Nos. 19-416 & 19-453

IN THE

Supreme Court of the United States

NESTLÉ USA, INC.,

Petitioner,

v.

JOHN DOE I, *et al.*,

Respondents.

CARGILL, INC.,

Petitioner,

v.

JOHN DOE I, *et al.*,

Respondents.

ON WRITS OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

BRIEF OF *AMICI CURIAE* ACCESS NOW, ARTICLE 19, CENTER FOR LONG-TERM CYBERSECURITY, ELECTRONIC FRONTIER FOUNDATION, PRIVACY INTERNATIONAL AND PROFESSOR RONALD DEIBERT IN SUPPORT OF RESPONDENTS

SOPHIA COPE
Counsel of Record
CINDY COHN
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
sophia@eff.org

Attorneys for Amici Curiae

298803

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

Cases

Page

Other Authorities

Cited Authorities

Cited Authorities

Cited Authorities

Page

Page

Page

Page

Page

Page

INTEREST OF *AMICI CURIAE*[1]

Amici curiae are nonpartisan non-governmental and academic organizations and individuals that advocate for civil liberties and human rights around the world. We have a strong interest in ensuring that the law discourages—and creates real accountability for—American companies that assist foreign governments in violating human rights.

Access Now is a non-governmental organization with offices in several international cities, including Washington, DC, and New York, that seeks to defend and extend the digital rights of users at risk around the world. It is nonpartisan, not-for-profit, and not affiliated with any country, corporation, or religion. Its activities include direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon. It runs the Digital Security Helpline, which is a 24/7, free-of-charge resource for civil society across the globe that assists journalists, activists, and human rights defenders who are targeted with spyware and other surveillance technologies on a regular basis.[2] It also routinely files *amicus* briefs with domestic jurisdictions, including the United States, on a variety of digital rights issues.

---

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 *amici 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. Access Now, *Digital Security Helpline*, https://www.accessnow.org/help/.

ARTICLE 19 was founded in 1987 and has an international office in London, UK, and regional offices in Brazil, Mexico, Senegal, Kenya, Bangladesh, and Myanmar. The organization, named for the corresponding article of the Universal Declaration of Human Rights, advocates for freedom of expression as a fundamental human right, including in the digital environment. It has participated as *amicus curiae* in free expression cases around the world, including in the United States. It also actively participates in discussions at the United Nations Human Rights Council and the United Nations General Assembly on issues related to digital technologies and human rights.

Center for Long-Term Cybersecurity (CLTC) was established in 2015 as a research and collaboration hub within University of California, Berkeley's School of Information. CLTC's mission is to help individuals and organizations address tomorrow's information security challenges to amplify the upside of the digital revolution. CLTC runs the Citizen Clinic, a multidisciplinary, public-interest digital security clinic that empowers civil society organizations to use technology to fulfill their missions and defend against digital threats from governments, powerful corporations, hate groups, and extremists. Citizen Clinic's client organizations across the globe are frequently the target of surveillance by repressive governments.

Electronic Frontier Foundation (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 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. It has led investigations into misuse of surveillance technologies by governments to target citizens for human rights abuses.[3] EFF has also participated as *amicus curiae* in cases focusing on the complicity of American corporations in governmental human rights abuses. It filed an *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).[4] It also filed *amicus* briefs in the Ninth Circuit in an ATS case 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).[5] The *Cisco* case is still pending and is contingent on the outcome of this case.

Privacy International was founded in 1990 and is based in London, UK. It was the first organization to campaign at an international level on privacy issues. It is committed to protecting people's privacy, dignity, and

---

3. Electronic Frontier Foundation, *Surveillance Technologies*, https://www.eff.org/issues/mass-surveillance-technologies.

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

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

freedoms from abuses by companies and governments. Through research, litigation and advocacy, it works to build a better future where technologies, laws, and policies contain modern safeguards to protect people and their data from exploitation.

Ronald Deibert is Professor of Political Science and Director of Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy at the University of Toronto in Canada that researches digital threats to privacy and free expression against civil society by nation-states and private actors.

INTRODUCTION AND SUMMARY OF ARGUMENT

This case does not just concern chocolate and children. 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 American companies are tremendously useful to uncontroversial customers, other technologies—or sometimes even the same technologies when deployed by repressive regimes—can facilitate horrific human rights abuses.

As experts focused on the intersection of civil liberties, human rights, and technology, *amici* support innovation while also calling for the responsible deployment of technology. We applaud the role that Silicon Valley has 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. To be clear, we do not believe that American technology companies should be liable for violations of international law under the Alien Tort Statute (ATS) *solely* because their general-purpose or dual-purpose technologies ended up in the hands of foreign governments or others who misused them to violate human rights.

However, when American technology companies put profits over basic human well-being, and people in foreign countries are seriously harmed or even killed by those choices, legal accountability is necessary. Accordingly, *amici* urge this Court to preserve U.S. corporate liability under the ATS, as well as the aiding and abetting claim (which is applicable under U.S. law to any other American),

to ensure accountability for American technology companies that provide their products and services to foreign governments that clearly intend to, and do, use them to commit gross human rights abuses. Victims of unlawful arrest and detention, torture, disappearances, summary execution, and other horrific human rights abuses abroad, that were enabled by powerful technologies provided by American companies, must have the ability to seek redress through civil suits under the ATS.[6]

Amici here support the arguments of the Plaintiffs-Respondents, but also write to emphasize that this conclusion is supported by the policy underlying the ATS, as well as internationally, by the United Nations' policy on business and human rights (Parts I & II). It is especially important in light of the fact that U.S. corporate complicity in human rights abuses is a widespread and ongoing problem (Part III), and the technology industry's voluntary accountability mechanisms have been largely ineffective (Part IV). In short, the rarely needed yet powerful statutory mechanism that the ATS provides should be available to those grossly harmed with the assistance of American companies.

6. *Amici* accept that liability under the ATS requires, in part, an American company's actions to sufficiently "touch and concern" the United States, consistent with *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1669 (2013).

ARGUMENT

I. ATS Policy Supports Preserving U.S. Corporate Liability Under the Statute

Preserving U.S. corporate liability under the ATS, including via an aiding and abetting claim, is consistent with the policy underlying the statute. As this Court noted, the First Congress passed the ATS to allow foreign plaintiffs to seek justice for "a narrow set of violations of the law of nations" where the lack of a clear pathway for accountability would otherwise "threaten[] serious consequences in international affairs." *Sosa v. Alvarez-Machain*, 542 U.S. 692, 715 (2004).[7] That was because "international law during the founding era was understood to place an affirmative obligation on the United States to redress certain violations of the law of nations, even when those violations were perpetrated by private individuals."[8] This Court further explained that "[t]he principal objective of the statute … was to avoid foreign entanglements by ensuring the availability of a federal forum where the failure to provide one might cause another nation to hold the United States responsible for an injury to a foreign citizen." *Jesner v. Arab Bank, PLC*, 138 S. Ct. 1386, 1397 (2018).[9]

---

7. For purposes of this brief, *amici* refer to this narrow set of international law violations as "gross" human rights abuses or violations.

8. Stephen P. Mulligan, *The Alien Tort Statute (ATS): A Primer*, Congressional Research Service, at 3 (June 1, 2018), https://fas.org/sgp/crs/misc/R44947.pdf.

9. *Jesner* then held that the ATS does not apply to *foreign* corporations, *id.* at 1408, reasoning that granting U.S. courts the ability, on behalf of foreign plaintiffs, to hold foreign corporations

Thus, it is wholly appropriate, and consistent with U.S. interests, for U.S. courts to exercise jurisdiction over American corporations under the ATS. *See id.* at 1414 (Gorsuch, J., concurring in part and concurring in the judgment) (arguing the ATS should be limited to "domestic defendant[s]").[10] Allowing foreign plaintiffs to hold American corporations accountable in U.S. courts for gross human rights violations may actually "promote harmony in international relations"—the positive goal of the ATS. *See id.* at 1406. As Justice Sotomayor explained with respect to *any* corporation, "[H]olding corporations accountable for violating the human rights of foreign citizens when those violations touch and concern the United States may well be necessary to avoid the international tension with which the First Congress was concerned." *Id.* at 1435 (Sotomayor, J., dissenting).

II. United Nations Policy Supports Preserving U.S. Corporate Liability Under the ATS

Preserving U.S. corporate liability under the ATS, including via an aiding and abetting claim, is not only supported by the legislative history of the statute, it is consistent with settled United Nations policy. The concept of "business and human rights," as a subset of corporate

---

liable for human rights abuses might cause "diplomatic strife" between the U.S. and the home countries of those foreign corporate defendants, *id.* at 1412 (Alito, J., concurring). Of course, Defendants here are American companies.

10. *See also* Mulligan, *supra* note 8, at 20 (Justice Gorsuch argued in *Jesner* that "the history of the ATS shows that the statute was intended to apply only to claims against U.S. defendants—regardless of whether they are corporations or natural persons.").

social responsibility, is over 25 years old.[11] 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.[12]

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 [3] the need for more effective access to remedies."[13] The Ruggie Report emphasizes that the governmental duty to protect and the corporate responsibility to respect human rights are distinct (albeit intertwined) obligations.[14]

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

11. 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.

12. 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.

13. *Id.* at 4.

14. *Id.* at 17.

framework.[15] The *Guiding Principles* provide, relevant here, that national governments should "take steps to prevent abuse *abroad* by business enterprises within their jurisdiction"[16] and "to ensure the effectiveness of domestic judicial mechanisms when addressing business-related human rights abuses."[17]

The *Guiding Principles* 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."[18] 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."[19]

---

15. 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://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G11/144/71/PDF/G1114471.pdf?OpenElement.

16. *Guiding Principles*, *supra* note 15, at 4 (emphasis added).

17. *Id.* at 28.

18. *Id.* at 29.

19. *Id.*

Thus, this Court should not facilitate "the avoidance of appropriate accountability." Rather, preserving U.S. corporate liability under the ATS, including via an aiding and abetting claim (which is a standard part of every modern legal system around the world), is consistent with the United Nations' goal of establishing judicial avenues for human rights victims to seek justice against domestic corporations that are complicit in abuses perpetrated in foreign countries.

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

Although this Court unfortunately foreclosed liability for foreign corporations under the ATS, this Court must preserve liability for American corporations, including through the standard aiding and abetting claim, so that foreign plaintiffs can hold American technology companies accountable for their complicity in gross human rights abuses. As noted above, liability helps protect U.S. interests from the vagaries of foreign governmental responses to U.S. corporate wrongdoing. *See supra* Part I. Moreover, the fact that the wrongdoing is done by corporations, rather than individuals, should not change the calculus. In *Jesner*, this Court correctly recognized that:

> natural persons can and do use corporations for sinister purposes, including conduct that violates international law … the 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.

138 S. Ct. at 1406. While this case involves more traditional companies, this concern is equally true for modern technology companies, including American companies that have provided sophisticated surveillance and censorship products and services to foreign governments that enable them to engage in repression on a massive scale. As numerous cases demonstrate, *see infra* Part III.B., powerful Internet surveillance tools, for example, not only invade digital privacy, they can also be used to identify and track journalists, activists, and religious minorities, and can facilitate physical apprehension, unlawful detention, torture, disappearances, and even summary execution.

The United Nations Special Rapporteur on Freedom of Opinion and Expression, in a scathing 2019 report on the surveillance industry's complicity in human rights abuses by repressive regimes, rightly asserted: "The lack of causes of action and remedies raises serious concerns about the likelihood of holding companies accountable for human rights violations."[20] This Court should not further block the availability of remedies to those victimized by repressive governments and the American technology companies that aid and abet those governments.

A. Researchers Chronicle the Widespread Problem of Technology Companies' Complicity in Human Rights Abuses

The complicity of some technology companies in human rights violations—especially violations of privacy,

20. 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 12 (May 28, 2019), https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx.

freedom of expression, and freedom of association, and physical abuse in the form of unlawful arrest and detention, torture, disappearances, and summary execution—is so widespread that a variety of organizations are dedicated to chronicling (and trying to combat) this global problem.

In his 2019 report, the Special Rapporteur 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."[21] His 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."[22]

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 Governments and non-State actors use the tools in legitimate ways."[23] In an op-ed, the Special Rapporteur rejected the notion that it is "complicated" to protect privacy and human rights: "All I can say is, give me a break."[24]

---

21. *Id.* at 4.

22. *Id.* at 3.

23. *Id.* (emphasis added).

24. David Kaye, *The Surveillance Industry is Assisting State Suppression. It Must be Stopped*, The Guardian (Nov. 26, 2019),

Several nonpartisan academic institutions also research the technology industry's contributions to human rights abuses. Most notable is Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy at the University of Toronto.[25] Citizen Lab has a research project dedicated to "targeted threats," which investigates "the prevalence and impact of digital espionage operations against civil society groups."[26] Citizen Lab also studies "Internet filtering, network interference, and other technologies and practices that impact freedom of expression online."[27] Citizen Lab has researched the world's most notorious private surveillance companies and their partnerships with repressive governments, including NSO Group, based in Israel,[28] and Hacking Team, based in Italy.[29]

The Center for Long-Term Cybersecurity (CLTC) at University of California, Berkeley, goes a step further

---

https://www.theguardian.com/commentisfree/2019/nov/26/surveillance-industry-suppression-spyware.

25. Citizen Lab, *About the Citizen Lab*, https://citizenlab.ca/about/.

26. Citizen Lab, *Targeted Threats*, https://citizenlab.ca/category/research/targeted-threats/.

27. Citizen Lab, *Free Expression Online*, https://citizenlab.ca/category/research/free-expression-online/.

28. *See, e.g.*, 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/.

29. *See, e.g.*, Amitpal Singh, *Hacking Team Leak Highlights Citizen Lab Research*, Citizen Lab (Aug. 6, 2015), https://citizenlab.ca/2015/08/hacking-team-leak-highlights-citizen-lab-research/.

and provides defensive help against the government surveillance fueled by private companies. CLTC manages the Citizen Clinic,[30] which is a "public-interest cybersecurity clinic" that "supports the capacity of politically-vulnerable organizations to defend themselves against online threats."[31] CLTC recognizes that "[w]ithout additional resources and methods for building under-resourced organizations' cybersecurity capacity, governments, hate groups, and private spyware companies will further disrupt the ability of civil society to operate online."[32]

Nonprofits or nongovernmental organizations (NGOs) also research the technology industry's involvement in human rights violations. *Amicus* 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 German company FinFisher and likely other private entities.[33] The report also revealed that the government of Kazakhstan used the same infrastructure

30. Center for Long-Term Cybersecurity, *About the Center*, https://cltc.berkeley.edu/about-us/.

31. Center for Long-Term Cybersecurity, *Citizen Clinic*, https://cltc.berkeley.edu/about-us/citizen-clinic/.

32. Center for Long-Term Cybersecurity, *Defending Politically Vulnerable Organizations Online*, https://cltc.berkeley.edu/defendingpvos/.

33. Lookout & Electronic Frontier Foundation, *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.

to target journalists, lawyers, and dissidents.[34] Similarly, Citizen Lab and *amicus* Access Now have chronicled the use of FinFisher technology by Middle Eastern governments against dissidents.[35]

Amicus Privacy International maintains the *Surveillance Industry Index*,[36] a database of over 500 private companies that have provided surveillance technologies to governments around the globe.[37] 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."[38] It further lamented the fact that "members of the private surveillance industry have gained a sense of impunity."[39]

Amicus Access Now publishes the *Transparency Reporting Index*, which tracks technology companies'

34. *Id.* at 1, 2, 4.

35. Lucie Krahulcova, *New Report: FinFisher Changes Tactics to Hook Critics*, Access Now (May 14, 2018), https://www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics/.

36. Privacy International, *Surveillance Industry Index*, https://sii.transparencytoolkit.org/.

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

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

39. *Id.*

transparency reports related to privacy and free expression.[40] "Such reports help users understand a company's policies and safeguards against government abuses. Disclosures illuminate the scope and scale of online surveillance, internet shutdowns, content removal, and a host of other practices impacting our fundamental rights."[41] Similarly, New America's Ranking Digital Rights Project[42] publishes the *Corporate Accountability Index*,[43] which ranks "the world's most powerful internet, mobile, and telecommunications companies" on their commitments and policies related to privacy and freedom of expression on the Internet.[44]

Traditional human rights organizations such as Human Rights Watch[45] and Amnesty International[46] now

40. Access Now, *Transparency Reporting Index*, https://www.accessnow.org/transparency-reporting-index/.

41. *Id.*

42. Ranking Digital Rights, *Governance*, https://rankingdigitalrights.org/who/governance/.

43. *See* Ranking Digital Rights, *2019 Corporate Accountability Index*, https://rankingdigitalrights.org/index2019/.

44. Ranking Digital Rights, *About Ranking Digital Rights*, https://rankingdigitalrights.org/about/.

45. *See, e.g.*, Yaqiu Wang, *Chinese Tech Firms Fueling Beijing's Repression*, Human Rights Watch (Sept. 28, 2020), https://www.hrw.org/news/2020/09/28/chinese-tech-firms-fueling-beijings-repression.

46. *See, e.g.*, Amnesty International, *EU Companies Selling Surveillance Tools to China's Human Rights Abusers* (Sept. 21, 2020), https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/.

have staff dedicated to the issue of the technology and human rights, and have highlighted the use of technology to spy on and censor journalists, activists, and other political opponents of repressive regimes.

B. American Technology Companies Have Been Complicit in Human Rights Abuses in Foreign Countries

Sadly, some American technology companies have contributed to the global problem of corporate complicity in human rights abuses committed by repressive governments. While by definition it will only be applied in a narrow set of extreme circumstances, the ATS, including the aiding and abetting claim, must remain a viable option for foreign victims of gross human rights violations to seek justice.

In a case currently pending before the Ninth Circuit (and contingent on the outcome of this case), members of the Falun Gong 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.).[47]

47. *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.

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.[48] 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.[49] He and other Chinese dissidents sued Yahoo! under the ATS and other laws in 2007, but the parties settled the case later that year.[50] More recently, Ning Xianhua, a pro-democracy activist from China, just last month 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.[51]

---

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

49. 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.

50. *Wang Xiaoning, et al. v. Yahoo! Inc., et al.*, 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/.

51. *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.

Victims of apartheid sued IBM under the ATS for aiding and abetting the human rights abuses they suffered at the hands of the South African 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* had been met. *Balintulo v. Ford Motor Co.,* 796 F.3d 160, 169 (2d Cir. 2015).[52] Similarly, a 450-page book 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.[53]

Repressive regimes in the Middle East used Internet surveillance and censorship tools from American technology companies against pro-democracy activists during the Arab Spring.[54] During the Tunisian revolution—

---

52. 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") 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.

53. Edwin Black, *IBM and the Holocaust: Expanded Edition* (Dialog Press 2012).

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

the spark of the Arab Spring[55]—the government used technologies from McAfee, Blue Coat Systems,[56] and NetApp.[57] The Syrian government also used Blue Coat Systems and NetApp products.[58] After the U.S. enacted sanctions in 2011,[59] evidence suggested that Syria was using 34 Blue Coat Systems servers.[60] Narus[61] provided

---

55. 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.

56. 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.

57. 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/.

58. *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.

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

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

61. 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

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.[62]

More recently, the notorious NSO Group was implicated in the government-ordered murder[63] of Saudi Arabian dissident and *Washington Post* journalist Jamal Khashoggi in 2018.[64] NSO Group, although based in Israel, was majority owned by the San Francisco-based private equity firm Francisco Partners[65] until February 2019.[66]

Journal (Jan. 12, 2015), https://www.wsj.com/articles/boeing-to-exit-commercial-cybersecurity-business-1421085602.

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

63. *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.

64. 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.

65. DJ Pangburn, *U.S. Fund Sells Israeli Hacking Firm NSO Group Amid Spy Mystery*, Fast Company (Feb. 14, 2019), https://www.fastcompany.com/90307864/u-s-fund-sells-israeli-hacking-firm-nso-group-amid-spy-mystery.

66. Involving another audacious campaign by NSO Group, the company was sued for targeting civil society users of Facebook's messaging app WhatsApp, albeit after the sale, in April and May 2019. *WhatsApp Inc. v. NSO Group Technologies Ltd.*, No. 4:19-cv-07123-PJH (N.D. Cal.), ECF 1 [Compl.] (Oct. 29, 2019), https://docs.justia.com/cases/federal/district-courts/california/candce/3:2019cv07123/350613/1. *See also* Stephanie Kirchgaessner, *US Judge: WhatsApp Lawsuit Against Israeli*

The government of Belarus used technology from Sandvine, currently owned by Francisco Partners, to block much of the Internet during the disputed presidential election in August of 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.[67] Congress is looking into whether the company violated U.S. sanctions against Belarus.[68] 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.[69]

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 American contractor.[70] Cyberpoint also

---

Spyware Firm NSO Can Proceed, The Guardian (July 17, 2020), https://www.theguardian.com/technology/2020/jul/17/us-judge-whatsapp-lawsuit-against-israeli-spyware-firm-nso-can-proceed.

67. 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.

68. *Id.*

69. 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.

70. Christopher Bing & Joel Schectman, *Inside the UAE's Secret Hacking Team of American Mercenaries*, Reuters (Jan.

partnered with Hacking Team, the notorious surveillance technology company from Italy, to sell Hacking Team's technology to the UAE, who used it against pro-democracy activists.[71]

Finally, the biotechnology firm Thermo Fisher provides the Chinese government with DNA testing kits.[72] 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 Uighurs.[73] Approximately one million Uighurs are presently detained is concentration camps in Xinjiang province.[74]

30, 2019), https://www.reuters.com/investigates/special-report/usa-spying-raven/.

71. 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/.

72. 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.

73. 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.

74. Jen Kirby, *Concentration Camps and Forced Labor: China's Repression of Uighurs, Explained*, Vox (Sept. 25, 2020), https://www.vox.com/2020/7/28/21333345/uighurs-china-internment-camps-forced-labor-xinjiang.

Every situation listed above likely would not result in a successful ATS claim, given the built-in hurdles of the "touch and concern" requirement under *Kiobel* and the standard tort elements of *mens rea* and *actus reus*, among others.[75] But the fact that American technology has been and is currently being widely used by repressive governments abroad should give this Court pause before removing this critical legal disincentive and avenue for redress.

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

It is especially important that this Court preserve the ATS as a statutory mechanism for redress given that voluntary mechanisms to hold technology 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."[76] 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."[77]

The Ruggie Report argues that companies, therefore, must practice "due diligence," which involves taking steps "to become aware of, prevent and address adverse

75. *See, e.g.*, *supra* note 52.

76. Ruggie, *supra* note 12, at 9.

77. *Id.* at 20.

human rights impacts."[78] Due diligence[79] includes the consideration of several factors, such as "whether [the company] might contribute to abuse through the relationships connected to their activities, such as with business partners, suppliers, State agencies, and other non-State actors."[80]

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.[81]

---

78. *Id.* at 17.

79. *Amicus* EFF 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*, Electronic Frontier Foundation (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*, Electronic Frontier Foundation (July 13, 2018), https://www.eff.org/deeplinks/2018/07/should-your-company-help-ice-know-your-customer-standards-evaluating-domestic.

80. Ruggie, *supra* note 12, at 17.

81. *Guiding Principles*, *supra* note 15, at 14-15.

However, the *Guiding Principles* expressly do not create any "new international law obligations."[82] Thus, the Ruggie Report's "due diligence" framework for companies is wholly voluntary.[83] The report instead contemplated that voluntary mechanisms would play a significant role in corporate accountability for human rights violations.[84] Unfortunately, while the Ruggie Report and the UN's *Guiding Principles* helped spur progress in defining the right courses of action on business and human rights, the hoped-for enforcement has been weak, at best—and this includes enforcement through voluntary corporate accountability mechanisms.

---

82. *Id.* at 1.

83. The United States and European Union have endorsed the *Guiding Principles* via their own voluntary guidelines. *See* 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/. *See also* European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (July 2, 2013), https://ec.europa.eu/anti-trafficking/publications/european-commission-sector-guides-implementing-un-guiding-principles-business-and-hum-0_en.

84. Ruggie, *supra* note 12, at 26. *See also Guiding Principles*, *supra* note 15, at 28, 31.

A. Limits of Multi-Stakeholder Initiatives

A recent report by MSI Integrity[85] 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."[86] This includes the leading technology-industry focused MSI, called the Global Network Initiative (GNI), discussed below. *See infra* Part IV.C.[87]

The report correctly recognized that MSIs can only achieve "positive outcomes where there is genuine commitment on the part of corporate members to change."[88] The report emphasized that "MSIs do not eliminate the need to protect rights holders from corporate abuses through effective regulation and enforcement."[89] While

---

85. 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/.

86. 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.

87. *Id.* at 24. The report also highlights the failure of MSIs to prevent child and forced labor in the cocoa industry. *Id.* at 45, 91, 134.

88. *Id.* at 5.

89. *Id.*

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 the ATS has an important role to play in enforcing—through a binding judicial process—human rights standards against those few American 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)[90] wrote the *Guidelines for Multinational Enterprises* that comprise recommendations for "responsible business conduct," which address the realm of human rights, among other areas.[91] 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.[92] The accountability mechanism

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

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

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

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*.[93] Specific Instances can lead to mediation between the complainant and the company.[94] The National Contact Point for the United States is housed at the State Department.[95] The key shortcomings of the NCP/Specific Instance system[96] are two-fold: 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,[97] with only one relating to the telecommunications industry

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

94. 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.

95. 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/.

96. *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/.

97. 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.

(involving T-Mobile and labor practices).[98] Second and more fundamentally, "the OECD Guidelines are non-binding on businesses and engagement in a Specific Instance process is voluntary."[99]

This latter shortcoming was on full display in the United Kingdom, providing a stark example for the technology industry.[100] *Amicus* 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,

98. 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.

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

100. 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/.

> who had not committed any criminal offences under Bahrain law, were subsequently detained and in some cases tortured by the Bahrain security forces.[101]

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.[102] 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.[103]

---

101. 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.

102. *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.

103. UK National Contact Point, *Follow Up Statement After Recommendations In Complaint From Privacy International Against Gamma International*, at 4 (Feb. 2016), https://assets.

C. Global Network Initiative

GNI is a human rights corporate accountability program that focuses specifically on the information and communications technology (ICT) sector.[104] 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 III.B.

GNI is a voluntary program that follows a multi-stakeholder model, where its members include not only technology companies—including major players such as Google and Facebook—but also civil society groups, academics, and investment firms.[105] Over two years of painstaking effort went into creating GNI,[106] including the foundational *Principles on Free Expression and Privacy*[107] and the related *Implementation Guidelines*, which require technology company members to submit to independent

---

publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/847364/uk-ncp-follow-up-statement-privacy-international-gamma-international.pdf.

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

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

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

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

"assessments" or audits of their implementation of the *Principles*.[108]

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. For example, *amicus* EFF 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 spearheaded by the National Security Agency. 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.[109] 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

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

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

are making good faith efforts to implement them; the question is whether they are in compliance with a set of standards."[110]

CONCLUSION

This Court must not shut the courthouse door to victims of gross human rights abuses powered by American companies. In the digital age, repressive governments rarely act alone to grossly violate human rights. They have accomplices—sometimes including American 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."[111]

We urge this Court to preserve U.S. corporate liability under the ATS, as well as the aiding and abetting claim, to allow a narrow slice of foreign plaintiffs to hold American companies, including technology companies, accountable for their active complicity in gross human rights abuses by repressive governments. This is important when the U.S. judicial system may be the only available form of

110. 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.

111. Kaye, *supra* note 20, at 6.

redress,[112] and when the lack of any other accountability mechanisms for American corporations may cause or heighten international tensions.

While this case is not specifically about technology, the impact it will have on technology is clear. Technology has the capacity to protect human rights, but it also can make violations ruthlessly efficient. Maintaining the ATS as a viable option for holding American companies accountable protects human rights victims and, ultimately, broader U.S. international interests, and helps ensure that American technological genius supports, rather than undermines, the rule of law.

October 21, 2020

Respectfully submitted,

Sophia Cope
Counsel of Record
Cindy Cohn
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
sophia@eff.org

Attorneys for Amici Curiae

112. *See, e.g.*, Resp. Br. (No. 19-416) 41 ("As a practical matter, Respondents have no ability to sue plantation owners in Ivorian courts. Nor is it clear that the plantation owners—who have profited less from this system of slavery than Petitioner—could satisfy any judgment.").