the WhatsApp hack: how an Israeli technology was used to spy*, Financial Times (Oct. 29, 2019), https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229. Opposition can be deadly. Since 1997, dozens of Rwandans have been injured, killed, or disappeared outside of Rwanda's borders, and authorities in Britain, France, Belgium, and Canada have warned Rwandan activists of plots to assassinate them.
[12] Srivastava & Smith, *supra* note 3; *see also From India to Rwanda, the victims of NSO Group's WhatsApp hacking speak out*, Access Now (Dec. 17, 2020), https://www.accessnow.org/nso-whatsapp-hacking-victims-stories/.
[13] For more information about Jambo asbl, *see* http://www.jamboasbl.com/.
[14] Srivastava & Wilson, *supra* note 11.

Kayumba has always known that this work is dangerous, as "all of [his] colleagues at the center of the party are monitored and threatened on a daily basis with assassination, disappearance, [and] imprisonment."[15] In 2016, FDU-Inkingi member Illuminée Iragena went missing and has never been found.[16] In 2018, the deputy leader of the FDU-Inkingi, Boniface Twagirimana, disappeared from his prison cell in southern Rwanda, and is presumed dead.[17] He had been held there on sham state security charges stemming from a free speech crackdown following the country's 2017 elections.[18] And in 2019, the body of Anselme Mutuyimana, an assistant to Ingabire, was found strangled in a forest in northwestern Rwanda.[19]

So Kayumba was not surprised to learn that Rwanda was utilizing NSO's technology.[20] Nor was he surprised when Citizen Lab and WhatsApp confirmed that he had been targeted.[21]

Still, the surveillance has impacted Kayumba and his work significantly. He once believed that WhatsApp was safe, but now he distrusts all technology, and

---

[15] *Id.*
[16] Lewis Mudge, *Another Mysterious Opposition Death in Rwanda*, Human Rights Watch (Mar. 12, 2019), https://www.hrw.org/news/2019/03/12/another-mysterious-opposition-death-rwanda.
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] Access, *supra* note 12; *see also* Marczak, *supra* note 7.
[21] Access, *supra* note 12; Srivastava & Wilson, *supra* note 11.

believes in person conversations are the only way to safely communicate.[22] He worries about his loved ones, because "they know about your family, where your children go to school. When you exchange messages, you don't know whether someone else could have them, that has criminal plans against you."[23] And now he fears that he cannot move freely.[24] This is true in Africa, where Kagame's regime can and has tracked and murdered its opponents, but it is also true in Belgium, where RPF cells are known to operate.[25] Even decades after leaving his home, Kayumba is still not safe.

2. Father Pierre Marie-Chanel Affognon – Togo

The NSO-linked attack on WhatsApp coincided with nation-wide protests in the West African country of Togo demanding constitutional reforms, including limiting the presidential mandates to two terms, in anticipation of its 2020 election.[26] Those protests were not the country's first: Two years after President Faure Gnassignbe was re-elected to a third mandate in 2015, opposition parties and

---

[22] Access, *supra* note 12.
[23] *Id*.
[24] *Id*.
[25] *Id*.; *see also Rwanda: Repression Across Borders*, Human Rights Watch (Jan. 28, 2014), https://www.hrw.org/news/2014/01/28/rwanda-repression-across-borders#.
[26] John Scott-Railton, Siena Anstis, Sharly Chan, Bill Marczak, & Ron Deibert, *Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware*, Citizen Lab (Aug. 3, 2020), https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/.

civil society groups organized massive demonstrations demanding reform.[27] Togo's government severely repressed the demonstrations by shutting down the internet and dispelling the crowds with live ammunition, tear gas, and batons.[28] The violent clashes left 11 people dead, including three children between the ages of 11 and 14.[29] Since then, the government has used oppressive laws, violence, arbitrary detentions, torture, and inhumane prison conditions to continue repressing opposition groups and civil society activists.[30]

In the lead up to the 2020 election, NSO's spyware was used to target phones belonging to several members of the Catholic church in Togo.[31] One of those targets was Father Pierre Marie-Chanel Affognon, a practicing priest, the founder of a movement to promote constitutional, institutional, and electoral

---

[27] *Freedom Around the World: Togo*, Freedom House, https://freedomhouse.org/country/togo/freedom-world/2020.
[28] *Togo—Shadow Report to the African Commission on Human and Peoples' Rights*, Amnesty International (2018) at 14, https://www.amnesty.org/download/Documents/AFR5782022018ENGLISH.pdf.
[29] Raluca Besliu, *Togo Rallies for Change After 50 Years of Rule by One Family*, New York Times (Nov. 4, 2017), https://www.nytimes.com/2017/11/04/world/africa/togo-protests-faure-gnassingbe.html.
[30] *Togo: Spiraling violence and repressive cybersecurity law hit the country ahead of contested parliamentary elections*, Amnesty International, (Dec. 13, 2018), https://www.amnesty.org/en/latest/news/2018/12/togo-spiraling-violence-and-repressive-cybersecurity-law/; Scott-Railton, *supra* note 26.
[31] Railton, *supra* note 26.

reform in the country, and a vocal critic of the human rights violations committed by Togolese authorities.[32]

The 2019 targeting of Father Affognon with Pegasus followed attempts by the Togolese government to undermine him. In 2018, it began an extensive disinformation campaign to smear him.[33] That campaign continued into 2019, and when the writings started to include information about his private life and his closest loved ones, he began to suspect that the government was successfully surveilling him.[34] It could only have obtained this information, Father Affognon says, by infiltrating his cellphone.[35]

Both WhatsApp and Citizen Lab later confirmed that he had been targeted with NSO's spyware.[36] The impact on Father Affognon has been "painful" and "difficult to describe."[37] He says "it is exactly like being undressed by someone in public, stripped naked, and you are powerless before an invisible hand and a terrifying faceless force."[38] And of course, Father Affognon thinks about his country.[39] He finds it "an enormous shock when one considers the public money

---

[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*; *see also* Access, *supra* note 12.
[36] Access, *supra* note 12.
[37] *Id.*
[38] *Id.*
[39] *Id.*

spent on acquiring the Israeli software whilst in my country, Togo, there is destitution everywhere."[40]

In May 2019, the National Assembly instituted presidential term limits, but the Constitutional Court validated Gnassignbe's fourth-term candidacy.[41] He went on to win the 2020 election despite opposition accusations of irregularities and voter fraud.[42] Following the election, the government placed the retired Archbishop of Lomé under house arrest for questioning the results.[43] And in July 2020, Togo issued an arrest warrant for Gnassingbe's primary opposition candidate.[44]

3. Fouad Abdelmoumni and Aboubakr Jamaï – Morocco

One day in Marrakech is all it takes to recognize that there are two Moroccos. While a sliver of its residents live in "large villas with extra rooms for a full-time butler and a chauffeur," a short walk down a dirt road leads to the homes of the wider Marrakech population, built of concrete blocks and mud and devoid of

[40] *Id*.
[41] Scott-Railton, *supra* note 26.
[42] *Id*. During the election, the government suspended opposition-friendly newspapers and forbade the Catholic church from poll-monitoring.
[43] *Id*.
[44] *Id*.

electricity and running water.[45] This unflinching juxtaposition typifies life in one of the Arab world's most economically unbalanced countries.[46]

Veterans of Morocco's civil society movement, which grew under King Hassan II's repressive reign in the 1970s and 1980s, saw reason to believe this contrast would lessen during the early tenure of Hassan's successor and son, King Mohammed VI.[47] In response to nationwide protests in 2011, he passed constitutional reforms and appeared to concede to growing demands for a true parliamentary democracy, freedom, and equality.[48]

But even as the Justice and Development Party led coalition governments following those reforms, Mohammed VI retained entire control, both through his ability to rule by decree and the immense economic power that he wields as one of Morocco's most powerful businessmen.[49] Nepotism and corruption thrive, while lack of political will maintains the status quo over two decades in.[50]

The Moroccan government wages a multi-front war to quell the protest, activism, and civil society movements that boil as a result. It has a troubling

---

[45] Deborah Amos, *In Morocco, The Arab Spring's Mixed Bounty*, NPR (Feb. 7, 2012), https://www.npr.org/2012/02/07/146526685/in-morocco-the-arab-springs-mixed-bounty.
[46] *Id*.
[47] Freedom In The World 2020: Morocco, *Freedom House*, https://freedomhouse.org/country/morocco/freedom-world/2020.
[48] Amos, *supra* note 45.
[49] *Id*. Freedom House, *supra* note 47.
[50] *Id*.

history of meeting assembly with force, most notably in 2017, when it deployed forces to bring the Hirak Rif protest movement to a brutal halt.[51] And it routinely targets NGOs seeking to work in Morocco, denying registration and pressuring venue owners and security forces to block those NGOs from accessing event spaces.[52]

But it also targets activists directly, and as Fouad Abdelmoumni discovered over the last two years, it has gained a powerful tool to do so in Pegasus. Abdelmoumni is a 62-year-old human rights activist in Morocco, currently working as a board advisor for Human Rights Watch and a campaigner for Transparency International.[53] He regularly speaks out against authoritarianism, corruption, and predation in Morocco and abroad.[54] And he speaks from experience: At just 20 years old, Hassan II's regime subjected him to torture, imprisonment, and several years of enforced disappearance for his activism.[55]

Since his phone was targeted with Pegasus,[56] Morocco's regime-friendly press, which regularly targeted Abdelmoumni with false stories, began peppering

---

[51] *Id*.
[52] *Id*.
[53] Access, *supra* note 12.
[54] *Id*.
[55] *Id*.
[56] Patrick Howell O'Neill, *Inside NSO, Israel's billion-dollar spyware giant*, MIT Technology Review (Aug. 19, 2020), https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/.

those articles with facts that could only be obtained by accessing his private spaces, documents, and communications.[57] In February 2020, anonymous individuals sent six sexually explicit videos depicting him and his partner, or people who closely resemble them, to dozens of people.[58] The government increasingly harassed Abdelmoumni during the following months, burdening him with tax audits and inexplicably cancelling investment grants worth over $30,000.[59] And in October 2020, the government-controlled press expanded its assault, this time publishing confidential information about his friends, including the family status of an 11-year-old child.[60]

All of this has left Abdelmoumni feeling "invaded, harassed and severely violated."[61] He always assumed that Morocco could surveil him, but never imagined it could obtain his private, secure WhatsApp communications, likely feeding a deliberate campaign to blackmail and terrorize him.[62] And though Abdelmoumni sought transparency and accountability when he joined seven other victims requesting an investigation by the National Control Commission for the

[57] Access, *supra* note 12.
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.*

Protection of Personal Data, the commission failed to respond beyond claiming it did not have jurisdiction.[63]

As Abdelmoumni's experience makes clear, the monarchy acts with impunity, especially from the media. Independent press is scarce in Morocco, and the state clamps down on critical reporting through draconian economic and legal sanctions, including pretextual criminal charges.[64]

Aboubakr Jamaï experienced this pushback firsthand. Jamaï spent over a decade as a journalist in Morocco, where he founded two weekly magazines, Le Journal Hebdomadaire and Assahifa al-Ousbouiya.[65] These groundbreaking outlets featured dogged reporting on governmental and corporate corruption, editorials critical of the king, and advocacy for a true constitutional democracy in Morocco.[66] His work received international acclaim, including the Committee to Protect Journalists' International Press Freedom Award in 2003.[67]

---

[63] *Id*.
[64] Freedom House *supra* note 47; *see also* Ruth Michaelson, *Moroccan journalist jailed for abortion that she says never happened*, The Guardian (Sept. 30, 2019), https://www.theguardian.com/world/2019/sep/30/moroccan-journalist-hajar-raissouni-jailed-abortion (Moroccan journalist critical of government imprisoned for fabricated abortion and premarital sex charges).
[65] Access, *supra* note 12.
[66] *Awards 2003 – Jamai*, CPJ (2003), https://cpj.org/awards/jamai/; Jane Kramer, *The Crusader*, The New Yorker (Oct. 9, 2006), https://www.newyorker.com/magazine/2006/10/16/the-crusader-2.
[67] CPJ, *supra* note 66.

But the work was also "a thorn in the side of the monarchy and the king because it [was] stubbornly uncorrupted," and the monarchy responded in kind.[68] The Moroccan Ministry of Communications banned both outlets on multiple occasions, and Jamaï was convicted of defamation, subjecting him to substantial fines.[69] Jamaï was forced out of Morocco in 2007, and in 2010, a state-led advertisement boycott bankrupted the publications.[70]

Jamaï now works as a consultant and professor in France.[71] While reporting in Morocco, Jamaï always assumed the state was tapping his phone, but in France, he hoped he could work without fear that Moroccan surveillance would jeopardize his reporting or professional relationships.[72] Not so. Twice in as many years, Moroccan state-friendly media outlets have leaked confidential work that Jamaï undertook for his consulting clients, including content it could only have obtained from his phone.[73] The impact on Jamaï's business cannot be overstated: since

[68] Kramer, *supra* note 66.
[69] CPJ, *supra* note 66.
[70] Access, *supra* note 12.
[71] *Id*.
[72] *Id*.
[73] *Id*.

Citizen Lab confirmed that his phone was targeted with Pegasus,[74] many clients have declined to use him for consulting work.[75]

Jamaï's personal relationships have suffered as well. Most of his family lives in Morocco, and although he occasionally visits them, they mostly communicate by phone.[76] These conversations are now emotionally distressing for Jamaï and his family, because they know that Pegasus allows the Moroccan state to listen.[77] Family reaches out less now, for reasons he sadly understands.[78] As he notes, "[y]ou put at risk your relatives and friends by the mere fact of freely talking to them on the phone."[79]

4. Bela Bhatia – India

Chhattisgarh, India has become ground zero for a vicious fight between the Indian government and some of its communities. Mining companies, alongside the government, have spent decades excavating the land to extract the state's rich mineral deposits,[80] in contravention of the special protections that the Indian

---

[74] *See also Morocco: Human Rights Defenders Targeted with NSO Group's Spyware*, Amnesty International (Oct. 10, 2019), https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/.
[75] Access, *supra* note 12.
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] Alok Putul, *Indian gov't report: 17 Adivasi falsely dubbed Maoists, shot dead*, Al Jazeera (Dec. 4, 2019), https://www.aljazeera.com/news/2019/12/4/indian-govt-

Constitution provides its native populations.[81] And in recent decades, the state has become a stronghold for the Communist Party of India (Maoist), an armed movement that the Indian government has deployed tens of thousands of troops to combat.[82] More than 4,000 people have been killed in Chhattisgarh since 2001, and the Adivasi people native to the region are caught in this crossfire. The State Police has jailed numerous Adivasis under false accusations of being Maoists.[83] Security forces have tortured, raped, and murdered countless more.[84]

Bela Bhatia is a researcher, activist, and lawyer, who has lived in Bastar, Chhattisgarh since 2015.[85] Her work focuses on protecting the rights and dignity of those Adivasi natives, whose lives have been turned upside down by both the mining activities that displace them and the counterinsurgency operations that have

---

report-17-adivasi-falsely-dubbed-maoists-shot-dead (noting that renewed mining activity in Chhattisgarh has displaced thousands of Adivasis).

[81] *See* The Panchayats (Extension to the Scheduled Areas) Act, 1996, http://legislative.gov.in/sites/default/files/A1996-40.pdf; *see also* Indian Constitution, Fifth Schedule, https://www.mea.gov.in/Images/pdf1/S5.pdf.

[82] Putul, *supra* note 83.

[83] *Id*.

[84] *Id*.; *see also* Raksha Kumar, *As Bastar mob hounds researcher Bela Bhatia out of her home, little has changed for activists here*, Scroll.in (Jan. 24, 2017), https://scroll.in/article/827500/as-bastar-mob-hounds-researcher-bela-bhatia-out-of-her-home-little-has-changed-for-activists-here (noting the National Human Rights Commission indicted security personnel for the rape of 16 Adivasi women in 2015 and 2016).

[85] Malini Subramaniam, *No change in Chhattisgarh yet, but I hope Congress will correct past wrongs: Activist Bela Bhatia*, Scroll.in (Jan. 13, 2019), https://scroll.in/article/909221/no-change-in-chhattisgarh-yet-but-i-hope-congress-will-correct-past-wrongs-activist-bela-bhatia.

wrought atrocities.[86] In 2015 and 2016, Bhatia joined other women activists to expose two instances of gang rape and sexual assault allegedly perpetrated by security forces, and assisted those victims in filing complaints with the Bijapur police.[87] She helped the National Human Rights Commission investigate and release a press note accusing Chhattisgarh police of raping at least 16 women.[88] And she has helped prepare reports and served on planning commission panels examining governance challenges in conflict areas, like the district of Bastar, where she lives.[89]

This work has made her a target for both the Indian government and vigilantes, who have viewed her as a "Naxalite agent," or Maoist sympathizer. In 2016, uniformed police officers burned effigies of Bhatia and several other activists in the streets of Chhattisgarh.[90] In that same year, over 100 anti-Naxal agitators stormed the Parpa village hoping to expel Bhatia, waving banners that read "Naxal supporter, leave Bastar" and passing out leaflets that read "Know the

---

[86] *Id.*
[87] Front Line Defenders, *Bela Bhatia – HRD*, https://www.frontlinedefenders.org/en/profile/bela-bhatia/.
[88] Front Line Defenders, *Take Action for Bela Bhatia*, https://www.frontlinedefenders.org/en/action/take-action-bela-bhatia.
[89] *Id.*
[90] *Security Forces in Chhattisgarh Burn Effigies of Petitioners, Journalist, Activists*,The Wire (Oct. 25, 2016), https://thewire.in/rights/security-forces-chhattisgarh-burn-effigies-petitioners-journalists-activists.

Naxal broker Bela Bhatia who is living amidst you."[91] And in 2017, over 30 men approached Bhatia's home, demanding she leave the village and threatening to burn down her home and kill her dog if she failed to comply.[92]

For Bhatia, this type of harassment is expected—and so is surveillance. Bhatia has always assumed that her phone was tapped, and her movements were tracked, long before the 2019 Pegasus attack.[93] So when Citizen Lab informed her that she had been targeted, she viewed it as the continuation of a years-long surveillance campaign by the Indian government in a more sophisticated package.[94]

This should not understate the impact that the surveillance has had on Bhatia's life. She now operates from a baseline of suspicion and restricts her activities.[95] Though she had toiled to build trust among her neighbors in the community, maintaining that trust has become more difficult. The surveillance has also made her more vulnerable.[96] She lives in constant apprehension of arrest on false charges—something she has seen happen to many of her fellow activists around India over the last few years.[97]

---

[91] Kumar, *supra* note 87.
[92] *Id.*
[93] Access, *supra* note 12.
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*

The stories above represent a small sampling of the victims of NSO's spyware, who are willing to speak publicly about what they have endured. So many more must stay silent—their lives depend on it. Their silence does not make them any less brave, nor does it lessen their suffering, fear, and isolation. And the impact of Pegasus-enabled surveillance extends beyond those directly affected, because in "environments subject to rampant illicit surveillance, the targeted communities know of or suspect such attempts at surveillance, which in turn shapes and restricts their capacity to exercise the rights to freedom of expression, association, religious belief, culture and so forth."[98] In countries haunted by NSO's surveillance technology, no one is free.

III. ARGUMENT

A. NSO's government clients use Pegasus to violate international laws that protect the right to privacy and free expression.

Mobile technology is ubiquitous. As of 2020, two-thirds of the world's population accesses telecom services with a mobile device,[99] which, in addition to holding intimate personal information, "faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters,

[98] UN General Assembly, Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, ¶ 21 (May 28, 2019), https://undocs.org/A/HRC/41/35.
[99] *The Mobile Economy 2020*, GSMA (March 5, 2020), https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf.

and other potentially revealing locales." *Carpenter v. United States*, 585 U.S. __, 138 S. Ct. 2206, 2214 (2018) (Roberts, C.J.). This creates new avenues for abusive surveillance by states and other actors, who increasingly "use digital surveillance tools to track down and target rights defenders and others perceived as critics."[100]

Digital surveillance threatens several human rights enshrined in international law, including the rights to information, peaceful assembly, family life, and health.[101] Individuals who would otherwise use technology to obtain or transmit information, plan a peaceful gathering, communicate with family, or share sensitive health information are chilled from doing so by the mere threat that their government could be listening.

The rights most directly threatened by surveillance technology like Pegasus are the rights to free expression and privacy, which are inextricably bound and which international law recognizes as foundational.[102] The International Covenant on Civil and Political Rights (ICCPR) Article 17 and the Universal Declaration of

---

[100] Michelle Bachelet, *Human rights in the digital age*, keynote speech (Oct. 17 2019), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E.

[101] UN General Assembly, Human Rights Council, *Report of the Office of the United Nations High Commissioner for Human Rights*, ¶ 14 (June 30, 2014), https://undocs.org/A/HRC/27/37.

[102] *International Principles of the Application of Human Rights to Communications Surveillance*, Electronic Frontier Foundation (May 2014), https://www.eff.org/files/necessaryandproportionatefinal.pdf.

Human Rights (UDHR) Article 12 both forbid the "arbitrary or unlawful interference with [] privacy, family, home, or correspondence."[103] Article 19 of both the ICCPR and UDHR also guarantee the right to opinion and expression, providing "freedom to seek, receive and impart information and ideas of all kinds . . . without interference." According to the UN Human Rights Committee General Comment 34 and UN Human Rights Council Resolutions,[104] restrictions on the rights to both freedom of expression and privacy must meet strict requirements of legality, necessity, and proportionality. Thus, such restrictions must be provided for by law, necessary for achieving a legitimate aim, and be in proportion to that aim. The restrictions "may never be invoked as a justification for the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights."[105] While states commonly claim national security to justify restrictions, the UN Special Rapporteur on the right to freedom of opinion and expression has found that such justifications should be limited to situations in which the interest of the

---

[103] The UN General Assembly adopted the UDHR in 1948 and it is customary international law. The United States ratified the ICCPR in 1992. *See* Jimmy Carter, *U.S. Finally Ratifies Human Rights Covenant*, The Carter Center (June 28, 1992), https://www.cartercenter.org/news/documents/doc1369.html. ICCPR available here: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. UDHR available here: https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf.

[104] UN General Assembly, Human Rights Committee, *General Comment No. 34*, ¶ 22 (Sept. 12, 2011), https://undocs.org/CCPR/C/GC/34; *see also, e.g.*, UN General Assembly, Human Rights Council, *The right to privacy in the digital age*, ¶ 2 (April 7, 2017), https://undocs.org/A/RES/34/7.

[105] General Comment 34 ¶ 23, *supra* note 104.

whole nation is at stake, rather than the interests of the government, a regime, or a power group alone.[106]

The UN Human Rights Committee and the UN General Assembly further clarified the application of these principles, determining that state surveillance requires robust and independent judicial oversight, must be carried out under a legal framework, and must remain consistent with international human rights obligations.[107] The Committee also underscored the importance of these principles when surveillance targets civil society by creating "incentives for self-censorship" and undermining "the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information."[108]

NSO's government clients violate these international laws when they deploy Pegasus to target individuals simply for exercising their internationally-recognized human rights. Frequently, oppressive laws purporting to authorize such surveillance are vague, grant far too much discretion to the officials who conduct

---

[106] Report, *supra* note 104, ¶ 25.
[107] UN General Assembly, Human Rights Committee, *Concluding observations on the fourth periodic report of the United States of America*, ¶ 22 (Apr. 23, 2014), https://undocs.org/CCPR/C/USA/CO/4; UN General Assembly, *Resolution 73/179, "The right to privacy in the digital age,"* (Jan. 21, 2019), https://undocs.org/en/A/RES/73/179.
[108] *Id*.

it, and lack independent judicial oversight.[109] And the intrusions on privacy and expression are neither necessary nor proportionate, because, *inter alia*, the alleged threats posed by those surveilled are generally fabricated and the surveillance itself is highly intrusive.[110]

B. NSO continues to supply surveillance technology to its clients while knowing they use it to violate international law, failing to fulfill its responsibility to respect human rights.

The United Nations Guiding Principles on Business and Human Rights (UNGPs)[111] also recognize that businesses like NSO bear responsibility for preventing human rights abuses. Section II of the UNGPs requires that all businesses respect human rights, avoid infringing on those rights, and address any adverse impacts that they cause or contribute to, independent of any state's

---

[109] *See, e.g.* Freedom House, *supra* notes 10, 27, 47.

[110] The threat is so great that the Special Rapporteurs on the right to freedom of expression and on racism and discrimination called for an immediate moratorium on the sale, transfer, and use of surveillance tools like Pegasus worldwide. *See* David Kaye, *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools*, OHCHR (June 25, 2019), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736; E. Tendayi Achiume, *UN expert joins call for immediate moratorium on sale, transfer and use of surveillance tech*, OHCHR (July 15, 2020), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26098&LangID=E.

[111] *Guiding Principles on Business and Human Rights*, UN Human Rights OHCHR (2011), https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

willingness to fulfill its own obligations.[112] It also requires businesses to prevent or mitigate any adverse human rights impacts directly linked to their operations.[113]

In addition, the UNGPs require that businesses have policies and processes in place to establish human rights policy commitments, engage in human rights due diligence, and implement remediation processes when they cause or contribute to adverse impacts.[114] If a violation occurs, companies must act to prevent or stop adverse impacts on human rights, including ending a business relationship entirely if necessary.[115] And they must engage in remediation through legitimate processes, including cooperation with other actors and judicial mechanisms.[116]

NSO's policy commitment pays lip service to these principles.[117] Yet, while NSO is well aware that many of its clients use Pegasus to violate human rights,[118] it ignores those violations in favor of the sale.[119] This cost-benefit analysis prioritizes profit to the detriment of human rights. And despite contributing to

---

[112] *Id*. at II.A.11, Comment; 13(a).
[113] *Id*. at II.A.13(b).
[114] *Id*. at II.A.15.
[115] *Id*. at II.B.19 Comment.
[116] *Id*. at II.B.22 Comment.
[117] *NSO Group spyware used against Moroccan journalist days after company pledged to respect human rights*, Amnesty International (June 22, 2020), https://www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist/.
[118] *NSO Group responds to human rights violations, but comes up short*, Access Now (Aug. 11, 2017), https://www.accessnow.org/nso-group-responds-human-rights-violations-comes-short/.
[119] O'Neill, *supra* note 56.

international law violations, NSO has done nothing to remediate adverse human rights impacts or prevent them from happening in the future, as the UNGPs require.[120]

The UNGPs clearly contemplate that private businesses like NSO can be held liable for their contribution to governmental violations. They state that due diligence alone "will [not] automatically and fully absolve them from liability for causing or contributing to human rights abuses."[121] Further, the Principles explicitly apply to business activity in conflict zones[122], as well as to entities under direct state ownership or control.[123]

This highlights the absurdity of NSO's immunity claim. Corporate responsibility is meaningless without a means to hold a corporation responsible. Immunity would place the surveillance industry wholly outside the framework of the UNGPs, which the international community spent years developing and the U.S. State Department continues to support.[124] The UNGPs build on and

---

[120] NSO continues to supply its technology to Morocco, despite documented instances of abuse. *See* Amnesty, *supra* note 74; *Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools*, Amnesty International (June 22, 2020), https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/.
[121] UNGPs, II.B.18 Comment, *supra* note 114.
[122] *Id*. at I.B.7.
[123] *Id*. at I.B.4-6.
[124] *See* Morgan Ortagus, Department Spokesperson, *Release of U.S. Department of State Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with*

complement the OECD Guidelines for Multinational Enterprises,[125] with full understanding that private companies often do business with foreign governments and should not be immune simply because they do so. NSO's theory is not only unrecognized under American law—it also undercuts the international principles developed specifically to address such business relationships.

C. Without hope for accountability in their countries, this suit provides many of NSO's victims their only avenue for justice.

The individual victims of NSO's spyware are unlikely to ever obtain redress in American courts. But neither will they find it in their own countries—the very countries that used NSO technology to surveil and harass them. In Togo, effective and efficient recourse for human rights violations is not guaranteed, given the failures of Togolese justice regarding recognized international principles in the past.[126] Rwandan judges are appointed by the president, confirmed by the RPF-dominated senate, and typically side with the government.[127] In Morocco, Mohammed VI chairs the Supreme Council of the Judiciary and regularly uses the courts as a tool to punish perceived opponents of the government, including human

---

Surveillance Capabilities, U.S. Department of State (Sept. 30, 2020), https://www.state.gov/release-of-u-s-department-of-state-guidance-on-implementing-the-un-guiding-principles-for-transactions-linked-to-foreign-government-end-users-for-products-or-services-with-surveillance-capabilities/.

[125] *OECD Guidelines for Multinational Enterprises*, OECD (2011), http://dx.doi.org/10.1787/9789264115415-en.

[126] *See* Freedom House, *supra* note 27.

[127] *See* Freedom House, *supra* note 10.

rights activists.[128] In India, a Public Interest Litigation filed for investigation before the country's Supreme Court was withdrawn in December 2019, and there are currently no pending cases on the NSO matter before any Indian courts.[129]

Indeed, the path to justice for abusive surveillance is fraught with obstacles. "[T]he barriers to successful litigation and formal complaints are significant, including the lack of judicial oversight, remedies, causes of action, enforcement and data preservation."[130] "Alternatives to litigation, providing for remedies consistent with international human rights law, appear unavailable."[131] And even when governments do take up requests from civil society organizations to investigate unlawful surveillance, those investigations "can be arbitrary or disorganized."[132]

WhatsApp has colorable claims for relief against NSO on its own. But for many victims of NSO's spyware, this action represents the only avenue for justice they will ever see. And though it may not directly compensate them for their suffering and quantifiable economic damages, it is no less remedial. Requiring that

---

[128] *See* Freedom House, *supra* note 47.
[129] *See* Sushovan Sircar, *Pegasus Spying Row: Ex-RSS Leader Withdraws Petition Seeking Probe*, The Quint (Dec. 2, 2019), https://www.thequint.com/news/india/govindacharya-withdraws-pil-supreme-court-whatsapp-pegasus-spyware-bobde.
[130] Report, *supra* note 104.
[131] *Id*.
[132] *Id*.

NSO stand accountable in an American court for its violation of American law significantly deters future surveillance abuses, especially given that many mobile technology companies call the United States home. It vindicates the tenets of international law set forth to protect the fundamental rights to privacy, association, peaceful assembly, and free expression that the broader global population enjoys. And it preserves the ability of civil society organizations and activists to communicate and work by securing the platforms that they rely on to do so.

Allowing the district court to exercise jurisdiction over NSO not only protects an American technology company that doubtless enjoys the protections of American laws; it also protects these brave civil society pioneers, and ensures that their work can continue unfettered by malicious intrusion on their fundamental human rights.

IV. CONCLUSION

For the foregoing reasons, Amici respectfully request that the District Court's decision be affirmed.

Dated: December 23, 2020

Respectfully submitted,

FARELLA BRAUN + MARTEL LLP

By: */s/ Kyle A. McLorg*
Kyle A. McLorg

Attorneys for Amici Curiae Access Now, Amnesty International, Committee to Protect Journalists, Internet Freedom Foundation, Paradigm Initiative, Privacy International, Red en Defensa de los Derechos Digitales, and Reporters Without Borders

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) 20-16408

I am the attorney or self-represented party.

This brief contains 6,950 **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.
- ◉ 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/ Kyle A. McLorg **Date** Dec 23, 2020

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

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

CERTIFICATE OF SERVICE

I hereby certify that 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 on December 23, 2020.

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.

/s/ Kyle A. McLorg
Kyle A. McLorg