NO. 20-16408

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

NSO GROUP TECHNOLOGIES LTD. ET AL.,

DEFENDANTS-APPELLANTS

v.

WHATSAPP, INC. ET AL.,

PLAINTIFFS-APPELLEES.

On Appeal from the United States District Court
for Northern District of California
Case No. 4:19-cv-07123-PJH

The Honorable Phyllis J. Hamilton, District Court Judge

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLEES AND AFFIRMANCE

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

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.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Rules

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 foreign governments in violating human rights. EFF is a San Francisco-based, member-supported, nonprofit civil liberties organization that has worked for 30 years to protect free speech, privacy, security, and innovation in the digital world. With over 35,000 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, for example, 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

---

[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. Plaintiffs-Appellees consented to the filing of this brief, and Defendants-Appellants have "no objection" to the filing of this brief.

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

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

EFF has also participated as *amicus curiae* in cases focusing on the complicity of American companies in human rights abuses. It filed an *amicus* brief in an Alien Tort Statute (ATS) case recently argued before the U.S. Supreme Court. *Nestlé USA, Inc. v. Doe I*, No. 19-416 (U.S.).[5] It filed *amicus* briefs in an ATS case pending before this Court where plaintiffs alleged 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 abuses. *Doe I v. Cisco Systems, Inc.*, No. 15-16909 (9th Cir.), ECF 15-2 (Jan. 11, 2016).[6] It filed an

---

[3] Lookout & EFF, *Dark Caracal: Cyber-Espionage at a Global Scale*, at 3-4 (2018), 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. *See also* Cooper Quintin & Eva Galperin, *Dark Caracal: You Missed a Spot*, EFF (Dec. 10, 2020), https://www.eff.org/deeplinks/2020/12/dark-caracal-you-missed-spot.

[5] EFF *amicus* brief available at: https://www.supremecourt.gov/DocsketPDF/19/19-416/158434/20201021172033931_19-416%20and%2019-453%20Brief.pdf.

[6] EFF's latest *amicus* brief available at: https://www.eff.org/document/eff-article-19-privacy-international-9th-circuit-amicus-brief.

.

amicus brief in the Second Circuit in an Alien Tort Statute (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.*, No. 14-4104-cv (2d Cir.), ECF 57 (Feb. 11, 2015).[7]

INTRODUCTION AND SUMMARY OF ARGUMENT

This case is not just a dispute between technology companies. The outcome of this case will also 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

[7] EFF *amicus* brief available at: https://www.eff.org/document/eff-amicus-brief-ibm-ats-claim.

good. However, when technology companies—whether foreign or domestic—put profits 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.

Accordingly, *amicus* urges this Court to *deny* Defendants-Appellants (collectively, "NSO Group") any form of foreign sovereign immunity—whether as conduct-based immunity under federal common law, or as derivative foreign sovereign immunity under the Foreign Sovereign Immunities Act. *Cf.* Appellants' Op. Br. 4-5. In so doing, *amicus* also urges this Court to craft a rule that denies foreign sovereign immunity to all private companies, especially those that facilitate violations of human rights. *Cf.* 1-ER-14-15 (citing *Butters v. Vance International, Inc.*, 225 F.3d 462, 466 (4th Cir. 2000)).

It is critical to hold *all* technology companies accountable when they provide their products and services to foreign governments 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 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—either directly or by proxy, as here, where WhatsApp is a Plaintiff although WhatsApp's users were the ultimate targets of NSO Group's surreptitious digital surveillance.

Amicus supports the arguments of the Plaintiffs-Appellees, but also writes to emphasize that denying Defendants-Appellants foreign sovereign immunity is appropriate in light of the fact that corporate complicity in human rights abuses is a widespread and ongoing problem, and that NSO Group in particular has a long history of assisting foreign governments in targeting civil society and violating the human rights of their citizens, along with American technology companies (Part I). This conclusion is also supported by the United Nations' 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 foreign governments.

ARGUMENT

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

This Court should not grant NSO Group or any similarly situated

corporation foreign sovereign immunity, so that Plaintiffs-Appellees here, representing the interests of their users (as well as their own), and human rights victims broadly, have a fighting chance to hold technology companies accountable for their complicity in the human rights abuses perpetrated by foreign governments. 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, 138 S. Ct. 1386, 1406 (2018). This concern is particularly acute for modern technology companies that provide sophisticated surveillance and censorship products and services to foreign governments, enabling those governments to engage in repression on a massive scale. As numerous cases demonstrate, *see infra* Parts I.B. & I.C., powerful digital surveillance tools, like NSO Group's "Pegasus" spyware, are used to identify and track journalists, democracy and human rights activists, and religious minorities. 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 Foreign Governments

There are at least 500 private companies that have provided surveillance technologies to governments around the globe,[8] compiled in the *Surveillance Industry Index* by the UK-based nonprofit organization Privacy International.[9] When Privacy International launched the project, 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."[10] It further lamented the fact that "members of the private surveillance industry have gained a sense of impunity."[11]

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

---

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

[9] Privacy International, *Surveillance Industry Index*, https://sii.transparencytoolkit.org/.

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

[11] *Id.*

Private industry has stepped in, unsupervised and with something close to impunity."[12]

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."[13] 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."[14]

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

---

[12] 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, at 4 (May 28, 2019), https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx.

[13] *Id.* at 3.

[14] *Id.* at 12.

Governments and non-State actors use the tools in legitimate ways."[15] 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."[16]

B. NSO Group is Notorious for Facilitating Human Rights Abuses by Foreign Governments

NSO Group facilitates the surreptitious surveillance of journalists, lawyers, political dissidents, and other members of civil society. NSO Group admits that its customers are "exclusively" foreign governments. Appellants' Op. Br. 31. 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.

WhatsApp discovered that NSO Group breached its systems in April and May 2019 and targeted approximately 1,400 WhatsApp users. 2-ER-70 (Compl. ¶ 42). Citizen Lab[17] conducted research on the WhatsApp hack and uncovered

---

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

[16] 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.

[17] 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/.

more than "100 cases of abusive targeting of human rights defenders and journalists in at least 20 countries across the globe."[18] These happened just weeks *after* NSO Group's new owners asserted that the company "already operates under an ethical governance framework that is significantly more robust than any of its peers."[19] Victims of the WhatsApp hack included Rwandan political dissidents living in exile, who fear that access to their private communications helped the Rwandan government carry out numerous assassinations.[20] NSO Group is also facing another lawsuit for the WhatsApp hack, brought by *Al Jazeera* journalist Ghada Oueiss who believes she was targeted by Saudi Arabia for her critical reporting.[21]

Notorious other cases of NSO Group facilitating the targeting of members

---

[18] 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/.

[19] Stephen Peel, *Response to Open Letter to Novalpina Capital on 18 February 2019*, Novalpina (March 1, 2019), https://www.novalpina.pe/response-to-open-letter-1/. *See also infra* notes 80-81.

[20] 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.

[21] *Oueiss v. Bin Salman Bin Abdulaziz Al Saud*, No. 1:20-cv-25022-JLK (S.D. Fla.), ECF 1 [Compl.] (Dec. 9, 2020), https://www.courthousenews.com/wp-content/uploads/2020/12/1-20cv25022-002.pdf. *See also* Mehul Srivastava, *Al Jazeera Journalist Sues Saudi Crown Prince and UAE Leader Over Phone Hack*, Financial Times (Dec. 10, 2020), https://www.ft.com/content/63d363e1-63bd-47ec-85d2-689330e9032a.

of civil society by foreign governments abound.

Outside of the 2019 WhatsApp hack, Saudi Arabia has used NSO Group's spyware to target critics of the kingdom. Such was the case with Omar Abdulaziz, a Saudi Arabian dissident living in Canada and confidant to fellow kingdom critic and *Washington Post* columnist Jamal Khashogghi.[22] The day after Citizen Lab published its report on the targeting of Mr. Abdulaziz, who regularly exchanged messages with Mr. Khashogghi, Mr. Khashogghi was murdered[23] by order of the Saudi government in the kingdom's embassy in Turkey.[24] Chillingly, Saudi officials tried to lure Mr. Abdulaziz to the kingdom's embassy in Canada.[25] His own family and friends have disappeared

[22] 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.

[23] 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/.

[24] *Jamal Khashoggi: All You Need to Know About Saudi Journalist's Death*, BBC News (July 2, 2020), https://www.bbc.com/news/world-europe-45812399.

[25] *Supra* note 22.

in Saudi Arabia.[26] He also filed a lawsuit in Israel against NSO Group,[27] which moved forward this year.[28] Additionally, the Saudi government targeted *New York Times* journalist Ben Hubbard, who covered the kingdom, for digital surveillance using NSO Group's technology.[29]

The Mexican government has aggressively used NSO Group's spyware to target journalists investigating drug cartels,[30] the wife of a murdered journalist,[31]

---

[26] 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/

[27] David D. Kirkpatrick, *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, New York Times (Dec. 2, 2018), https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html.

[28] Oliver Holmes & Stephanie Kirchgaessner, *Israeli Spyware Firm Fails to Get Hacking Case Dismissed*, The Guardian (Jan. 16, 2020), https://www.theguardian.com/world/2020/jan/16/israeli-spyware-firm-nso-hacking-case.

[29] *Supra* note 23.

[30] John Scott-Railton, et al., *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 (Dec. 30, 2018), https://www.eff.org/deeplinks/2018/12/where-government-hack-their-own-people-and-people-fight-back-latin-american.

[31] John Scott-Railton, et al., *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/.

and lawyers representing the families of a murdered women's rights activist and other victims.[32] The lawyers often criticized the government's handling of high-profile crimes.[33] The Mexican government also targeted its own scientists who supported a soda tax[34] and opposition-party politicians.[35]

Thus, NSO Group's suggestion that its technology is only used to track terrorists and other criminals is manifestly misleading. Appellants' Op. Br. 2.

C. American Technology Companies Have Facilitated Human Rights Abuses by Foreign Governments

American technology companies have also contributed to the global problem of corporate complicity in human rights abuses committed by repressive governments.

In a case currently pending before this Court, members of the Falun Gong

---

[32] John Scott-Railton, et al., *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/.

[33] Associated Press in Mexico City, *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.

[34] 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/.

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

religious minority sued Cisco Systems under the ATS for aiding and abetting human rights abuses by the Chinese government, based on the company's custom development, beginning in the late 1990s, of the "Golden Shield" (also called the "Great Firewall")—a sophisticated Internet surveillance system that enabled the Chinese government to efficiently identify and locate Falun Gong practitioners, who were then apprehended and subjected to torture, forced conversion, and other human rights abuses. *Doe I v. Cisco Systems, Inc.*, No. 15-16909 (9th Cir.).[36]

Similarly, Shi Tao was a well-known pro-democracy journalist in China who was arrested in 2004, convicted in 2005, and imprisoned for nine years because he forwarded to foreign media an email with information about the Chinese government's plan to quell potential protests on the 15th anniversary of the Tiananmen Square massacre.[37] Shi Tao's arrest was directly aided and abetted by Yahoo!, which shared information from his email account with the Chinese government who used it to identify and arrest him.[38] He and other

---

[36] *See also Doe I v. Cisco Systems, Inc.*, No. 5:11-cv-02449-EJD (N.D. Cal.), ECF 113 [Second Amend. Compl.] (Sept. 18, 2013), https://www.eff.org/document/plaintiffs-second-amended-complaint-0.

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

[38] Associated Press in Beijing, *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.

Chinese dissidents sued Yahoo! under the ATS and other laws in 2007, but the parties settled the case later that year.[39] More recently, Ning Xianhua, a pro-democracy activist from China, sued the successor companies, founder, and former CEO of Yahoo! under the ATS for sharing his private emails with the Chinese government, which led to his arrest, imprisonment, and torture.[40]

Victims of South Africa's apartheid sued IBM under the ATS for aiding and abetting the human rights abuses they suffered at the hands of the government. The Second Circuit considered the plaintiffs' allegation that IBM created a customized computer-based national identification system that facilitated the "denationalization" of country's Black population, and concluded that that the "touch and concern" requirement per *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1669 (2013) had been met. *Balintulo v. Ford Motor Co.*, 796 F.3d 160, 169 (2d Cir. 2015).[41] Similarly, a 450-page book

---

[39] *Wang Xiaoning v. Yahoo! Inc.*, No. 4:07-cv-02151-CW (N.D. Cal.). *See also* Business & Human Rights Resource Centre, *Yahoo! Lawsuit (re China)* (June 15, 2015), https://www.business-humanrights.org/en/latest-news/yahoo-lawsuit-re-china/.

[40] *Ning Xianhua v. Oath Holdings, Inc.*, No. 5:20-cv-06185-VKD (N.D. Cal.), ECF 1 [Compl.] (Sept. 2, 2020), https://www.courthousenews.com/wp-content/uploads/2020/09/Ning-v-Yahoo-.pdf.

[41] The Second Circuit ultimately rejected plaintiffs' ATS claim on a separate ground: the plaintiffs had not sufficiently alleged that IBM had the mens rea of "purpose" to facilitate human rights violations by the South African government. *Id*. at 170. What *mens rea* is required ("knowledge" or "purpose")

chronicled in exhaustive detail the fact that, before and during World War II, IBM provided Nazi Germany with early computing technology—their punch card systems—that allowed the Third Reich to efficiently identify and track Jews and other "undesirable" populations. In fact, the infamous numbers tattooed on the arms of Auschwitz inmates began as punch card system identification numbers.[42]

Repressive regimes in the Middle East used Internet surveillance and censorship tools from American technology companies against pro-democracy activists during the Arab Spring.[43] During the 2011 Tunisian revolution—the spark of the Arab Spring[44]—the government used technologies from McAfee,

---

for an ATS aiding and abetting claim is unsettled across the circuits. *See*, *e.g.*, Srish Khakurel, *The Circuit Split on Mens Rea for Aiding and Abetting Liability Under the Alien Tort Statute*, 59 B.C.L. Rev. 2953, 2966 (2018), https://lawdigitalcommons.bc.edu/bclr/vol59/iss8/17.

[42] Edwin Black, IBM and the Holocaust: Expanded Edition (Dialog Press 2012).

[43] Daniel Calingaert, *Hacking the Revolution*, Foreign Policy (Dec. 5, 2011), https://foreignpolicy.com/2011/12/05/hacking-the-revolution/.

[44] Marc Fisher, *In Tunisia, Act of One Fruit Vendor Sparks Wave of Revolution Through Arab World*, Washington Post (March 26, 2011), https://www.washingtonpost.com/world/in-tunisia-act-of-one-fruit-vendor-sparks-wave-of-revolution-through-arab-world/2011/03/16/AFjfsueB_story.html.

Blue Coat Systems,[45] and NetApp.[46] The Syrian government also used Blue Coat Systems and NetApp products.[47] After the U.S. enacted sanctions in 2011,[48] evidence suggested that Syria was using 34 Blue Coat Systems servers.[49] Narus[50] provided Telecom Egypt with Internet surveillance and censorship technology that the government used against protestors during the revolution that eventually ousted longtime Egyptian dictator Hosni Mubarak.[51]

---

[45] Blue Coat Systems has since been acquired by Symantec. Liana B. Baker, *Symantec to Buy Blue Coat for $4.7 Billion to Boost Enterprise Unit*, Reuters (June 12, 2016), https://www.reuters.com/article/us-bluecoat-m-a-symantec/symantec-to-buy-blue-coat-for-4-7-billion-to-boost-enterprise-unit-idUSKCN0YZ0BM.

[46] Elinor Mills, *"Dark Trade" in Web-Censoring Tools Exposed by Pakistan Plan*, CNET (March 20, 2012), https://www.cnet.com/news/dark-trade-in-web-censoring-tools-exposed-by-pakistan-plan/.

[47] *Id. See also* Hamed Aleaziz, *Syria Uses US Technology in Cyber Crackdown*, Mother Jones (Oct. 19, 2011), http://www.motherjones.com/politics/2011/10/blue-coat-systems-internet-blocking-syria.

[48] *See* U.S. State Dept., *Syria Sanctions*, https://www.state.gov/syria-sanctions/.

[49] Cindy Cohn & Dave Maass, *A Warning to Know Your Customer: Computerlinks Fined for Dealing Blue Coat Surveillance Technology to Syria*, EFF (May 28, 2013), https://www.eff.org/deeplinks/2013/05/blue-coat-syria-scandal-next-shoe-drops-computerlinks-fzco.

[50] Narus was formerly a subsidiary of Boeing, which later struck a deal with Symantec. Danny Yadron & Doug Cameron, *Boeing to Exit Commercial Cybersecurity Business*, Wall Street Journal (Jan. 12, 2015), https://www.wsj.com/articles/boeing-to-exit-commercial-cybersecurity-business-1421085602.

[51] Ryan Singel, *Lawmaker Calls for Limits on Exporting Net-Spying Tools*, Wired (Nov. 2, 2011), https://www.wired.com/2011/02/narus/.

The government of Belarus used technology from Sandvine to block much of the Internet during the disputed presidential election earlier this year. The company's technology "played a central role in censoring social media, news and messaging platforms used by protesters rallying against" the re-election of longtime dictator President Alexander Lukashenko.[52] Congress is looking into whether the company violated U.S. sanctions against Belarus.[53] Sandvine's technology is also used by Turkey, Syria, and Egypt against Internet users to redirect them to websites that contain spyware or to block their access to political, human rights, and news content.[54]

Cyberpoint was involved in Project Raven, a surveillance operation ordered by the government of the United Arab Emirates (UAE) against, among others, citizens who criticized the monarchy. "Some days it was hard to swallow, like [when you target] a 16-year-old kid on Twitter," said one

---

[52] Ryan Gallagher, *U.S. Company Faces Backlash After Belarus Uses Its Tech to Block Internet*, Bloomberg (Sept. 11, 2020), https://www.bloomberg.com/news/articles/2020-09-11/sandvine-use-to-block-belarus-internet-rankles-staff-lawmakers.

[53] *Id.*

[54] Ryan Gallagher, *Belarusian Officials Shut Down Internet With Technology Made by U.S. Firm*, Bloomberg (Aug. 28, 2020), https://www.bloomberg.com/news/articles/2020-08-28/belarusian-officials-shut-down-internet-with-technology-made-by-u-s-firm.

American contractor.[55] Cyberpoint also partnered with Hacking Team, the notorious Italian surveillance technology company, to sell Hacking Team's technology to the UAE, who used it against pro-democracy activists.[56]

Finally, the biotechnology firm Thermo Fisher provides the Chinese government with DNA testing kits.[57] The kits are a key component of the government's massive campaign of biometric surveillance—and ultimate control and persecution—against the wider Chinese population, as well as disfavored minority groups such as Tibetans and Muslim Uyghurs.[58] Approximately one million Uyghurs are presently detained is concentration camps in Xinjiang province.[59]

---

[55] Christopher Bing & Joel Schectman, *Inside the UAE's Secret Hacking Team of American Mercenaries*, Reuters (Jan. 30, 2019), https://www.reuters.com/investigates/special-report/usa-spying-raven/.

[56] Lee Fang, *Why Did the Firm That Sold Spyware to the UAE Win a Special Export License from State Department?*, The Intercept (July 7, 2015), https://theintercept.com/2015/07/07/baltimore-firm-supplying-united-arab-emirates-surveillance-software-won-special-export-license-state-department/.

[57] Sui-Lee Wee, *China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment*, New York Times (June 17, 2020), https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html.

[58] Jim Nash, *U.S. DNA Firm Thermo Fisher Reportedly Still Helping China Tamp Unrest, Crime*, Biometric Update (June 19, 2020), https://www.biometricupdate.com/202006/u-s-dna-firm-thermo-fisher-reportedly-still-helping-china-tamp-unrest-crime.

[59] Jen Kirby, *Concentration Camps and Forced Labor: China's Repression of Uighurs, Explained*, Vox (Sept. 25, 2020),

II. United Nations Policy on Business and Human Rights Supports Denying NSO Group Foreign Sovereign Immunity

Denying foreign sovereign immunity to NSO Group or any similarly situated corporation 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 25 years old.[60] It took a powerful step forward 12 years ago 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

---

https://www.vox.com/2020/7/28/21333345/uighurs-china-internment-camps-forced-labor-xinjiang.

[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 emphasizes 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 United States has endorsed the *Guiding Principles* as they specifically apply to U.S. companies that provide digital surveillance technologies to foreign governments.[65]

---

[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. *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.

[65] 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/. *Cf.* European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (July

The *Guiding Principles* 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 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]

This Court should not facilitate "the avoidance of appropriate accountability."[70] Rather, ensuring that companies like NSO Group cannot avoid accountability through foreign sovereign immunity is consistent with the United Nations' goal of establishing judicial avenues for human rights victims to seek

---

2, 2013), https://ec.europa.eu/anti-trafficking/publications/european-commission-sector-guides-implementing-un-guiding-principles-business-and-hum-0_en.

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

[67] *Id.* at 28.

[68] *Id.* at 29.

[69] *Id.*

[70] *Id.* at 29.

justice against corporations that are complicit in abuses perpetrated by governments. The unavailability of foreign sovereign immunity to companies 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, 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*, 133 S. Ct. at 1669 and sufficiently meet the standard tort elements of *mens rea* and *actus reus*, among others.[71]

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

It is especially important that this Court deny companies like NSO Group foreign sovereign immunity—and thereby give plaintiffs a fighting chance in U.S. courts—given that voluntary mechanisms for holding technology

[71] *See, e.g.*, *supra* note 41.

companies accountable for their roles in human rights abuses have proven inadequate. The Ruggie Report recognizes that "companies can affect virtually all internationally recognized rights."[72] The report even uses 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."[73]

The Ruggie Report argues that companies, therefore, must practice "due diligence," which involves taking steps "to become aware of, prevent and address adverse human rights impacts."[74] Due diligence[75] includes the consideration of several factors, such as "whether [the company] might contribute to abuse through the relationships connected to their activities, such

---

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

[73] *Id.* at 20.

[74] *Id.* at 17.

[75] *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 (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 (July 13, 2018), https://www.eff.org/deeplinks/2018/07/should-your-company-help-ice-know-your-customer-standards-evaluating-domestic.

as with business partners, suppliers, State agencies, and other non-State actors."[76] 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.[77]

However, the *Guiding Principles* expressly do not create any "new international law obligations."[78] Thus, the Ruggie Report's "due diligence" framework for companies is wholly voluntary. The report contemplates that voluntary mechanisms would play a significant role in corporate accountability for human rights violations.[79] 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 fact that NSO Group itself has a "due diligence" human rights

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

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

[78] *Id.* at 1.

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

program[80] yet governmental abuses continue.[81] Enforcement generally of human rights standards through voluntary corporate accountability mechanisms has been weak at best.

A. Limits of Multi-Stakeholder Initiatives

A recent report by MSI Integrity[82] 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."[83] This includes the leading

---

[80] NSO Group, *Human Rights Policy*, https://www.nsogroup.com/governance/human-rights-policy/. *See also* Novalpina Capital, *NSO Group Announces New Human Rights Policy and Governance Framework* (Sept. 11, 2019), https://www.novalpina.pe/nso-group-announces-new-human-rights-policy-and-governance-framework/.

[81] *See, e.g.*, 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/.

[82] 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/.

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

technology-industry focused MSI, called the Global Network Initiative (GNI), discussed below. *See infra* Part III.C.[84]

The report correctly recognized that MSIs can only achieve "positive outcomes where there is genuine commitment on the part of corporate members to change."[85] The report emphasized that "MSIs do not eliminate the need to protect rights holders from corporate abuses through effective regulation and enforcement."[86] 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.

This Court must recognize that denying companies like NSO Group foreign sovereign immunity gives human rights victims a chance to enforce—through a binding judicial process—human rights standards against foreign or domestic corporations that are not willing to police themselves and that cause grave harm to individuals around the world.

---

[84] *Id.* at 24.

[85] *Id.* at 5.

[86] *Id.*

B. OECD Guidelines for Multinational Enterprises

The Organization for Economic Cooperation & Development (OECD)[87] wrote the *Guidelines for Multinational Enterprises* that comprise recommendations for "responsible business conduct," which address the realm of human rights, among other areas.[88] The human rights chapter specifically cites the Ruggie Report's "due diligence" framework and the UN's *Guiding Principles* as the bases for the OECD's human rights recommendations.[89] 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*.[90] Specific Instances can lead to mediation between the complainant

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

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

[89] Organization for Economic Cooperation & Development, *OECD Guidelines for Multinational Enterprises, 2011 Edition*, at 31-34, http://www.oecd.org/daf/inv/mne/48004323.pdf.

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

and the company.[91] The National Contact Point for the United States is housed at the State Department.[92] The key shortcomings of the NCP/Specific Instance system are two-fold.[93] 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,[94] with only one relating to the telecommunications industry (involving T-Mobile and labor practices).[95] Second and more fundamentally, "the OECD Guidelines are non-binding on businesses and engagement in a Specific Instance process is voluntary."[96]

---

[91] Organization for Economic Cooperation & Development, *Frequently Asked Questions: National Contact Points for OECD Guidelines for Multinational Enterprises* (2017), http://www.oecd.org/investment/mne/National-Contact-Points-for-RBC-Frequently-Asked-Questions.pdf.

[92] U.S. State Dept., *U.S. National Contact Point for the OECD Guidelines for Multinational Enterprises* (April 11, 2019), https://www.state.gov/u-s-national-contact-point-for-the-oecd-guidelines-for-multinational-enterprises/.

[93] *See, e.g.*, U.S. State Dept., *Specific Instance Process* (April 24, 2019), https://www.state.gov/u-s-national-contact-point-for-the-oecd-guidelines-for-multinational-enterprises/specific-instance-process/.

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

[95] 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.

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

This latter shortcoming was on full display in the United Kingdom, providing a stark example for the technology industry.[97] Privacy International 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.[98]

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

---

[97] Similarly, the UK-based nonprofit Business & Human Rights Resource Centre collects human rights complaints against companies and solicits 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* ("The overall worldwide company response rate to us is an average of 73%."), https://www.business-humanrights.org/en/from-us/company-response-mechanism/.

[98] 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.*, at 2 (June 2013), 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.

> progress (or effort) towards meeting the recommendations made in the Final Statement.[99] The UK NCP therefore sees no reason to 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.[100]

C. Global Network Initiative

GNI is a human rights corporate accountability program that focuses specifically on the information and communications technology (ICT) sector.[101] GNI was born out of the tragic case of Shi Tao, discussed above, where Yahoo! shared information from his email account with the Chinese government, which led to his arrest and imprisonment for nearly a decade. *See supra* Part I.C.

GNI is a voluntary program that follows a multi-stakeholder model, where its members include American and foreign technology companies, as well as

---

[99] *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.

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

[101] GNI is a U.S.-based nonprofit organization. Global Network Initiative, *Financials*, https://globalnetworkinitiative.org/team/financials/.

civil society groups, academics, and investment firms.[102] Over two years of painstaking effort went into creating GNI,[103] including the foundational *Principles on Free Expression and Privacy*[104] and the related *Implementation Guidelines*, which require technology company members to submit to independent "assessments" or audits of their implementation of the *Principles*.[105]

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—presently only 15 companies participate in GNI. 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.

---

[102] Global Network Initiative, *Our Members*, https://globalnetworkinitiative.org/#home-menu.

[103] Global Network Initiative, *About GNI*, https://globalnetworkinitiative.org/about-gni/.

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

[105] Global Network Initiative, *Implementation Guidelines*, https://globalnetworkinitiative.org/implementation-guidelines/.

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.[106] Additionally, the NYU Stern Center for Business & Human Rights resigned from GNI in 2016 due, in part, to the organization'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. As representatives for the Center wrote, "This is not a meaningful 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."[107]

CONCLUSION

This Court must not shut the courthouse door to victims of human rights abuses powered by foreign or domestic corporations. In the digital age, repressive governments rarely act alone to violate human rights. They have

---

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

[107] 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), https://bhr.stern.nyu.edu/blogs/cbhr-letter-of-resignation-gni.

accomplices—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."[108]

Technology has the capacity to protect human rights, but it also can make violations ruthlessly efficient. We urge this Court to *deny* Defendants-Appellants any form of foreign sovereign immunity—whether as conduct-based immunity under federal common law, or as derivative foreign sovereign immunity under the Foreign Sovereign Immunities Act. In so doing, this Court should craft a rule that denies foreign sovereign immunity to all private companies, especially those that facilitate violations of human rights. It is critical that U.S. courts remain a viable avenue for holding all 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 avenue of redress. This Court can help ensure that technological

[108] Kaye, *supra* note 12, at 6.

genius supports, rather than undermines, the rule of law.

December 21, 2020

Respectfully submitted,

By: */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 6,637 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: December 21, 2020

By: *<u>/s/ Sophia Cope</u>*
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 December 21, 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.

Dated: December 21, 2020 By: */s/ Sophia Cope*
Sophia Cope