No. 24-856

IN THE

Supreme Court of the United States

CISCO SYSTEMS, INC., *et al.*,

Petitioners,

v.

DOE I, *et al.*,

Respondents.

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

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF RESPONDENTS

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

Attorneys for Amicus Curiae Electronic Frontier Foundation

389489

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Table of Contents

Table of Contents

TABLE OF CITED AUTHORITIES

Page

Cases

Page

Other Authorities

Cited Authorities

Page

Cited Authorities

Page

Cited Authorities

Cited Authorities

Page

Page

Page

STATEMENT OF INTEREST OF AMICUS CURIAE[1]

Amicus curiae Electronic Frontier Foundation (EFF) has a strong interest in ensuring that the law discourages—and creates real accountability for—American companies that assist foreign governments in violating human rights. EFF is a San Francisco-based, member-supported, nonprofit civil liberties organization that has worked for over 35 years to protect free speech, privacy, security, and innovation in the digital world. With over 30,000 members, and harnessing the talents of lawyers, activists, and technologists, EFF represents the interests of technology users in court cases and broader policy debates regarding the application of law to the internet and other technologies. EFF has participated as *amicus curiae* in several cases focusing on the complicity of American companies in human rights abuses, including the present case in the Ninth Circuit.[2] EFF is also representing a Saudi women's rights activist whose smartphone was hacked by spyware company DarkMatter, which led to her arrest and torture.[3]

---

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.

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

3. *Alhathloul v. DarkMatter Group*, No. 3:21-cv-01787-IM (D. Or.), https://www.eff.org/cases/alhathloul-v-darkmatter-group.

INTRODUCTION AND SUMMARY OF ARGUMENT

This is not a case about a company that merely provided routers or other general-purpose technologies to a foreign government. It is about a company that purposefully and actively assisted in the persecution of a religious group.

Petitioners are accused of working within the United States to develop China's nationwide surveillance system known as the "Golden Shield," that was then used by its customer, the Chinese government, to identify, detain, and torture members of a disfavored religion through a well-documented policy of forced conversion. Cisco not only customized its technology to help identify the targets, who became the victims of these human rights abuses, the communications and information it provided to its customer were specifically used in torture sessions aimed at forcing the victims to renounce their religion.

Sadly, Petitioners' choice to aid and abet torture and other gross human rights abuses by a foreign regime is not unique.[4] There is a growing set of companies—including American companies—that provide surveillance technologies that are vulnerable to, and indeed are being used to, support gross human rights abuses. Because of this, the outcome of this case will have profound

4. *Amici* understand that the Alien Tort Statute (ATS) covers a "narrow set" of international law violations, *Sosa v. Alvarez-Machain*, 542 U.S. 692, 715 (2004) including gross human rights abuses, or "universally condemned behavior" such as "torture, genocide, crimes against humanity, and war crimes," *id.* at 762 (Breyer, J., concurring in part and concurring in the judgment).

implications for millions of people who rely on digital technologies in their everyday lives, including to practice their religion.

While many technologies developed by American companies are beneficial for individuals, including when adopted by governmental customers, some are not. As a longstanding technology-focused organization, *amicus* supports American and international innovation. We applaud the role that American companies, in particular, have played in spreading the benefits of the internet and other technologies around the world. We believe that American-developed technology can be and often has been a force for good.

As a result, we do not believe that American technology companies should be liable for violations of international law under the ATS solely because their technologies ended up in the hands of foreign governments who misused them to violate human rights, or solely because the technologies are being misused in ways that are beyond the ongoing control of the companies.

However, when American technology companies design and develop technologies in the United States to specifically target disfavored groups, and promote and sell or license those technologies abroad to facilitate the persecution of such disfavored groups—and those technologies are in fact used to do so—legal accountability in the United States for the victims of those human rights abuses is appropriate and necessary.

Amicus urges this Court to preserve corporate *aiding and abetting* liability under the ATS to ensure a path to

accountability for American technology companies that actively provide their powerful products and services to foreign governments, which clearly intend to, and do, use them to commit gross human rights abuses. Digital surveillance has become central to the ability of repressive regimes to unlawfully arrest and detain, torture, disappear, and summarily execute victims. And victims of human rights abuses that were enabled by powerful technologies provided by American companies have very few options for redress, which is generally unavailable in the country where they were abused, either against the government or the companies. To ensure that victims of horrific human rights harms have any remedies at all, those victims must have the ability to seek redress from the companies who aided and abetted those harms through civil suits under the ATS.

Amicus supports the arguments of the Plaintiffs-Respondents, and writes to emphasize that the American technology industry's complicity in global human rights abuses is a real and ongoing problem, including in China (Part I); that corporate ATS aiding and abetting liability is supported by the policy underlying the statute (Part II), as well as by United Nations and United States policy on business and human rights (Part III). Preserving the aiding and abetting claim is especially important in light of the fact that U.S. trade policy is often delayed in protecting human rights (Part IV), and the technology industry's voluntary and informal accountability mechanisms are largely ineffective (Part V). The rarely needed yet powerful statutory mechanism that the ATS provides should be available to those grossly harmed with the assistance of American companies.

ARGUMENT

I. THE TECHNOLOGY INDUSTRY PLAYS A MAJOR ROLE IN HUMAN RIGHTS ABUSES WORLDWIDE

In *Jesner v. Arab Bank, PLC*, 584 U.S. 241, 270 (2018) this Court correctly recognized that:

> [N]atural 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.

This concern is especially true for modern technology companies, yet rarely if ever are they going to be principal perpetrators, since they sell or license their technologies to customers who, in turn, use those technologies to violate international law.

Aiding and abetting liability under the ATS is critical because American technology companies provide sophisticated digital surveillance (and censorship) tools to foreign governments that enable those governments to engage in repression in ways that they simply cannot without those surveillance tools, including on a massive scale.

A. Surveillance Companies Facilitate Human Rights Abuses by Governments

As this case and others demonstrate, *see infra* Parts I.B-D., powerful surveillance tools like those developed

by Cisco for the Chinese government are particularly problematic. Not only do they invade digital privacy, which can be a human rights violation itself, they also chill freedom of expression and association,[5] can be used to identify and track religious minorities (as happened here), journalists, and activists, and can facilitate classic human rights abuses including unlawful physical arrest and detention, torture, disappearances, and even summary execution.

There are over 500 private companies that have provided surveillance technologies to governments around the globe,[6] according to Privacy International. When the U.K.-based nonprofit began its research in 2013, it wrote, "In repressive regimes," technology provided by Western companies enables "spying that stifles dissent, has chilling effects across society, and in many cases allows governments to hunt down those it wishes to silence."[7] It further lamented the fact that "members of the private surveillance industry have gained a sense of impunity."[8]

In a scathing 2019 report on the surveillance industry's complicity in human rights abuses by repressive regimes,

---

5. *See* G.A. Res. 217A (III), Universal Declaration of Human Rights, arts. 12 & 19 (Dec. 10, 1948), https://www.un.org/en/about-us/universal-declaration-of-human-rights ("UDHR").

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

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

8. *Id.*

the United Nations Special Rapporteur on Freedom of Opinion and Expression similarly 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."[9] He also stated: "The lack of causes of action and remedies raises serious concerns about the likelihood of holding companies accountable for human rights violations."[10]

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."[11]

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

---

9. 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*, U.N. Human Rights Council 4 (May 28, 2019), https://www.ohchr.org/en/calls-for-input/report-adverse-effect-surveillance-industry-freedom-expression.

10. *Id.* at 12.

11. *Id.* at 3.

and non-State actors use the tools in legitimate ways."[12] 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."[13]

More recently, researchers concluded that litigation is "perhaps the most direct way" for victims of digital surveillance "to obtain access to justice and remedies, as targets can initiate this process independently and tailor the remedy requested," yet substantial legal hurdles exist.[14] This Court should not contribute to this problem by rejecting the ATS aiding and abetting claim.

B. Cisco's Customized Technology Facilitated Human Rights Abuses in China

This Court should keep top of mind what happened to Plaintiffs-Respondents in this case, and the significant and active role that Petitioners played in the human rights abuses they suffered, so as not to lose sight of the reality on the ground.

Plaintiffs are members of a religious minority called the Falun Gong who sued Cisco under the ATS for

---

12. *Id.* (emphasis added).

13. 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.

14. Siena Anstis & Jillian Sprenger, *Civil Society and Access to Justice: Challenges of Seeking Remedy in the Global Fight Against Spyware*, Int'l J. of Human Rights (Jan. 2, 2026), https://doi.org/10.1080/13642987.2025.2603540.

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"—a sophisticated societal surveillance system that includes internet surveillance. Importantly, that system included specific features that enabled the Chinese government to efficiently identify and locate the religious practitioners, who were then subjected to torture, forced conversion, and other human rights abuses.[15] While this case is still at the motion to dismiss phase, there is evidence that Cisco specifically developed its system to facilitate the identification of members of this disfavored religion based upon their viewing and sharing of religious materials. The thirteen Plaintiffs represent themselves and their family members, at least one of whom died by beating while being detained.

As Plaintiffs explain, "[s]ince Chinese engineers did not have the expertise to develop these technologies, the [Communist] Party in concert with Chinese security sought the assistance of Western technology companies, including Cisco…." SAC ¶ 55.[16] The Chinese government did not simply purchase generally available off-the-shelf technology and use it for unlawful purposes. Among other things, Cisco's *customized* system included:

> **a "library of 'signatures,' i.e., carefully analyzed patterns of Falun Gong Internet**

15. *See* UDHR, *supra* note 5, art. 18 ("Everyone has the right to freedom of thought, conscience and religion….").

16. *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 ("SAC").

> **activity to enable the intelligent identification of individual Falun Gong Internet users,"** "real time monitoring" of "Falun Gong Internet traffic patterns and behaviors," and widespread integration of Falun Gong databases "with Cisco security software systems not only to enable the identification and tracking of Falun Gong, but also and specifically to give Chinese security [officers] **access to the sensitive information to facilitate the *zhuanhua* (forced conversion through torture)** of Falun Gong believers."…
>
> One upgrade was the addition of "Ironport," which included a tool **"marketed by Cisco as able to identify Falun Gong online email communication ... to facilitate the identification and apprehension of Falun Gong believers** who typically sent and forwarded pictorial Falun Gong images to others in China." Cisco "actively help[ed] Chinese security forces build a nationwide, **networked video surveillance system**." This system "has been a primary means" of identifying Falun Gong practitioners through non-internet activities, such as protests or religious practice.

Doe I v. Cisco Systems, Inc., 73 F.4th 700, 711 (9th Cir. 2023), *cert. granted,* 2026 WL 73088 (emphasis added). *See also* SAC ¶¶ 75, 80, 85, 97-98, 101.

Once located and detained due to Cisco's surveillance system, Plaintiffs suffered horrific torture. They were beaten with steel rods with sharp screw threads, shocked

with electric batons, forced to endure sleep deprivation and force-feeding, and placed in "reeducation" labor camps, all in attempt to get them to renounce their religion. Plaintiffs' private emails, text messages, and other information—intercepted, collected, and shared by Cisco's Golden Shield with the torture sites—were shown to them and used as part of their torture and forced conversion. SAC ¶¶ 234, 235, 279, 280, 317.

The Ninth Circuit recognized an ATS aiding and abetting claim, and held that Cisco's actions in California, as alleged in the Second Amended Complaint, amounted to "significant technological assistance" to the principal perpetrator, the Chinese government, sufficient to meet the *actus reus* standard and the requirement under *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 124-25 (2013) and *Nestlé USA, Inc. v. Doe*, 593 U.S. 628, 634 (2021) that ATS claims have a sufficient domestic basis. *Doe I*, 73 F.4th at 717, 738-39. The court also held that the company met both "knowledge" and "purpose" *mens rea* standards. *Id.* at 734-35, 735 n.22.

C. Other American Technology Companies Facilitated Human Rights Abuses in China

While Petitioners' assistance was especially significant, other American technology companies have contributed to the global problem of corporate complicity in human rights abuses committed by repressive governments, including in China.

One case was that of Shi Tao, 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.[17] Shi Tao's arrest, along with that of another journalist, was directly enabled by Yahoo!, which shared information from his email account with the Chinese government who used it to identify and arrest him.[18] He and other Chinese dissidents sued Yahoo! under the ATS and other laws in 2007.[19] As part of the settlement of that case, the CEO of Yahoo! apologized to the family members of the detained journalist.[20]

More recently, the Associated Press conducted an in-depth investigation that confirmed that: "Over the past quarter century, American tech companies to a large degree designed and built China's surveillance state, playing a far greater role in enabling human rights abuses than previously known."[21]

---

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

18. 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.

19. *Wang Xiaoning, et al. v. Yahoo! Inc., et al.*, No. 4:07-cv-02151-CW (N.D. Cal.). *See also Yahoo! Lawsuit (re China)*, Business & Human Rights Centre (April 1, 2007), https://www.business-humanrights.org/en/latest-news/yahoo-lawsuit-re-china/.

20. Ewen MacAskill, *Yahoo Forced to Apologise to Chinese Dissidents Over Crackdown on Journalists*, The Guardian (Nov. 14, 2007), https://www.theguardian.com/technology/2007/nov/14/news.yahoo.

21. Dake Kang & Yael Grauer, *Silicon Valley Enabled Brutal Mass Detention and Surveillance in China, Internal Documents*

Companies including Cisco, IBM, Oracle, and Microsoft sold tens of millions of dollars' worth of products to Chinese police to upgrade the Golden Shield.[22] American companies expanded China's capacity for "predictive policing," "enabling Chinese police to preemptively detain people for crimes they have not even committed. Such systems mine a vast array of information—texts, calls, payments, flights, video, DNA swabs, mail deliveries, the internet, even water and power use—to unearth individuals deemed suspicious and predict their movements."[23] Most damningly, *marketing materials* from Cisco, IBM, Dell, and Seagate show that the companies "directly pitched their tech as tools for Chinese police to control citizens."[24]

The Chinese government has a particular interest in suppressing disfavored religious groups—not only Falun Gong practitioners, but also Muslim Uyghurs, Tibetan

---

Show, AP (Sept. 8, 2025), https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-8e000601dadb6aea230f18170ed54e88 ("*Silicon Valley*").

22. *Id.*

23. Dake Kang, *How the AP Uncovered U.S. Big Tech's Role in China's Digital Police State*, AP (Sept. 8, 2025), https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-00bed6421ad8d2ccc6e69f104babe892 ("*Big Tech*").

24. Dake Kang & Yael Grauer, *Takeaways From AP's Investigation Into How U.S. Tech Companies Enabled China's Digital Police State*, AP (Sept. 9, 2025), https://apnews.com/article/chinese-surveillance-silicon-valley-uyghurs-tech-xinjiang-7ddfd2a3260a541fd9ffedddb44e34f4 ("*Takeaways*").

Buddhists, and Christians.[25] Dell "promoted a 'military-grade' AI-powered laptop with 'all-race recognition' on its official WeChat account in 2019."[26] "IBM, Oracle, HP, and ArcGIS developer Esri sold hundreds of thousands of dollars' worth of geographic and mapping software to Chinese police that allows officers to detect when blacklisted Uyghurs, Tibetans or dissidents stray out of provinces or villages."[27] "And until contacted by AP in August [2025], biotech giant Thermo Fisher Scientific's website marketed DNA kits to the Chinese police as 'designed' for the Chinese population, including 'ethnic minorities like Uyghurs and Tibetans.'"[28] Over one million Uighurs have been detained in concentration camps in Xinjiang province since 2017.[29]

---

25. Nick Schifrin & Claire Mufson, *China's Xi Launches Largest Crackdown on Country's Christians in Years*, PBS News (Oct. 25, 2025), https://www.pbs.org/newshour/show/chinas-xi-launches-largest-crackdown-on-countrys-christians-in-years.

26. *Takeaways*, *supra* note 24.

27. *Silicon Valley*, *supra* note 21.

28. *Takeaways*, *supra* note 24. *See also* Sui-Lee Wee, *China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment*, N.Y. Times (June 17, 2020), https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html.

29. Lindsay Maizland, *China's Repression of Uyghurs in Xinjiang*, Council on Foreign Relations (Oct. 3, 2025), https://www.cfr.org/backgrounders/china-xinjiang-uyghurs-muslims-repression-genocide-human-rights.

D. American Technology Companies Facilitated Human Rights Abuses in Other Foreign Countries

While modern technologies may provide extra power to repressive governments, technological facilitation of human rights abuses is not new.

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).[30]

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.[31]

---

30. 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.

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

Repressive regimes in the Middle East used internet surveillance and censorship tools from American technology companies against pro-democracy activists during the Arab Spring.[32] During the Tunisian revolution—the spark of the Arab Spring[33]—the government used technologies from McAfee, Blue Coat Systems, and NetApp.[34] The Syrian government also used Blue Coat Systems and NetApp products.[35] After the U.S. enacted new sanctions in 2011,[36] evidence suggested that Syria was using 34 Blue Coat Systems servers.[37] Narus provided

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

33. Marc Fisher, *In Tunisia, Act of One Fruit Vendor Sparks Wave of Revolution Through Arab World*, Wash. 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.

34. 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/.

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

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

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

Telecom Egypt with internet surveillance and censorship technology that the government used against protestors during the revolution that eventually ousted Egyptian dictator Hosni Mubarak.[38]

The notorious NSO Group[39] facilitates the surreptitious surveillance of journalists, human rights defenders, lawyers, political dissidents, and other members of civil society by licensing its "Pegasus" spyware to governments around the world, including authoritarian regimes.[40] The company was implicated in the government-ordered murder[41] of Saudi dissident and *Washington Post* journalist Jamal Khashoggi in 2018.[42] In 2019, NSO Group hacked into the messaging application WhatsApp, which resulted in more than "100 cases of abusive targeting

38. Ryan Singel, *Lawmaker Calls for Limits on Exporting Net-Spying Tools*, Wired (Feb. 11, 2011), https://www.wired.com/2011/02/narus/.

39. Although based in Israel, NSO Group has undergone multiple changes in ownership and is once again owned by U.S. investors. Lorenzo Franceschi-Bicchierai, *Spyware Maker NSO Group Confirms Acquisition by U.S. Investors*, TechCrunch (Oct. 10, 2025), https://techcrunch.com/2025/10/10/spyware-maker-nso-group-confirms-acquisition-by-us-investors/.

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

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

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

of human rights defenders and journalists in at least 20 countries across the globe."[43] Victims of the WhatsApp hack included Rwandan political dissidents living in exile, who feared that access to their private communications helped the Rwandan government carry out numerous assassinations.[44] The company later adopted a human rights policy in September 2019[45] and a human rights due diligence process in April 2020.[46] Yet human rights abuses continued[47] afterward.[48]

Cyberpoint was involved in Project Raven, a surveillance operation ordered by the government of

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

44. Mehul Srivastava & Tom Wilson, *Inside the WhatsApp Hack: How an Israeli Technology Was Used to Spy*, Fin. Times (Oct. 29, 2019), https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229.

45. *Human Rights Policy*, NSO Group (Sept. 2019), https://www.nsogroup.com/governance/human-rights-policy/.

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

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

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

the United Arab Emirates (UAE) against individuals who criticized the monarchy or insulted the government. "Some days it was hard to swallow, like [when you target] a 16-year-old kid on Twitter," said one American worker.[49]

The government of Belarus used technology from Sandvine to block much of the internet during the disputed presidential election in August 2020.[50] 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 dictator President Alexander Lukashenko.[51]

More recently, *amicus* sent letters to Microsoft, Amazon, and Google regarding contracts with the Israeli government for the companies' AI and cloud computing technologies.[52] We questioned how the companies'

---

49. 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/.

50. Although based in Canada, Sandvine was owned by Francisco Partners and is currently owned by U.S. investors. *Sandvine Announces New Ownership and Capital Infusion*, Sandvine (Sept. 19, 2024), https://www.applogicnetworks.com/press-releases/sandvine-announces-new-ownership-and-capital-infusion.

51. 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.

52. *EFF and Five Human Rights Organizations Urge Action Around Microsoft's Role in Israel's War on Gaza*, EFF Deeplinks (Oct. 13, 2025), https://www.eff.org/deeplinks/2025/10/eff-and-five-

public human rights commitments are consistent with reports that their technologies are being used for mass surveillance and appear to have facilitated various human rights violations, including what a U.N. commission has called a genocide in Gaza.[53] Other companies including Cisco, Palantir, Starlink, and OpenAI have also been implicated in Israel's war in Gaza.[54]

While every situation mentioned above would not create liability under an aiding and abetting claim given the high and careful standards of the ATS, these examples show that the situation is serious and that removing the possibility of corporate accomplice liability will only further contribute to the ongoing problem of American technology companies contributing to human rights abuses around the world.

The high standards of the ATS also demonstrate the incorrectness of Cisco's hyperbolic statement that

---

human-rights-organizations-urge-action-around-microsofts-role-israels; Betty Gedlu & Cindy Cohn, *Amazon and Google Must Keep Their Promises on Project Nimbus*, EFF Deeplinks (Dec. 2, 2024), https://www.eff.org/deeplinks/2024/12/amazon-and-google-must-keep-their-promises-project-nimbus.

53. *Israel Has Committed Genocide in the Gaza Strip, U.N. Commission Finds*, U.N. Human Rights Office of the High Commissioner (Sept. 16, 2025), https://www.ohchr.org/en/press-releases/2025/09/israel-has-committed-genocide-gaza-strip-un-commission-finds.

54. *Big Tech Companies Face Allegations of War Crimes Complicity Amid Israel's War in Gaza*, Business & Human Rights Centre (May 5, 2025), https://www.business-humanrights.org/en/latest-news/big-tech-companies-allegedly-complicit-in-war-crimes-amid-israels-war-in-gaza-incl-company-responses/ ("*Allegations*").

"ordinary commercial activity … conducted with improper intent" will be subject to a "new wave of ATS litigation." Pet. Br. 33. Of course, there is nothing "ordinary" about what Cisco did here—purposefully customizing surveillance tools for a customer government to violently target a religious minority. But any ATS aiding and abetting claim will have to pass the significant hurdles of the "touch and concern" requirement under *Kiobel*, 569 U.S. at 124-25, and *Nestlé*, 593 U.S. at 634 (holding insufficient U.S.-based "general corporate activity" and "operational decisions" related to the foreign business); and the standard tort elements of *mens rea* (whether "knowledge" or "purpose")[55] and *actus reus*, among others. *See Doe I*, 73 F.4th at 724.

Thus, there is no danger of opening the floodgates of ATS litigation. Moreover, contrary to Petitioners' assertion, when American companies choose to put profit over fundamental human well-being, any reputational harm that flows to them is the companies' own doing, and not that of ATS aiding and abetting litigation. Pet. Br. 39.

But the fact that American technology has been and is currently being widely used by repressive governments abroad reinforces the need to preserve the outer limits of liability that the ATS aiding and abetting claim provides. Removing this critical legal disincentive and avenue for redress will be read as a green light for American

55. 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.

companies to provide even more technological assistance that will result in more human rights abuses by their governmental customers.

II. ATS POLICY SUPPORTS PRESERVING U.S. CORPORATE AIDING AND ABETTING LIABILITY UNDER THE STATUTE

A. Applying the ATS to Corporations Will Be Meaningless Without the Aiding and Abetting Claim

In *Nestlé*, five justices of this Court (Sotomayor, Breyer, Kagan, Gorsuch, Alito) agreed that the ATS *should* apply to U.S. corporations. As Justice Gorsuch said, "Nothing in the ATS supplies corporations with special protections against suit. … Generally, [] the law places corporations and individuals on equal footing when it comes to assigning rights and duties." *Nestlé*, 593 U.S. at 641 (Gorsuch, J., concurring).

Yet preserving U.S. corporate liability under the ATS but *not also aiding and abetting* liability would essentially eliminate corporate liability, particularly as it relates to American technology companies. As noted above, American companies often provide the technologies that make it ruthlessly efficient for repressive regimes to violate the human rights of religious and other disfavored groups. Without the possibility of an aiding and abetting claim, U.S. corporations that help foreign governments violate human rights will operate with impunity. *See supra* Part I.

B. The Foreign Policy Goals of the ATS Are Supported By the Aiding and Abetting Claim

Preserving U.S. corporate aiding and abetting liability under the ATS 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*, 542 U.S. at 715. 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."[56] 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*, 584 U.S. at 255.

It is wholly appropriate, and consistent with U.S. interests, for U.S. courts to exercise jurisdiction over U.S. corporations under the ATS, for what they did *domestically* (per *Kiobel* and *Nestlé*) to contribute to human rights abuses abroad. *See Sosa*, 542 U.S. at 761 (Breyer, J., concurring in part and concurring in the judgment) ("[C]omity concerns normally do not arise (or at least are mitigated) if the conduct in question takes place

56. Stephen Mulligan, *The Alien Tort Statute (ATS): A Primer*, Cong. Research Service (Jan. 11, 2022), https://www.congress.gov/crs-product/R44947.

in the country that provides the cause of action or if that conduct involves that country's own national."). Allowing foreign plaintiffs to hold American companies accountable for actions that have a sufficient domestic basis but also aid and abet human rights violations abroad may actually "promote harmony in international relations." *See Jesner*, 584 U.S. at 270. 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 320 (Sotomayor, J., dissenting). And as Respondents argue, ATS aiding and abetting liability "helps reduce friction in America's foreign relations by ensuring the United States fulfills its international obligations." Resp. Br. 27.

In an attempt to sow fear for step two of the *Sosa* analysis (which evaluates foreign policy implications when considering new causes of actions under the ATS, *see Sosa*, 542 U.S. at 727-28; *Jesner*, 584 U.S. at 258), Cisco argues that sustaining the ATS aiding and abetting claim creates "the most extreme form of diplomatic friction" because it requires a U.S. "court to establish a primary violation of international law by a foreign state exercising sovereign authority as to its own people within its territory." Pet. Br. 15, 17. But foreign governments do not have the "sovereign authority" to torture or otherwise perpetrate the narrow slice of human rights abuses that have been recognized

as falling under the ATS. It should not be diplomatically controversial for a U.S. court to declare as much, and to hold a corporate accomplice responsible for its part in such human rights abuses.

Cisco also argues that, "[b]y bringing aiding and abetting claims against the private associates of those foreign actors, plaintiffs can evade the limitations of sovereign immunity." Pet. Br. 33. Cisco seems to suggest that foreign victims of human rights abuses should *only* sue the governments that were the principal perpetrators of those abuses. But as Cisco well knows, victims are unlikely to be able to sue their own governments in their home countries, and such suits brought in U.S. courts would almost certainly be blocked by foreign sovereign immunity. *See, e.g.*, *Kidane v. Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017). And, in many cases, the company would not be subject to suit in the foreign country either. In short, Cisco seeks to have this Court send Plaintiffs down a dead-end street. Even if some such litigation avenues could theoretically be available, Plaintiffs should not be so limited—all avenues of justice should be available to those whose most fundamental rights have been violated, including suing American corporate accomplices in U.S. courts.

When it comes to technology, governments can rarely build sophisticated technology solutions on their own, whether for mass surveillance or other purposes. They need the help of the private sector—and if the standards of aiding and abetting are met, the private sector should be held accountable for its role in subsequent human rights abuses. In other contexts, corporate technology defendants are fair game—and

it is irrelevant that their government customers would have foreign sovereign immunity in U.S. courts if sued directly. *WhatsApp Inc. v. NSO Group Technologies Ltd.*, 17 F.4th 930, 940 (9th Cir. 2021), *cert. denied*, 143 S.Ct. 562.

III. UNITED NATIONS AND UNITED STATES POLICY ON BUSINESS AND HUMAN RIGHTS SUPPORTS ALLOWING CORPORATE AIDING AND ABETTING LIABLITY UNDER THE ATS

Preserving the aiding and abetting claim under the ATS is consistent with settled United Nations policy on business and human rights. The concept of "business and human rights," as a subset of corporate social responsibility, is over 30 years old.[57] It took a powerful step forward with the 2008 report written by the United Nations Special Representative on Business and Human Rights, John Ruggie, known as the Ruggie Report.[58]

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**

57. 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. *Our Story*, Business for Social Responsibility, https://www.bsr.org/en/about/story; *Focus Areas*, Business for Social Responsibility, https://www.bsr.org/en/expertise.

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

for more effective access to remedies."[59] The Ruggie Report emphasized that the governmental duty to protect and the corporate responsibility to respect human rights are distinct (albeit intertwined) obligations.[60]

The 2008 Ruggie Report led to the 2011 publication of the United Nations *Guiding Principles on Business and Human Rights*, which adopted and sought to operationalize the Ruggie Report framework.[61] The *Guiding Principles* provide that national governments should "take steps to prevent abuse abroad by business enterprises within their jurisdiction"[62] and "to ensure the effectiveness of domestic judicial mechanisms when addressing business-related human rights abuses."[63] 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."[64] 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."[65]

---

59. *Id.* at 4 (emphasis added).

60. *Id.* at 17.

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

62. *Id.* at 4.

63. *Id.* at 28.

64. *Id.* at 29.

65. *Id.*

In 2020, the first Trump Administration endorsed the *Guiding Principles* as they specifically apply to U.S. companies that provide digital surveillance technologies to foreign governments.[66] In 2021, the Biden Administration launched a multilateral effort "to help stem the tide of authoritarian government misuse of technology and promote a positive vision for technologies anchored by democratic values."[67] In 2022, the Biden Administration published a National Security Strategy that included the commitment to combat the "illegitimate use of technology, including commercial spyware and surveillance technology" and to "stand against digital authoritarianism."[68]

---

66. *U.S. Department of State Guidance on Implementing the "UN Guiding Principles" for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities*, U.S. State Dept. (Sept. 30, 2020) (2017-2021 archive), https://2017-2021.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/

67. *Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy*, White House (Dec. 10, 2021), https://web.archive.org/web/20211211105848/https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/. *See also Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy*, U.S. State Dept. (March 30, 2023) (2021-2025 archive), https://2021-2025.state.gov/export-controls-and-human-rights-initiative-code-of-conduct-released-at-the-summit-for-democracy/.

68. *National Security Strategy*, White House 33 (Oct. 12, 2022), https://web.archive.org/web/20221012160318/https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

This Court should not facilitate "the avoidance of appropriate accountability."[69] Ensuring that companies like Cisco cannot avoid accountability is consistent with the United Nations' and United States' goals of stemming the tide of governmental human rights abuses facilitated by private technology companies. While U.N. and U.S. policies are important, they are not sufficient—human rights victims deserve access to the courthouse.

IV. DELAYED U.S. TRADE POLICY INSUFFICIENTLY PROTECTS HUMAN RIGHTS

Cisco consistently argues that it has been in compliance with U.S. export controls. Pet. Br. 38.[70] However, trade policy does not always focus on human rights, and even when it does, it generally lags behind the reality on the ground, only changing after victims have already suffered human rights harms.

As Respondents point out, there is no evidence that Congress back in the 1990s and early 2000s could have anticipated the internet surveillance technologies at issue in this case. Resp. Br. 29. Similarly, it was not until 2021 that the Biden Administration began addressing the global spyware problem and, in particular, the notorious company NSO Group. The government put the company

---

69. *Guiding Principles*, *supra* note 61, at 29.

70. *See also Silicon Valley*, *supra* note 21 ("IBM, Dell, Cisco, Intel, Thermo Fisher and Amazon Web Services all said they adhere to export control policies.").

on the Entity List,[71] which was years after disturbing reports of NSO Group's role in government repression. *See supra* Part I.D.

V. VOLUNTARY AND INFORMAL MECHANISMS FOR HOLDING THE TECHNOLOGY INDUSTRY ACCOUNTABLE FOR HUMAN RIGHTS ABUSES ARE INADEQUATE

It is especially important that this Court give victims of human rights abuses like the Falun Gong practitioners here a fighting chance in U.S. courts given that voluntary and informal mechanisms for holding technology companies accountable for their roles in human rights abuses have proven inadequate to prevent such abuses and to provide redress to victims.

A. Voluntary Corporate Human Rights Policies Insufficiently Protect Human Rights

The Ruggie Report recognized that "companies can affect virtually all internationally recognized rights."[72] The report even used a technology example to illustrate the potential breadth of a company's impact on human rights: "violations of privacy rights by Internet service providers can endanger dispersed end-users."[73]

---

71. Drew Harwell et al., *Biden Administration Blacklists NSO Group Over Pegasus Spyware*, Wash. Post (Nov. 3, 2021), https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/.

72. Ruggie, *supra* note 58, at 9.

73. *Id.* at 20.

The Ruggie Report argued that companies, therefore, must practice "due diligence," which involves taking steps "to become aware of, prevent and address adverse human rights impacts."[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 as with business partners, suppliers, State agencies, and other non-State actors."[76] The UN's *Guiding Principles* similarly provide that companies should "[a]void 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]

---

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 York, *"Know Your Customer" Standards for Sales of Surveillance Equipment*, EFF Deeplinks (Oct. 24, 2011), https://www.eff.org/tr/deeplinks/2011/10/its-time-know-your-customer-standards-sales-surveillance-equipment?language=tr; Cindy Cohn, *Should Your Company Help ICE? "Know Your Customer" Standards for Evaluating Domestic Sales of Surveillance Equipment*, EFF Deeplinks (July 13, 2018), https://www.eff.org/deeplinks/2018/07/should-your-company-help-ice-know-your-customer-standards-evaluating-domestic.

76. Ruggie, *supra* note 58, at 17.

77. *Guiding Principles*, *supra* note 61, at 14-15.

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 contemplated, however, that voluntary mechanisms would play a significant role in corporate accountability for human rights violations.[79]

Unfortunately, the weakness of voluntary enforcement is evidenced by the fact that not all companies have human rights policies and due diligence processes, and governmental abuses continue even when companies do have them. *See supra* Part I.D. The ATS must remain a viable avenue of justice for those victimized by repressive governments and the American technology companies that aid and abet those governments, given the insufficiency of companies' voluntary human rights policies.

Here, Petitioners are not simply challenging the conclusion that Plaintiffs' factual allegations about the company meet the legal standards—they are attacking the ATS aiding and abetting claim itself. Cisco's position in this appeal not only evidences the company's desire to fiercely fight any accountability for itself, it carries the water for other American companies that also wish to avoid human rights accountability.

This is a bold position to take for a company that purports to care about human rights. Cisco first published

78. *Id.* at 1.

79. Ruggie, *supra* note 58, at 26. *See also Guiding Principles*, *supra* note 61, at 28, 31.

its Global Human Rights Policy in 2012, a year after this case was filed in 2011.[80] Since then, the company has never provided redress for what its customized Falun Gong features of the Golden Shield caused plaintiffs to suffer, despite stating:

> Where we have identified that we have caused or contributed to an adverse human rights impact, we are committed to providing access to and cooperating in remediation for affected individuals, workers, and communities through legitimate processes.[81]

To the extent Cisco has a human rights "framework to assess and mitigate known risks," there is a question whether this is meaningful given that Cisco helped to upgrade the Golden Shield and that contracts to maintain its systems exist,[82] and more recently the company has been called out for its role in what the U.N. deemed a genocide in Gaza.[83]

---

80. Dev Stahlkopf, *Cisco's Commitment to Human Rights: A Tribute to the 75th Anniversary of the Universal Declaration of Human Rights*, Cisco (Dec. 20, 2023), https://blogs.cisco.com/news/ciscos-commitment-to-human-rights-a-tribute-to-the-75th-anniversary-of-the-universal-declaration-of-human-rights.

81. *Global Human Rights Policy*, Cisco (Aug. 14, 2025), https://www.cisco.com/c/dam/assets/csr/pdf/Human-Rights-Policy.pdf.

82. *Silicon Valley*, *supra* note 21.

83. *Allegations*, *supra* note 54.

B. Informal Corporate Human Rights Accountability Mechanisms Are Weak

The Organization for Economic Cooperation & Development (OECD)[84] wrote the *Guidelines for Multinational Enterprises on Responsible Business Conduct* "to encourage positive contributions enterprises can make to economic, environmental and social progress, and to minimise adverse impacts … that may be associated with an enterprise's operations, products and services."[85]

The accountability mechanism for the OECD *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*.[86] Specific Instances can lead to mediation between the complainant and the company.[87] The National Contact Point for the

---

84. The OECD is an international organization funded by member countries. *Budget*, OECD https://www.oecd.org/about/budget/.

85. *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct*, OECD (June 8, 2023), https://www.oecd.org/en/publications/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_81f92357-en.html.

86. *National Contact Points for Responsible Business Conduct*, OECD, https://www.oecd.org/en/networks/national-contact-points-for-responsible-business-conduct.html.

87. *FAQ on the NCP Grievance Mechanism; How Do NCP Handle Cases?*, OECD, https://www.oecd.org/content/dam/oecd/en/networks/national-contact-points/FAQ-NCP-grievance-mechanism.pdf.

United States is housed at the State Department.[88] The key shortcomings of the NCP/Specific Instance system are two-fold.[89] 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,[90] with only one relating to the telecommunications industry (regarding labor practices).[91] Second and more fundamentally, "the OECD Guidelines are non-binding on businesses and engagement in a Specific Instance process is voluntary."[92]

This latter shortcoming was on full display in the United Kingdom, providing a stark example for the technology industry. Privacy International filed a complaint with the U.K.'s NCP alleging that Gamma International U.K. Ltd.:

---

88. *U.S. National Contact Point for the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct*, U.S. State Dept., https://www.state.gov/bureau-of-economic-and-business-affairs/u-s-national-contact-point-for-the-oecd-guidelines-for-multinational-enterprises.

89. *Specific Instance Process*, U.S. State Dept. (2009-2017 archive), https://www.state.gov/u-s-national-contact-point-for-the-oecd-guidelines-for-multinational-enterprises/specific-instance-process/.

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

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

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

> 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.[93]

After initially responding to Privacy International's complaint, Gamma went silent. The U.K. 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.[94] 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

93. *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.*, U.K. National Contact Point 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.

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

> under the OECD Guidelines. The UK NCP regrets Gamma's failure to engage.[95]

Similarly, the U.K.-based nonprofit Business & Human Rights Centre collects human rights complaints against companies and solicits company responses. Companies can choose to ignore the complaints—the response rate averages 43 percent—and even if they do respond, there is no guarantee they will change their practices.[96]

CONCLUSION

This Court must not shut the courthouse door to victims of human rights abuses that are actively powered by American corporations. In the digital age, repressive governments rarely act alone to violate human rights. They have 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."[97]

---

95. *Follow Up Statement After Recommendations in Complaint From Privacy International Against Gamma International*, U.K. National Contact Point 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.

96. *Company Response Mechanism*, Business & Human Rights Centre, https://www.business-humanrights.org/en/from-us/company-response-mechanism/.

97. Kaye, *supra* note 9, at 6.

Technology has the capacity to protect human rights, but it also can make violations ruthlessly efficient. We urge this Court to preserve U.S. corporate aiding and abetting liability under the ATS, to allow a narrow slice of foreign plaintiffs to hold American technology companies accountable for their active complicity in human rights abuses by repressive governments. This is important when the U.S. judicial system may be the only available forum for redress, and the lack of any other meaningful accountability mechanisms for American companies may cause or heighten international tensions. Maintaining the aiding and abetting claim under the ATS thus not only protects human rights victims, but also broader U.S. international interests. It also helps ensure that American technological genius supports, rather than undermines, human rights and the rule of law.

Respectfully submitted,

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

Attorneys for Amicus Curiae
Electronic Frontier Foundation

Dated: March 27, 2026