Nos. 24-2179 (lead) and 24-3463

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CARLOS DADA, ET AL.,

PLAINTIFFS-APPELLANTS,

v.

NSO GROUP TECHNOLOGIES LIMITED, ET AL.,

DEFENDANTS-APPELLEES.

On Appeal from the United States District Court
for Northern District of California
Case No. 3:22-CV-07513-JD
The Honorable James Donato, District Court Judge

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLANTS AND REVERSAL

Sophia Cope
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
sophia@eff.org
andrew@eff.org
(415) 436-9333

Counsel for Amicus Curiae
Electronic Frontier Foundation

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus curiae* Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

/s/ Sophia Cope
Sophia Cope

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Rules

STATEMENT OF INTEREST OF *AMICUS CURIAE*[1]

Amicus curiae Electronic Frontier Foundation (EFF) has a strong interest in ensuring that the law provides accountability for corporations that assist governments in violating human rights. EFF is a San Francisco-based, member-supported, nonprofit civil liberties organization that has worked for over 30 years to protect free speech, privacy, security, and innovation in the digital world. With over 30,000 members, and harnessing the talents of lawyers, activists, and technologists, EFF represents the interests of technology users in court cases and broader policy debates regarding the application of law to the internet and other technologies.

EFF has led investigations into misuse of surveillance technologies by governments to target citizens for human rights abuses.[2] EFF published a report that uncovered evidence that the Lebanese government had been engaging in a massive global cyber-espionage campaign against activists, journalists, lawyers, and educational institutions, among others, using technology developed by the

[1] No counsel for a party authored this brief in whole or in part, and no such counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amicus curiae*, or its counsel, made a monetary contribution intended to fund its preparation or submission. All parties have consented to the filing of this brief.

[2] EFF, *Surveillance Technologies*, https://www.eff.org/issues/mass-surveillance-technologies.

German company FinFisher and likely other private entities.[3] The report also revealed that the government of Kazakhstan[4] used the same infrastructure to target journalists, lawyers, and dissidents.[5]

EFF has also participated as *amicus curiae* in cases focusing on the complicity of American companies, especially technology companies, in human rights abuses. EFF filed an *amicus* brief in an Alien Tort Statute (ATS) case before the U.S. Supreme Court. *Nestlé USA, Inc. v. Doe I*, 593 U.S. 628 (2021).[6] EFF filed *amicus* briefs in an ATS case recently before this Court where plaintiffs allege that Cisco Systems specially built internet surveillance and censorship products for the Chinese government that targeted the Falun Gong religious minority, who were then subjected to torture and other human rights

[3] Lookout & EFF, *Dark Caracal: Cyber-Espionage at a Global Scale* (2018) at 3-4 , https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf.

[4] *Id.* at 1, 2, 4.

[5] *See also* Cooper Quintin & Eva Galperin, *Dark Caracal: You Missed a Spot*, EFF Deeplinks (Dec. 10, 2020), https://www.eff.org/deeplinks/2020/12/dark-caracal-you-missed-spot.

[6] *See* Sophia Cope & Cindy Cohn, *Supreme Court Narrows Ability to Hold U.S. Corporations Accountable for Facilitating Human Rights Abuses Abroad*, EFF Deeplinks (July 21, 2021), https://www.eff.org/deeplinks/2021/07/supreme-court-narrows-ability-hold-us-corporations-accountable-facilitating-human.

abuses. *Doe I v. Cisco Systems, Inc.*, 73 F.4th 700, 707 (9th Cir. 2023).[7] EFF filed an *amicus* brief in the Second Circuit in an ATS case where plaintiffs alleged that IBM built a national identification system for the South African government that assisted the apartheid regime's human rights violations against the country's Black population. *Balintulo v. Ford Motor Co.*, 796 F.3d 160 (2d Cir. 2015).[8]

More recently, EFF filed an *amicus* brief in this Court in WhatsApp's lawsuit against NSO Group, the Defendants-Appellees here. *WhatsApp Inc. v. NSO Group Technologies Ltd.*, 17 F.4th 930, 932 (9th Cir. 2021).[9] EFF is also representing a Saudi women's rights activist whose iPhone was hacked by spyware company DarkMatter, which led to her arrest and torture. *Alhathloul v.*

[7] *See* Sophia Cope & Cindy Cohn, *Victory! Ninth Circuit Allows Human Rights Case to Move Forward Against Cisco Systems*, EFF Deeplinks (July 12, 2023), https://www.eff.org/deeplinks/2023/07/victory-ninth-circuit-allows-human-rights-case-move-forward-against-cisco-systems.

[8] *See* Sophia Cope, *Unrealistic Pleading Standards: Another Injustice for Human Rights Victims*, EFF Deeplinks (July 30, 2015), https://www.eff.org/deeplinks/2015/07/unrealistic-pleading-standards-another-injustice-human-rights-victims.

[9] *See* Sophia Cope & Matthew Guariglia, *Ninth Circuit: Surveillance Company Not Immune from International Lawsuit*, EFF Deeplinks (Nov. 10, 2021), https://www.eff.org/deeplinks/2021/11/ninth-circuit-surveillance-company-not-immune-international-lawsuit.

DarkMatter Group, 3:21-cv-01787-IM (D. Or.).[10]

INTRODUCTION AND SUMMARY OF ARGUMENT

The outcome of this case will have profound implications for millions of internet users and other citizens of countries around the world. While many technologies developed, licensed, and sold by both foreign and domestic corporations are tremendously useful to law-abiding customers, other technologies—or sometimes even the same technologies when deployed by repressive regimes—can facilitate human rights abuses.

With its focus on the intersection of civil liberties, human rights, and technology, *amicus* supports innovation while also calling for the responsible deployment of technology. We applaud the role that private companies have played in spreading the benefits of the internet and other technologies around the world. We believe that technology can be and has often been a force for good. However, when technology companies put profit over basic human well-being, and facilitate the violation of the human rights of people across the globe—where they are spied upon, and their privacy and freedom of speech and association are undermined, which often leads to them being physically harmed or even killed as a result—legal accountability is necessary.

[10] Case page *available at*: https://www.eff.org/cases/alhathloul-v-darkmatter-group.

Accordingly, *amicus* urges this Court to reverse the district court's dismissal of the complaint under *forum non conveniens* for Defendants-Appellees (collectively, "NSO Group"), who are sophisticated international actors already defending two other lawsuits related to their spyware within this jurisdiction.[11] Additionally, the Supreme Court has said that "if the remedy provided by the alternative forum is so clearly inadequate or unsatisfactory that it is no remedy at all," dismissal pursuant to *forum non conveniens* "would not be in the interests of justice." *Piper Aircraft Co. v. Reyno*, 454 U.S. 235, 254 (1981). *Accord Ceramic Corp. of America v. Inka Maritime Corp. Inc.*, 1 F.3d 947, 949 (9th Cir. 1993) ("the alternative forum must provide some potential avenue for redress"). It is dubious how receptive Israeli courts would be to a lawsuit by foreign plaintiffs against their own corporate citizen, as NSO Group is based in Israel. As a representative of Amnesty International Israel said, "It's been a longstanding tradition for the Israeli courts to be a rubber stamp for the Israeli Ministry of Defense," which provides an export license to NSO Group.[12]

---

[11] *See WhatsApp, Inc. v. NSO Group Technologies Ltd.*, No. 4:19-cv-07123-PJH (N.D. Cal.); *Apple, Inc. v. NSO Group Technologies Ltd.*, No. 3:21-cv-09078-JD (N.D. Cal.).

[12] *See, e.g.*, Ilan Ben Zion, *Israeli Court Rejects Petition to Curb Spyware Company*, Associated Press (July 13, 2020), https://www.courthousenews.com/israeli-court-rejects-petition-to-curb-spyware-company/.

Moreover, reports that the company's spyware had been deployed *within Israel* by the Israeli National Police against Israeli citizens—"political activists, mayors, heads of local authorities, officials in government ministries, and journalists"—demonstrated that local courts have been very accommodating to NSO Group in particular.[13]

As such, U.S. courts must remain a viable forum for victims of unjustified digital surveillance to vindicate their human rights.[14] It is critical to hold all technology companies accountable when they provide their products and services to governments around the world that use them to commit human rights abuses. Unlawful digital surveillance invades victims' privacy and chills their freedom of speech and association, and often leads to unlawful arrest and

---

[13] *See* Tal Mimran & Lior Weinstein, *A Path Forward for Israel Following the NSO Scandal*, Lawfare (June 12, 2023) ("One would assume that the courts in Israel, entrusted with authorizing the deployment of spyware, would be cautious in authorizing its use. Another important discovery, however, was that out of those 1,000 uses of the spyware by the police, only six requests were denied by the courts. This is an alarming number, demonstrating that the courts seem to favor the needs of the police and raising concerns in terms of safeguarding the possible infringement of core human rights—such as the right to privacy and the right to due process."), https://www.lawfaremedia.org/article/a-path-forward-for-israel-following-the-nso-scandal.

[14] *See also* Emma Pinedo, *Spain's High Court Shelves Israeli Spyware Probe on Lack of Cooperation*, Reuters (July 10, 2023), https://www.reuters.com/world/europe/spains-high-court-shelves-israeli-spyware-probe-lack-cooperation-2023-07-10/.

detention, torture, disappearances, and summary execution. Victims of human rights abuses enabled by powerful technologies must have the ability to seek redress through civil suits in U.S. courts against both foreign and domestic corporations.

Amicus supports the arguments of the Plaintiffs-Appellants, but also writes to emphasize that reversing the district court's *forum non conveniens* ruling is appropriate given the broader context—that corporate complicity in human rights violations is a widespread and ongoing problem, that NSO Group in particular has a long history of assisting governments in targeting civil society and violating the rights of their citizens, and that the company's internal human rights accountability mechanisms have failed (Part I). This conclusion is also supported by United Nations and United States policy on business and human rights (Part II), and by the fact that the technology industry's voluntary accountability mechanisms have been largely ineffective (Part III). In short, this Court should not expand the ability of technology companies like NSO Group to avoid accountability for facilitating human rights abuses by governments around the world, especially authoritarian ones.

ARGUMENT

I. The Technology Industry Plays a Major Role in Human Rights Abuses Worldwide

This Court should reverse the district court's dismissal on *forum non conveniens* so that Plaintiffs-Appellants here, seeking to vindicate their rights and representing the interests of human rights victims broadly, have an opportunity to hold one of the most notorious technology companies accountable for its complicity in the human rights abuses perpetrated by governments around the world. As the Supreme Court has recognized, corporations can be just as culpable as the individuals who comprise them:

> [N]atural persons can and do use corporations for sinister purposes, including conduct that violates international law … [T]he corporate form can be an instrument for inflicting grave harm and suffering … So there are strong arguments for permitting the victims to seek relief from corporations themselves.

Jesner v. Arab Bank, PLC, 584 U.S. 241, 270 (2018). This concern is particularly acute for modern technology companies that provide sophisticated surveillance and censorship products and services to governments, enabling those governments to engage in repression on a massive scale. As numerous cases demonstrate, NSO Group's "Pegasus" spyware and other powerful digital surveillance tools are used to identify and track journalists, democracy and human rights activists, and religious minorities, among others. These tools not

only invade digital privacy and compromise freedom of speech and association, they can also facilitate physical apprehension, unlawful detention, torture, disappearances, and even summary execution.

A. Surveillance Companies Facilitate Human Rights Abuses by Governments

The private spyware industry was estimated to be worth $12 billion as of 2022.[15] There are at least 500 private companies that have provided surveillance technologies to governments around the globe,[16] according to Privacy International. When the UK-based nonprofit began its research in 2013, it wrote, "In repressive regimes, these technologies enable spying that stifles dissent, has chilling effects across society, and in many cases allows governments to hunt down those it wishes to silence."[17] It further lamented the fact that "members of the private surveillance industry have gained a sense of impunity."[18]

Similarly, in a scathing 2019 report on the surveillance industry's

---

[15] Ronan Farrow, *How Democracies Spy on Their Citizens*, The New Yorker (April 18, 2022), https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.

[16] Privacy International, *The Global Surveillance Industry* (Feb. 16, 2018), https://privacyinternational.org/explainer/1632/global-surveillance-industry.

[17] Privacy International, *The Surveillance Industry Index: An Introduction* (Nov. 18, 2013), https://privacyinternational.org/blog/1214/surveillance-industry-index-introduction.

[18] *Id.*

complicity in human rights abuses by repressive regimes, the United Nations Special Rapporteur on Freedom of Opinion and Expression explained that "[d]igital surveillance is no longer the preserve of countries that enjoy the resources to conduct mass and targeted surveillance based on in-house tools. Private industry has stepped in, unsupervised and with something close to impunity."[19]

The Special Rapporteur's research revealed that digital surveillance can have real-world human rights consequences: "Surveillance of specific individuals—often journalists, activists, opposition figures, critics and others exercising their right to freedom of expression—has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings."[20] He rightly asserted: "The lack of causes of action and remedies raises serious concerns about the likelihood of holding companies accountable for human rights violations."[21]

The Special Rapporteur was so alarmed by what he found through his

---

[19] David Kaye, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, United Nations Human Rights Council (May 28, 2019) at 4, https://www.ohchr.org/en/calls-for-input/report-adverse-effect-surveillance-industry-freedom-expression.

[20] *Id.* at 3.

[21] *Id.* at 12.

research that he called for "an *immediate moratorium* on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways."[22] In an op-ed, he rejected the notion that it is "complicated" to protect privacy and human rights: "All I can say is, give me a break."[23]

B. NSO Group is Notorious for Facilitating Human Rights Abuses by Governments and Fails to Regulate Itself

NSO Group facilitates the surreptitious surveillance of journalists, political dissidents, lawyers, and other members of civil society. NSO Group admits that its customers are "exclusively" governments.[24] Thus, any harm to citizens that flows from the use of NSO Group's surveillance technology is because the company provides its "Pegasus" spyware directly to government officials—and oftentimes to those in authoritarian regimes.

Over the past several years, a massive amount of information has come to

---

[22] *Id.* at 3 (emphasis added).

[23] David Kaye, *The Surveillance Industry is Assisting State Suppression. It Must be Stopped*, The Guardian (Nov. 26, 2019), https://www.theguardian.com/commentisfree/2019/nov/26/surveillance-industry-suppression-spyware.

[24] *See* NSO Group, *About Us* ("NSO products are used exclusively by government intelligence and law enforcement agencies to fight crime and terror."), https://www.nsogroup.com/about-us/.

light about how extensive the use of NSO Group's spyware has been by governments around the globe for purposes that implicate human rights.[25]

As Plaintiffs-Appellants explain, the present case arose from the research of Citizen Lab[26] and the nonprofits Access Now and Amnesty International. ER-024 (Amd. Compl. [ECF 31] ¶ 41). The researchers published a report in 2022 that found that at least 35 people in El Salvador had their iPhones hacked with NSO Group's spyware between July 2020 and November 2021.[27] Targets included the *El Faro* Plaintiffs in this case, as well as other journalists and activists.[28] The perpetrator appears to have been the government of El Salvador, given that NSO Group only sells to governments and that the attacks of the *El Faro* journalists coincided with their investigative reporting into President

---

[25] *See, e.g.*, Omar Benjakob, *The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware*, Haaretz (April 5, 2022), https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000.

[26] Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy at the University of Toronto. Citizen Lab, *About the Citizen Lab*, https://citizenlab.ca/about/.

[27] John Scott-Railton et al., *Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador With Pegasus Spyware*, Citizen Lab (Jan. 12, 2022), https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

[28] Mary Beth Sheridan & Craig Timberg, *Report: 22 Journalists at Salvadoran News Site Hit With Pegasus Hack*, Washington Post (Jan. 12, 2022), https://www.washingtonpost.com/world/2022/01/12/salvador-pegasus-faro-nso/.

Nayib Bukele's administration.[29]

In 2021, a consortium of journalists called Forbidden Stories along with Amnesty International's Security Lab launched the Pegasus Project.[30] ER-026 (Amd. Compl. [ECF 31] ¶ 47). The consortium was comprised of more than 80 reporters from 17 media outlets in 10 countries.[31] The Pegasus Project team had access to a leak of more than 50,000 phone numbers selected for surveillance by the customers of NSO Group across 50 countries since 2016.[32] Among the listed phone numbers, 180 of them belonged to journalists,[33] while others were associated with "human rights defenders, academics, businesspeople, lawyers, doctors, diplomats, union leaders, politicians and several heads of states."[34] The team was further able to technically confirm that some of the numbers listed were associated with phones that indeed had a spyware infection or attempted

---

[29] *Id.*

[30] Forbidden Stories, *About the Pegasus Project* (July 18, 2021), https://forbiddenstories.org/about-the-pegasus-project/.

[31] *Id.*

[32] *Id.*

[33] Phineas Rueckert, *Pegasus: The New Global Weapon for Silencing Journalists*, Forbidden Stories, (July 18, 2021), https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

[34] *About the Pegasus Project*, *supra* note 30.

infection.[35]

Citizen Lab research in 2019 helped the smartphone messaging application WhatsApp discover that NSO Group's spyware breached its systems in April and May 2019 and targeted approximately 1,400 users.[36] Citizen Lab found that the WhatsApp hack resulted in more than "100 cases of abusive targeting of human rights defenders and journalists in at least 20 countries across the globe."[37] Victims of the WhatsApp hack included Rwandan political dissidents living in exile, who feared that access to their private communications helped the Rwandan government carry out numerous assassinations.[38]

Notorious other cases of NSO Group facilitating the targeting of members of civil society by governments around the world abound.

Saudi Arabia has used NSO Group's spyware to target critics of the

---

[35] *Takeaways from the Pegasus Project*, Washington Post (Aug. 2, 2021), https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.

[36] Nicole Perlroth, *WhatsApp Says Israeli Firm Used Its App in Spy Program*, New York Times (Oct. 29, 2019), https://www.nytimes.com/2019/10/29/technology/whatsapp-nso-lawsuit.html.

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

[38] 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.

kingdom, including Omar Abdulaziz, a Saudi Arabian dissident living in Canada and confidant to fellow kingdom critic and *Washington Post* columnist Jamal Khashoggi.[39] The day after Citizen Lab published its report on the targeting of Mr. Abdulaziz, who regularly exchanged messages with Mr. Khashoggi, Mr. Khashoggi was murdered[40] by order of the Saudi government in the kingdom's embassy in Turkey.[41] Chillingly, Saudi officials tried to lure Mr. Abdulaziz to the kingdom's embassy in Canada.[42] His own family and friends have disappeared in Saudi Arabia.[43] The Pegasus Project later revealed that the

---

[39] Nina dos Santos & Michael Kaplan, *Jamal Khashoggi's Private WhatsApp Messages May Offer New Clues to Killing*, CNN (Dec. 4, 2018), https://www.cnn.com/2018/12/02/middleeast/jamal-khashoggi-whatsapp-messages-intl/index.html.

[40] Bill Marczak, et al., *Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator*, Citizen Lab (Jan. 28, 2020), https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/.

[41] *Jamal Khashoggi: All You Need to Know About Saudi Journalist's Death*, BBC News (Feb. 24, 2021), https://www.bbc.com/news/world-europe-45812399.

[42] Dos Santos, *supra* note 39.

[43] Bill Marczak, et al., *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*, Citizen Lab (Oct. 1, 2018), https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

women in Mr. Khashoggi's life were also targeted with NSO Group's spyware.[44] Additionally, the Saudi government targeted *New York Times* journalist Ben Hubbard, who covered the kingdom, for digital surveillance using NSO Group's technology.[45]

The Mexican government has aggressively used NSO Group's spyware to target journalists investigating drug cartels,[46] the wife of a murdered journalist,[47] and lawyers representing the families of a murdered women's rights activist and other victims.[48] The lawyers often criticized the government's handling of high-

---

[44] Dana Priest *et al.*, *Jamal Khashoggi's Wife Targeted With Spyware Before His Death*, Washington Post (July 18, 2021), https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/.

[45] Marczak, *supra* note 40.

[46] John Scott-Railton, et al., *Reckless VI: Mexican Journalists Investigating Cartels Targeted With NSO Spyware Following Assassination of Colleague*, Citizen Lab (Nov. 27, 2018), https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/. *See also* Katitza Rodriguez, *Where Governments Hack Their Own People and People Fight Back: 2018 in Review*, EFF Deeplinks (Dec. 30, 2018), https://www.eff.org/deeplinks/2018/12/where-government-hack-their-own-people-and-people-fight-back-latin-american.

[47] John Scott-Railton, et al., *Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted With NSO Group's Spyware*, Citizen Lab (March 20, 2019), https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/.

[48] John Scott-Railton, et al., *Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted With NSO Spyware*, Citizen Lab (Aug. 2, 2017), https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/.

profile crimes.[49] The Mexican government also targeted its own scientists who supported a soda tax[50] and opposition-party politicians.[51]

As previously mentioned, NSO Group's spyware has even been used against Israeli citizens. An investigation and report ordered by Israel's attorney general found that the Israeli National Police "had knowingly infringed on the law by using wider taps than permissible" and "also confirmed that private data was saved on NSO servers, alongside those of the police, which raises serious concerns regarding data protection and privacy rights."[52]

Thus, NSO Group's suggestion that its technology is only used to track terrorists and other criminals is manifestly wrong.[53]

The company's self-regulation has also fallen gravely short. The April to

---

[49] Associated Press, *Mexico Spying Scandal: Human Rights Lawyers Investigating Murders Targeted*, The Guardian (Aug. 3, 2017), https://www.theguardian.com/world/2017/aug/03/mexico-spying-scandal-human-rights-lawyers-investigating-murders-targeted.

[50] John Scott-Railton, et al., *Bitter Sweet Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*, Citizen Lab (Feb. 11, 2017), https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

[51] John Scott-Railton, et al., *Reckless Redux: Senior Mexican Legislators and Politicians Targeted With NSO Spyware*, Citizen Lab (June 29, 2017), https://citizenlab.ca/2017/06/more-mexican-nso-targets/.

[52] Mimran, *supra* note 13.

[53] *See About Us*, *supra* note 24 (NSO Group helps "government agencies detect and prevent terrorism and crime.").

May 2019 WhatsApp hack happened just weeks *after* NSO Group's then-new owners had asserted that the company "already operates under an ethical governance framework that is significantly more robust than any of its peers."[54] The company later adopted a human rights policy in September 2019[55] and a human rights due diligence procedure in April 2020.[56] These moves were ineffective, as the hacks of Plaintiffs-Appellees here occurred from July 2020 to November 2021 *after* the policies were adopted.[57] More recently, NSO Group claims to have terminated a mere six customer accounts after a human rights review.[58]

---

[54] Stephen Peel, *Response to Open Letter to Novalpina Capital on 18 February 2019*, Novalpina (March 1, 2019), https://web.archive.org/web/20200805082629/https://www.novalpina.pe/response-to-open-letter-1/.

[55] NSO Group, *Human Rights Policy* (Sept. 2019) [report], https://www.nsogroup.com/wp-content/uploads/2019/09/NSO-Human-Rights-Policy_September19.pdf. *See also* NSO Group, *Human Rights Policy* [webpage], https://www.nsogroup.com/governance/human-rights-policy/.

[56] NSO Group, *Transparency and Responsibility Report* (2023) at 13, https://www.nsogroup.com/wp-content/uploads/2023/12/2023-Transparency-and-Responsibility-Report.pdf.

[57] *See also* Amnesty International, *NSO Group Spyware Used Against Moroccan Journalist Days After Company Pledged to Respect Human Rights* (June 22, 2020), https://www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist/.

[58] Vas Panagiotopoulos, *Notorious Spyware Maker NSO Group is Quietly Plotting a Comeback*, WIRED (Jan. 24, 2024), https://www.wired.com/story/nso-group-lobbying-israel-hamas-war/.

No amount of multimillion dollar lobbying[59] can change the fact that NSO Group facilitates violations of human rights.

II. United Nations and United States Policy on Business and Human Rights Supports Allowing This Case to Move Forward

Allowing cases like this one to move forward in U.S. courts is consistent with settled United Nations policy on business and human rights. The concept of "business and human rights," as a subset of corporate social responsibility, is over 30 years old.[60] It took a powerful step forward with the 2008 report written by the United Nations Special Representative on Business and Human Rights, John Ruggie, known as the Ruggie Report.[61]

The Ruggie Report created an "authoritative focal point" for the issue of business and human rights through a framework consisting of three principles: "[1] the State duty to protect against human rights abuses by third parties, including business; [2] the corporate responsibility to respect human rights; and

---

[59] *Id.*

[60] The non-profit consulting firm Business for Social Responsibility (BSR), for example, founded in 1992, focuses on human rights, as well as myriad other issues. Business for Social Responsibility, *Our Story*, https://www.bsr.org/en/about/story; *Areas of Expertise*, https://www.bsr.org/en/expertise.

[61] John Ruggie, *Protect, Respect and Remedy: A Framework for Business and Human Rights*, United Nations Human Rights Council (April 7, 2008), https://media.business-humanrights.org/media/documents/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf.

[3] the need for more effective access to remedies."[62] The Ruggie Report emphasized that the governmental duty to protect and the corporate responsibility to respect human rights are distinct (albeit intertwined) obligations.[63]

The 2008 Ruggie Report led to the 2011 publication by the United Nations Human Rights Council of the *Guiding Principles on Business and Human Rights*, which adopted and sought to operationalize the Ruggie Report framework.[64] The *Guiding Principles*[65] provide that national governments should "take steps to prevent abuse abroad by business enterprises within their jurisdiction"[66] and "to ensure the effectiveness of domestic judicial mechanisms

---

[62] *Id.* at 4.

[63] *Id.* at 17.

[64] United Nations Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (June 16, 2011), https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[65] *See also* United Nations Human Rights Council, *Resolution on Human Rights and Transnational Corporations and Other Business Enterprise* [A/HRC/RES/17/4] (July 6, 2011), https://ap.ohchr.org/documents/dpage_e.aspx?si=A%2FHRC%2FRES%2F17%2F4; European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (June 28, 2013), https://op.europa.eu/en/publication-detail/-/publication/ab151420-d60a-40a7-b264-adce304e138b.

[66] *Guiding Principles*, *supra* note 64, at 4.

when addressing business-related human rights abuses."[67] They express concern about "legal barriers" to justice, including "[t]he way in which legal responsibility is attributed among members of a corporate group under domestic criminal and civil laws facilitates the avoidance of appropriate accountability."[68] They also caution against creating a situation where human rights victims "face a denial of justice in a host State and cannot access home State courts regardless of the merits of the claim."[69]

In 2020, the U.S. government endorsed the *Guiding Principles* as they specifically apply to U.S. companies that provide digital surveillance technologies to foreign governments.[70]

The U.S. government has also recognized the specific problem of private companies selling powerful spyware to governments around the world that do not respect human rights and has taken various steps to this address this problem.

---

[67] *Id.* at 28.

[68] *Id.* at 29.

[69] *Id.*

[70] U.S. State Dept., *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* (Sept. 30, 2020), https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/.

In 2021, the Biden Administration launched a multilateral effort called the Export Controls and Human Rights Initiative "to help stem the tide of authoritarian government misuse of technology and promote a positive vision for technologies anchored by democratic values."[71] As part of this initiative, the Commerce Department placed NSO Group (and another Israeli company) on the Entity List "based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers … Such practices threaten the rules-based international order."[72] ER-027 (Amd. Compl. [ECF 31] ¶ 50). The Entity List designation is a type of sanctions that "prohibits export from the United States to NSO of any type of hardware or software, severing the company from a vital source of technology."[73]

---

[71] White House, *Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy* (Dec. 10, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/.

[72] U.S. Commerce Dept., *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[73] Drew Harwell *et al.*, *Biden Administration Blacklists NSO Group Over Pegasus Spyware*, Washington Post (Nov. 3, 2021),

In 2022, the Biden Administration published a National Security Strategy that included the commitment to combat the "illegitimate use of technology, including commercial spyware and surveillance technology" and to "stand against digital authoritarianism."[74]

In 2023, as follow on work to the Export Controls and Human Rights Initiative, the group of participating governments created "a voluntary, nonbinding written code of conduct outlining political commitments by Subscribing States to apply export control tools to prevent the proliferation of goods, software, and technologies that enable serious human rights abuses."[75]

Thus, this Court should not facilitate "the avoidance of appropriate accountability."[76] Rather, ensuring that companies like NSO Group cannot avoid accountability is consistent with the United Nations' and United States' goals of stemming the tide of governmental abuses via spyware technologies and of

---

https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/.

[74] White House, *National Security Strategy October 2022* (Oct. 12, 2022) at 33, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[75] U.S. State Dept., *Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy* (March 30, 2023), https://www.state.gov/export-controls-and-human-rights-initiative-code-of-conduct-released-at-the-summit-for-democracy/.

[76] *Guiding Principles*, *supra* note 64, at 29.

establishing judicial avenues for human rights victims to seek justice against corporations that are complicit in abuses perpetrated by governments.

Using the doctrine of *forum non conveniens* exceedingly sparingly—particularly in cases like this one involving fundamental human rights—does not mean that U.S. courts would have unfettered authority over foreign corporations, or any corporation for that matter. The rules of personal jurisdiction continue to circumscribe the reach of U.S. courts. *See* Fed. R. Civ. P. 4(k), 12(b)(2); *International Shoe Co. v. Washington*, 326 U.S. 310 (1945); *AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201, 1207-09 (9th Cir. 2020). As do the required elements of any claim, from the Computer Fraud & Abuse Act (relevant here), with its requirement of "damage" or "loss," 18 U.S.C. § 1030(g); to the Alien Tort Statute, 28 U.S.C. §1350, which requires that any claim by a foreign plaintiff against an American corporation for aiding and abetting governmental human rights abuses "touch and concern" the United States per *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 124-25 (2013), and sufficiently meet the standard tort elements of *mens rea* and *actus reus*, among others. *See Doe I v. Cisco Systems, Inc.*, 73 F.4th 700, 724 (9th Cir. 2023).

III. Voluntary Mechanisms for Holding the Technology Industry Accountable for Human Rights Abuses are Inadequate

It is especially important that this Court give plaintiffs like the journalists

here a fighting chance in U.S. courts given that voluntary mechanisms for holding technology companies accountable for their roles in human rights abuses have proven inadequate. The Ruggie Report recognized that "companies can affect virtually all internationally recognized rights."[77] The report even used a technology example to illustrate the potential breadth of a company's impact on human rights: "violations of privacy rights by Internet service providers can endanger dispersed end-users."[78]

The Ruggie Report argued that companies, therefore, must practice "due diligence," which involves taking steps "to become aware of, prevent and address adverse human rights impacts."[79] Due diligence[80] includes the consideration of several factors, such as "whether [the company] might

---

[77] Ruggie, *supra* note 61, at 9.

[78] *Id.* at 20.

[79] *Id.* at 17.

[80] *Amicus* proposed a specific version of this due diligence framework called "Know Your Customer" for technology companies to follow before closing a deal with a foreign government or the U.S. government, where there is a possibility the technology could be used in human rights violations. *See* Cindy Cohn & Jillian C. York, *"Know Your Customer" Standards for Sales of Surveillance Equipment*, EFF Deeplinks (Oct. 24, 2011), https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment. *See also* Cindy Cohn, *Should Your Company Help ICE? "Know Your Customer" Standards for Evaluating Domestic Sales of Surveillance Equipment*, EFF Deeplinks (July 13, 2018), https://www.eff.org/deeplinks/2018/07/should-your-company-help-ice-know-your-customer-standards-evaluating-domestic.

contribute to abuse through the relationships connected to their activities, such as with business partners, suppliers, State agencies, and other non-State actors."[81] The UN's *Guiding Principles* similarly provide that companies should "avoid causing or contributing to adverse human rights impacts through their own activities," and should "prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships," whether those relationships are with governmental or non-governmental actors.[82]

However, the *Guiding Principles* expressly do not create any "new international law obligations."[83] Thus, the Ruggie Report's "due diligence" framework for companies is wholly voluntary. The report contemplated, however, that voluntary mechanisms would play a significant role in corporate accountability for human rights violations.[84] The Ruggie Report and the UN's *Guiding Principles* helped spur progress in defining the right courses of action on business and human rights.

Unfortunately, weakness of voluntary enforcement is evidenced by the

---

[81] Ruggie, *supra* note 61, at 17.

[82] *Guiding Principles*, *supra* note 64, at 14-15.

[83] *Id.* at 1.

[84] Ruggie, *supra* note 61, at 26. *See also Guiding Principles*, *supra* note 64, at 28, 31.

fact that NSO Group itself has a human rights policy and due diligence procedure yet governmental abuses continue.[85] *See supra* Part I.B. Enforcement generally of human rights standards through voluntary corporate accountability mechanisms has been weak at best.

A. Limits of Multi-Stakeholder Initiatives

A report by MSI Integrity[86] concluded that multi-stakeholder initiatives (as a subset of voluntary human rights corporate accountability mechanisms) "are not effective tools for holding corporations accountable for abuses, protecting rights holders against human rights violations, or providing survivors and victims with access to remedy."[87] This includes the leading technology-industry focused MSI, called the Global Network Initiative (GNI), discussed below. *See infra* Part III.C.[88]

---

[85] *Human Rights Policy*, *supra* note 55; *Transparency and Responsibility Report*, *supra* note 56.

[86] The Institute for Multi-Stakeholder Initiative Integrity (MSI Integrity) was originally incubated at the International Human Rights Clinic at Harvard Law School from 2010 to 2012. It is now an independent U.S.-based nonprofit organization. MSI Integrity, *History*, https://www.msi-integrity.org/test-home/history/.

[87] MSI Integrity, *Not Fit-for-Purpose: The Grand Experiment of Multi-Stakeholder Initiatives in Corporate Accountability, Human Rights and Global Governance* (July 2020) at 4, https://www.msi-integrity.org/wp-content/uploads/2020/07/MSI_Not_Fit_For_Purpose_FORWEBSITE.FINAL_.pdf.

[88] *Id.* at 24.

The report correctly recognized that MSIs can only achieve "positive outcomes where there is genuine commitment on the part of corporate members to change."[89] The report emphasized that "MSIs do not eliminate the need to protect rights holders from corporate abuses through effective regulation and enforcement."[90] While supporting companies that are committed to avoiding human rights abuses is a useful role, the difference between these initiatives and law is clear: law ensures accountability for companies that do not care about—or are actively opposed to—respecting human rights.

Denying companies like NSO Group an easy out to avoid the merits of human rights cases gives victims a chance to enforce—through a binding judicial process—human rights standards against corporations that are not willing to police themselves and that cause grave harm to individuals around the world.

B. OECD Guidelines for Multinational Enterprises

The Organization for Economic Cooperation & Development (OECD)[91] wrote the *Guidelines for Multinational Enterprises on Responsible Business*

---

[89] *Id.* at 5.

[90] *Id.* at 4.

[91] The OECD is an international organization funded by member countries. Organization for Economic Cooperation & Development, *Budget*, https://www.oecd.org/about/budget/.

Conduct "to shape government policies and help businesses [minimize] the adverse impacts of their operations and supply chains, while providing a venue for the resolution of alleged corporate, social, environmental, [labor] or human rights abuses.[92] The human rights chapter states that companies should conduct human rights due diligence, specifically citing the Ruggie Report and the UN's *Guiding Principles* as the bases for the OECD's human rights recommendations.[93]

The accountability mechanism for the *Guidelines* is the system of "National Contact Points" (NCPs), which are offices set up by participating countries to accept complaints—"Specific Instances"—that companies have violated the *Guidelines*.[94] Specific Instances can lead to mediation between the complainant and the company.[95] The National Contact Point for the United

---

[92] Organization for Economic Cooperation & Development, *Responsible Business Conduct: OECD Guidelines for Multinational Enterprises*, http://mneguidelines.oecd.org/.

[93] Organization for Economic Cooperation & Development, *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct* (June 8, 2023) at 25, https://www.oecd-ilibrary.org/finance-and-investment/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_81f92357-en.

[94] Organization for Economic Cooperation & Development, *Responsible Business Conduct: OECD Guidelines for Multinational Enterprises, National Contact Points*, http://mneguidelines.oecd.org/ncps/.

[95] Organization for Economic Cooperation & Development, *How Do NCPs Handle Cases?*, https://mneguidelines.oecd.org/ncps/how-do-ncps-handle-cases.htm.

States is housed at the State Department.[96] The key shortcomings of the NCP/Specific Instance system are two-fold.[97] First, the Specific Instance process in the U.S. has not been widely used. Between 2000 and 2016, only 45 cases were submitted to the State Department,[98] with only one relating to the telecommunications industry (involving T-Mobile and labor practices).[99] Second and more fundamentally, "the OECD Guidelines are non-binding on businesses and engagement in a Specific Instance process is voluntary."[100]

This latter shortcoming was on full display in the United Kingdom, providing a stark example for the technology industry.[101] Privacy International

---

[96] U.S. State Dept., *U.S. National Contact Point for the OECD Guidelines for Multinational Enterprises*, https://www.state.gov/u-s-national-contact-point-for-the-oecd-guidelines-for-multinational-enterprises/.

[97] *See, e.g.*, U.S. State Dept., *Specific Instance Process*, https://www.state.gov/u-s-national-contact-point-for-the-oecd-guidelines-for-multinational-enterprises/specific-instance-process/.

[98] U.S. State Dept., *Chart of U.S. NCP Specific Instance Cases Since 2000*, at 1, https://www.state.gov/wp-content/uploads/2019/04/U.S.-NCP-Specific-Instances-Chart-2000-2017.pdf.

[99] U.S. State Dept., *U.S. NCP Final Assessment: Communications Workers of America (AFL-CIO, CWA)/ver.di and Deutsche Telekom AG* (July 9, 2013), https://2009-2017.state.gov/e/eb/oecd/usncp/links/rls/211646.htm.

[100] U.S. State Dept., *Specific Instance Process, Frequently Asked Questions* (Archive 2009-2017), https://2009-2017.state.gov/e/eb/oecd/usncp/specificinstance/faq/index.htm.

[101] Similarly, the UK-based nonprofit Business & Human Rights Resource Centre collects human rights complaints against companies and solicits

filed a complaint with the UK's NCP alleging that Gamma International UK Ltd.:

> supplied to the Bahrain authorities "malware" products which allowed them to hear/see and record private conversations, correspondence and other records (e.g. address books) of individuals involved in pro-democracy activities in Bahrain … [O]n the basis of information obtained by this surveillance, these individuals, who had not committed any criminal offences under Bahrain law, were subsequently detained and in some cases tortured by the Bahrain security forces.[102]

After initially responding to Privacy International's complaint, Gamma went silent. The UK NCP concluded:

> [I]n the absence of an update from Gamma[,] the UK NCP can only conclude that Gamma International UK Limited has made no progress (or effort) towards meeting the recommendations made in the Final Statement.[103] The UK NCP therefore sees no reason to

---

company responses. Companies can choose to ignore the complaints, and even if they respond, there is no guarantee they will change their practices. *See* Business & Human Rights Resource Centre, *Company Response Mechanism* ("Our all time, global response rate for companies is 59%."), https://www.business-humanrights.org/en/from-us/company-response-mechanism/.

[102] UK National Contact Point, *Initial Assessment by the UK National Contact Point for the OECD Guidelines for Multinational Enterprises: Complaint from Privacy International and Others Against Gamma International UK Ltd.* (June 2013) at 2, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/847361/UK-NCP-initial-complaint-privacy-international-and-others-against-gamma-international-uk-ltd.pdf.

[103] *See generally* UK National Contact Point, *Privacy International Complaint to UK NCP About Gamma International UK Ltd.* (Feb. 26, 2016), https://www.gov.uk/government/publications/privacy-international-complaint-to-uk-ncp-about-gamma-international-uk-ltd.

> change the view reached in its Final Statement that Gamma's [behavior] is inconsistent with its obligations under the OECD Guidelines. The UK NCP regrets Gamma's failure to engage.[104]

C. Global Network Initiative

The Global Network Initiative (GNI) is a human rights corporate accountability program that focuses specifically on the information and communications technology (ICT) sector.[105] GNI was born out of the tragic case of Shi Tao, a pro-democracy journalist in China.[106] Yahoo! had shared information from his email account with the Chinese government, which led to his identification, arrest, and imprisonment for nearly a decade—all because he forwarded to foreign media an email about the Chinese government's plan to quell potential protests on the 15th anniversary of the Tiananmen Square massacre.[107]

---

[104] UK National Contact Point, *Follow Up Statement After Recommendations in Complaint From Privacy International Against Gamma International* (Feb. 2016) at 4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/847364/uk-ncp-follow-up-statement-privacy-international-gamma-international.pdf.

[105] GNI is a U.S.-based nonprofit organization. Global Network Initiative, *Financial Reports*, https://globalnetworkinitiative.org/about/financials/.

[106] *See* Pen America, *Shi Tao: China*, https://pen.org/advocacy-case/shi-tao/.

[107] *See* Associated Press, *Shi Tao: China Frees Journalist Jailed Over Yahoo Emails*, The Guardian (Sept. 8, 2013), https://www.theguardian.com/world/2013/sep/08/shi-tao-china-frees-yahoo.

GNI is a voluntary program that follows a multi-stakeholder model, where its members include American and foreign technology companies, as well as civil society groups, academics, and investment firms.[108] Over two years of painstaking effort went into creating GNI culminating in its launch in 2008.[109] The GNI accountability process is based upon the foundational *Global Principles on Freedom of Expression and Privacy*[110] and the related *Implementation Guidelines*, which require technology company members to submit to independent "assessments" of their implementation of the *Principles*.[111]

While GNI should be credited for recruiting major technology companies and operationalizing human rights accountability for the ICT sector, the program has two major shortcomings. First, not all technology companies are members—

[108] Global Network Initiative, *Members*, https://globalnetworkinitiative.org/who-we-are/members/.

[109] Global Network Initiative, *Inaugural Report 2010* (2010) at 2, https://globalnetworkinitiative.org/wp-content/uploads/2018/02/GNI_Annual_Report_2010.pdf.

[110] Global Network Initiative, *The GNI Principles*, https://globalnetworkinitiative.org/gni-principles/.

[111] Global Network Initiative, *Implementation Guidelines*, *Section 5: Governance, Accountability, and Transparency*, https://globalnetworkinitiative.org/implementation-guidelines/.

presently only 15 companies participate in GNI.[112] Second and more importantly, the program's success hinges on the candor and cooperation of the member companies, which has been lacking.

Amicus was once a civil society member of GNI, until it resigned in 2013 from the organization after GNI members were implicated in mass internet surveillance by the U.S. National Security Agency (NSA). GNI's corporate representatives were unable to accurately represent to civil society organizations and other GNI members the nature and extent of the illegal surveillance conducted within their systems by the U.S. government.[113]

Additionally, the NYU Stern Center for Business & Human Rights resigned from GNI in 2016 due, in part, to GNI's board having removed the term "compliance" from the *Principles* and *Implementation Guidelines*, and added language stating that GNI would instead assess whether a company was "committed" to the *Principles* and was acting in "good faith" to implement them.[114] As representatives for the Center wrote, "This is not a meaningful

---

[112] *Members*, *supra* note 108.

[113] EFF, *Press Release: EFF Resigns from Global Network Initiative* (Oct. 10, 2013), https://www.eff.org/press/releases/eff-resigns-global-network-initiative.

[114] Sarah Labowitz & Michael Posner, *NYU Center for Business and Human Rights Resigns Its Membership in the Global Network Initiative*, NYU Stern Center for Business & Human Rights (Feb. 1, 2016),

standard. Our assumption is that all member companies are committed to the principles and are making good faith efforts to implement them; the question is whether they are in compliance with a set of standards."[115]

CONCLUSION

This Court must not shut the courthouse door to victims of human rights abuses powered by private corporations. In the digital age, repressive governments rarely act alone to violate human rights. They have accomplices—sometimes including technology companies that have the sophistication and technical know-how that those repressive governments lack. As the United Nations Special Rapporteur on Freedom of Opinion and Expression noted, "Governments have requirements that their own departments and agencies may be unable to satisfy. Private companies have the incentives, the expertise and the resources to meet those needs."[116]

Technology has the capacity to protect human rights, but it also can make violations ruthlessly efficient. We urge this Court to reverse the district court's dismissal of the complaint under *forum non conveniens* for Defendants-

---

https://web.archive.org/web/20200715032640/https://bhr.stern.nyu.edu/blogs/cbhr-letter-of-resignation-gni.

[115] *Id.*

[116] Kaye, *supra* note 19, at 6.

Appellees. It is critical that U.S. courts remain a viable avenue for holding technology companies accountable for their complicity in human rights abuses committed by repressive governments, especially when the U.S. judicial system may be the only available forum for redress. This Court can help ensure that technological genius supports, rather than undermines, the rule of law.

July 19, 2024

Respectfully submitted,

/s/ Sophia Cope
Sophia Cope
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109-7701
Tel: (415) 436-9333
Fax: (415) 436-9993
sophia@eff.org
andrew@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) because this brief contains 6,851 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5), and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2018 in 14 point Times New Roman font.

Dated: July 19, 2024

/s/ Sophia Cope
Sophia Cope

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 July 19, 2024.

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: July 19, 2024

/s/ Sophia Cope
Sophia Cope