UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No. 1:20-civ-25022-KMM

GHADA OUEISS,

Plaintiff,

v.

MOHAMMED BIN SALMAN BIN ABDULAZIZ AL SAUD, MOHAMMED BIN ZAYED AL NAHYAN, DARKMATTER, FAISAL AL BANNAI, SAUDI 24 TV, A BROADCAST TELEVISION STATION OWNED BY THE KINGDOM OF SAUDI ARABIA, AL ARABIYA, A BROADCAST TELEVISION STATION OWNED BY THE KINGDOM OF SAUDI ARABIA, PRINCE MOHAMMED BIN SALMAN ABDULAZIZ FOUNDATION D/B/A MISK FOUNDATION, SAUD AL QAHTANI BADER AL-ASAKER, SAUDI ARABIAN CULTURAL MISSION, TEREK ABOU ZEINAB, TURKI AL-OWERDE, FAISAL AL MENAIA, AWWAD AL OTAIBI, SHARON COLLINS, CHRISTANNE SCHEY, HUSSAM AL-JUNDI, ANNETTE SMITH, JOHN DOES 1-20,

Defendants.

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFF AGAINST DEFENDANT DARKMATTER'S MOTION TO DISMISS

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

Rules

INTEREST OF AMICUS CURIAE[1]

Amicus curiae Electronic Frontier Foundation (EFF) has a strong interest in ensuring that the law provides accountability for corporations that assist foreign governments in violating human rights. EFF is a San Francisco-based, member-supported, nonprofit civil liberties organization that has worked for over 30 years to protect free speech, privacy, security, and innovation in the digital world. With over 38,000 members, and harnessing the talents of lawyers, activists, and technologists, EFF represents the interests of technology users in court cases and policy debates regarding the application of law to the Internet and other technologies. EFF has led investigations into misuse of surveillance technologies by governments to target citizens for human rights abuses,[2] and filed *amicus* briefs in cases focusing on the complicity of corporations, including technology companies, in human rights abuses.[3]

---

[1] No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than the *amicus curiae* or their counsel made a monetary contribution intended to fund the brief's preparation or submission.

[2] EFF, *Surveillance Technologies*, https://www.eff.org/issues/mass-surveillance-technologies; Lookout & EFF, *Dark Caracal: Cyber-Espionage at a Global Scale*, at 3-4 (2018), https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf; Cooper Quintin & Eva Galperin, *Dark Caracal: You Missed a Spot*, Deeplinks (Dec. 10, 2020), https://www.eff.org/deeplinks/2020/12/dark-caracal-you-missed-spot.

[3] EFF *amicus* brief (Oct. 21, 2020), *Nestlé USA, Inc. v. Doe I*, No. 19-416 (U.S.), https://www.supremecourt.gov/DocketPDF/19/19-416/158434/20201021172033931_19-416%20and%2019-453%20Brief.pdf; ECF 41 (Dec. 21, 2020), *WhatsApp v. NSO Group*, No. 20-16408 (9th Cir.), https://www.eff.org/document/eff-amicus-brief-whatsapp-v-nso-group-9th-cir; ECF 15-2 (Jan. 11, 2016) (EFF's most recent *amicus* brief), *Doe I v. Cisco Systems, Inc.*, No. 15-16909 (9th Cir.), https://www.eff.org/document/eff-article-19-privacy-international-9th-circuit-amicus-brief; ECF 57 (Feb. 11, 2015), *Balintulo v. Ford Motor Co.*, No. 14- 4104-cv (2d Cir.), https://www.eff.org/document/eff-amicus-brief-ibm-ats-claim.

INTRODUCTION AND SUMMARY OF ARGUMENT

This case is not just a dispute between a journalist and her political opponents. The outcome of this case will have profound implications for millions of Internet users and other citizens of countries around the world. While many technologies developed, licensed, and sold by both foreign and domestic corporations are tremendously useful to law-abiding customers, other technologies—or sometimes even the same technologies when deployed by repressive regimes—can facilitate human rights abuses.

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

Accordingly, *amicus* urges this Court to *deny* Defendant DarkMatter any form of foreign sovereign immunity, whether conduct-based immunity or status-based immunity under federal common law, or derivative foreign sovereign immunity under the Foreign Sovereign Immunities Act. *Cf.* Def. DarkMatter MTD Br., ECF 165, 17-19. In so doing, *amicus* also urges this Court to craft a rule that denies foreign sovereign immunity to all private companies, especially those that facilitate violations of human rights. *See* Pl. MTD Op. Br., ECF 172, 18-26.

It is critical to hold *all* technology companies accountable when they provide their products and services to foreign governments that use them to commit human rights abuses. Unlawful digital surveillance invades victims' privacy and chills their freedom of speech and association, and often leads to unlawful arrest and detention, torture, disappearances, and summary execution. Victims of human rights abuses enabled by powerful technologies—such as Ms. Oueiss, Plaintiff here—must have the ability to seek redress through civil suits in U.S. courts against both foreign and domestic corporations.

Amicus supports the arguments of Plaintiff against granting foreign sovereign immunity to DarkMatter and writes to emphasize that this is appropriate in light of the fact that corporate complicity in human rights abuses is a widespread and ongoing problem. DarkMatter has a long history of assisting foreign governments in targeting civil society and violating the human rights of their citizens, as a major player in an unscrupulous international cybersurveillance market that American technology companies also participate in (Part I). Denial of immunity here is also supported by the United Nations' policy on business and human rights (Part II), and by the fact that the technology industry's voluntary accountability mechanisms have been largely ineffective (Part III). This Court should not expand the ability of technology companies like DarkMatter to avoid accountability for facilitating human rights abuses by foreign governments.

ARGUMENT

I. Foreign Sovereign Immunity Should Be Denied to Technology Companies, Which Play a Major Role in Human Rights Abuses Worldwide

This Court should not grant DarkMatter or any corporation foreign sovereign immunity, so that Plaintiff and human rights victims broadly have a fighting chance to hold technology companies accountable for their complicity in the abuses perpetrated by foreign

governments. As the Supreme Court has recognized, corporations can be just as culpable as the individuals who comprise them:

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

Jesner v. Arab Bank, PLC, 138 S. Ct. 1386, 1406 (2018). And just this summer, a majority of Supreme Court justices agreed that the ATS should apply to U.S. companies (not just natural persons) and that federal courts may continue to recognize new causes of action for violations of modern conceptions of human rights. *Nestlé USA, Inc. v. Doe I*, 141 S. Ct. 1931, 1941, 1944 (2021) (Gorsuch, J., concurring) (Sotomayor, J., concurring in part and concurring in the judgment).

The need for accountability is particularly acute for modern technology companies that provide sophisticated surveillance and censorship products and services to foreign governments, enabling those governments to engage in repression on a massive scale. As numerous cases demonstrate, *see infra* Parts I.B. & I.C., powerful digital surveillance tools like those deployed by DarkMatter are used to identify and track journalists, democracy and human rights activists, and religious minorities. These tools not only invade digital privacy and compromise freedom of speech and association, they can also facilitate physical apprehension, unlawful detention, torture, disappearances, and even summary execution.

A. Surveillance Companies Facilitate Human Rights Abuses by Foreign Governments

There are at least 500 private companies that have provided internet and digital

surveillance technologies to governments around the globe,[4] compiled in the *Surveillance Industry Index* by the UK-based nonprofit organization Privacy International.[5] These companies reflect a market value of about $12 billion annually.[6] When Privacy International launched the *Index*, 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."[7] It further lamented the fact that "members of the private surveillance industry have gained a sense of impunity."[8]

Cybersurveillance companies have many willing customers, including at least 45 of the 70 countries that are home to 88% of the world's internet users, according to Freedom House.[9] These countries are suspected of using "sophisticated spyware or data-extractive technology" from companies like NSO Group, Cellebrite, Circles, and FinFisher.[10] The report discusses case studies of governments targeting journalists and activists with these technologies, including that of Ms. Oueiss here.[11] As the authors concluded, "Limited regulation of the sale and purchase of these tools, coupled with their near ubiquity and low

---

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

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

[6] Ryan Gallagher, *Silicon Valley Investment Firm Profits From Surveillance States*, Bloomberg Businessweek (Jan. 26, 2021), https://www.bloomberg.com/news/features/2021-01-26/private-equity-firm-francisco-partners-profits-from-surveillance-censorship.

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

[8] *Id*.

[9] Freedom House, *Freedom of the Net 2021: The Global Drive to Control Big Tech* (2021), at 4, 9, https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

[10] *Id.* at 9.

[11] *Id*.

cost in practice, has created a crisis for human rights."[12]

In a scathing 2019 report on the cybersurveillance industry's complicity in human rights abuses by repressive regimes, the United Nations Special Rapporteur on Freedom of Opinion and Expression explained that "[d]igital surveillance is no longer the preserve of countries that enjoy the resources to conduct mass and targeted surveillance based on in-house tools. Private industry has stepped in, unsupervised and with something close toimpunity."[13]

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."[14] He rightly asserted: "The lack of causes of action and remedies raises serious concerns about the likelihood of holding companies accountable for human rights violations."[15]

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."[16] In an op-ed, he rejected the notion that it is "complicated" to protect privacy and

---

[12] *Id*.

[13] David Kaye, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, United Nations Human Rights Council, at 4 (May 28, 2019), https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx.

[14] *Id.* at 3.

[15] *Id.* at 12.

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

human rights: "All I can say is, give me a break."[17]

B. DarkMatter is Notorious for Carrying Out Human Rights Abuses for Foreign Governments

DarkMatter surreptitiously surveils journalists, political dissidents, and other members of civil society, violating privacy rights and often leading to more serious human rights abuses. As cited by Plaintiff, Reuters has reported extensively on how DarkMatter's "Raven" team conducted digital hacking and spying operations in the U.A.E. and other countries for years—and even targeted U.S. citizens. *See* Am. Compl., ECF 135, ¶ 76.[18] This spying has led to detention and torture. In 2017, DarkMatter targeted Loujain al-Hathloul for surveillance, a Saudi women's rights activist.[19] The following year, the U.A.E. unlawfully arrested and deported her to Saudi Arabia, where the allied government imprisoned and tortured her.[20]

DarkMatter is a major player in the global cybersurveillance market and collaborates with fellow unscrupulous foreign and U.S. companies and individuals against foreign and U.S. targets. DarkMatter poached American former intelligence officers to develop its hacking and surveillance programs.[21] As DarkMatter employees, those Americans then bought sophisticated "zero-click" digital exploits from U.S. companies to hack users of Apple's

---

[17] 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.

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

[19] Joel Schectman & Christopher Bing, *White House Veterans Helped Gulf Monarchy Build Secret Surveillance Unit*, Reuters (Dec. 10, 2019), https://www.reuters.com/investigates/special-report/usa-raven-whitehouse/.

[20] *Id*.

[21] Schectman & Bing, *supra* n.18.

iPhone.[22] American company Accuvant developed and sold a hacking tool to DarkMatter,[23] which further modified it such that the tool had the capability of accessing tens of millions of Apple devices, and when deployed had a 90-95% success rate.[24]

Similarly, as alleged by Plaintiff, DarkMatter bought and used "Pegasus" spyware from NSO Group. Am. Compl., ECF 135, ¶ 152. NSO Group and foreign governments have used Pegasus to target the mobile devices of people and companies around the world, including in the U.S.[25] For example, WhatsApp discovered that NSO Group breached its systems using Pegasus in April and May 2019 and targeted approximately 1,400 WhatsApp users.[26] Citizen Lab[27] conducted research on the WhatsApp hack and uncovered more than "100 cases of abusive targeting of human rights defenders and journalists in at least 20 countries across the globe."[28] These happened just weeks *after* NSO Group's new owners

---

[22] Joel Schectman & Christopher Bing, *UAE Used Cyber Super-Weapon to Spy on iPhones of Foes*, Reuters (Jan. 30, 2019) (stating that "Karma [spyware] did not require a target to click on a link sent to an iPhone"), https://www.reuters.com/investigates/special-report/usa-spying-karma/.

[23] Patrick H. O'Neill, *This US Company Sold iPhone Hacking Tools to UAE Spies*, MIT Technology Review (Sept. 15, 2021), https://www.technologyreview.com/2021/09/15/1035813/us-sold-iphone-exploit-uae/.

[24] Deferred Prosecution Agreement (DPA), Ex. A, Factual Statement (Sept. 14, 2021), ¶¶ 46, 49, 51, 56-57, *United States v. Marc Baier, et al*., No. 21-CR-577 (D.D.C.), https://www.justice.gov/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million.

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

[26] Compl., ECF 1 (Oct. 29, 2019), ¶ 42, *WhatsApp v. NSO Group*, No. 4:19-cv-07123-PJH (N.D. Cal.), https://www.washingtonpost.com/context/read-the-whatsapp-complaint-against-nso-group/abc0fb24-8090-447f-8493-1e05b2fc1156/?itid=lk_inline_manual_4; *appeal pending*, No. 20-16408 (9th Cir.).

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

[28] 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/.

asserted that the company "already operates under an ethical governance framework that is significantly more robust than any of its peers."[29] Victims of the WhatsApp hack included, among others, Rwandan political dissidents living in exile, who fear that access to their private communications helped the Rwandan government carry out numerous assassinations.[30]

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

Far beyond helping DarkMatter and its government clients, American technology companies have assisted numerous repressive regimes in human rights abuses. In rejecting DarkMatter's bid for foreign sovereign immunity, *amicus* urges this Court not to leave open the door for any private corporation—whether foreign or domestic—to benefit from foreign sovereign immunity, especially those that put profits over fundamental human rights.

In a case currently set for oral argument before the Ninth Circuit, 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

---

[29] Stephen Peel, *Response to Open Letter to Novalpina Capital on 18 February 2019*, Novalpina (March 1, 2019), https://web.archive.org/web/20200805082629/https://www.novalpina.pe/response-to-open-letter-1/. *See also infra* n.77-78. Novalpina Capital has since dissolved. Mark Kleinman, *Pegasus Spyware Owner Novalpina to Be Liquidated After Failure to Resolve Internal Bust-Up*, Sky News (July 27, 2021), https://news.sky.com/story/pegasus-spyware-owner-novalpina-to-be-liquidated-after-failure-to-resolve-internal-bust-up-12365638.

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

subjected to torture, forced conversion, and other human rights abuses.[31]

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.[32] 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.[33] He and other Chinese dissidents sued Yahoo! under the ATS and other laws in 2007, but the parties settled the case later that year.[34] More recently, Ning Xianhua, a pro-democracy activist from China, sued the successor companies, founder, and former CEO of Yahoo! under the ATS for sharing his private emails with the Chinese government, which led to his arrest, imprisonment, and torture.[35]

Victims of South Africa's apartheid sued IBM under the ATS for aiding and abetting the human rights abuses they suffered at the hands of the government. The Second Circuit considered the plaintiffs' allegation that IBM created a customized computer-based national identification system that facilitated the "denationalization" of country's Black population,

---

[31] *Doe I v. Cisco Systems, Inc.*, No. 15-16909 (9th Cir.). *See also* Sec. Am. Compl., ECF 113 (Sept. 18, 2013), *Doe I v. Cisco Systems, Inc.*, No. 5:11-cv-02449-EJD (N.D. Cal.), https://www.eff.org/document/plaintiffs-second-amended-complaint-0.

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

[33] 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.

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

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

and concludedthat that the "touch and concern" requirement per *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1669 (2013) had been met. *Balintulo v. Ford Motor Co.,* 796 F.3d 160, 169 (2d Cir. 2015).[36] 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 punchcard 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.[37]

Repressive regimes in the Middle East used Internet surveillance and censorship tools from American technology companies against pro-democracy activists during the Arab Spring.[38] During the 2011 Tunisian revolution—the spark of the Arab Spring[39]—the government used technologies from McAfee, Blue Coat Systems,[40] and NetApp.[41] The Syrian

---

[36] The Second Circuit ultimately rejected the 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/.

[37] Edwin Black, *IBM and the Holocaust: Expanded Edition*, at 352 (Dialog Press 2012).

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

[39] 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-arabworld/2011/03/16/AFjfsueB_story.html.

[40] 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.

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

government also used Blue Coat Systems and NetApp products.[42] After the U.S. enacted sanctions in 2011,[43] evidence suggested that Syria was using 34 Blue Coat Systems servers.[44] Narus[45] provided Telecom Egypt with Internet surveillance and censorship technology that the government used against protestors during the revolution that eventually ousted longtime Egyptian dictator Hosni Mubarak.[46]

The government of Belarus used technology from Sandvine to block much of the Internet during the disputed presidential election last year. The company's technology "played a central role in censoring social media, news and messaging platforms used by protesters rallying against" the reelection of longtime dictator President Alexander Lukashenko.[47] Congress is looking into whether the company violated U.S. sanctions against Belarus.[48] 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

---

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

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

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

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

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

[47] 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.

[48] *Id*.

rights, and news content.[49] In 2018, the company's "business ethics committee" had decided to exclude questions about internet censorship from customer ethics reviews.[50]

CyberPoint was involved in the "Raven" surveillance operation in U.A.E. that, as described above, DarkMatter eventually took over. "Some days it was hard to swallow, like [when you target] a 16-year-old kid on Twitter," said one American contractor.[51] CyberPoint also partnered with Hacking Team, the notorious Italian surveillance technology company, to sell Hacking Team's technology to the U.A.E., who used it against pro-democracy activists.[52]

Finally, the biotechnology firm Thermo Fisher provides the Chinese government with DNA testing kits.[53] The kits are a key component of the government's massive campaign of biometric surveillance—and ultimate control and persecution—against the wider Chinese population, as well as disfavored minority groups such as Tibetans and Muslim Uyghurs.[54] Approximately one million Uyghurs are presently detained is concentration camps in Xinjiang

---

[49] 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.

[50] Gallagher, *supra* n.6.

[51] Schectman & Bing, *supra* n.18

[52] 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/.

[53] 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.

[54] 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.

province.[55]

II. United Nations Policy on Business and Human Rights Supports Denying Foreign Sovereign Immunity to Technology Companies

Denying foreign sovereign immunity to DarkMatter and any corporation is consistent with settled United Nations policy on business and human rights. The concept of "business and human rights," as a subset of corporate social responsibility, is over 25 years old.[56] It took a powerful step forward 13 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.[57]

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."[58] The Ruggie Report emphasizes that the governmental duty to protect and the corporate responsibility to respect human rights are distinct (albeit intertwined) obligations.[59]

The 2008 Ruggie Report led to the 2011 publication by the United Nations Human

---

[55] 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.

[56] The nonprofit 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.

[57] 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.

[58] *Id.* at 4.

[59] *Id.* at 17.

Rights Council of the *Guiding Principles on Business and Human Rights*, which adopted and sought to operationalize the Ruggie Report framework.[60] The United States has endorsed the *Guiding Principles* as they specifically apply to U.S. companies that provide digital surveillance technologies to foreign governments.[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]

---

[60] United Nations Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (June 16, 2011), https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. *See also* United Nations Human Rights Council, *Resolution on Human Rights and Transnational Corporations and Other Business Enterprise* [A/HRC/RES/17/4] (July 6, 2011), https://ap.ohchr.org/documents/dpage_e.aspx?si=A%2FHRC%2FRES%2F17%2F4.

[61] U.S. State Dept., *U.S. Department of State Guidance on Implementing the "UN Guiding Principles" for Transactions Linked to Foreign Government End- Users for Products or Services with Surveillance Capabilities* (Sept. 30, 2020), https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/. *Cf.* European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (July 2, 2013), https://ec.europa.eu/anti-trafficking/publications/european-commission-sector-guides-implementing-un-guiding-principles-business-and-hum-0_en.

[62] *Guiding Principles*, *supra* n.60, at 4.

[63] *Id.* at 28.

[64] *Id.* at 29.

[65] *Id*.

This Court should not facilitate "the avoidance of appropriate accountability."[66] Rather, ensuring that companies like DarkMatter cannot avoid accountability through foreign sovereign immunity is consistent with the United Nations' goal of establishing judicial avenues for human rights victims to seek justice against corporations that are complicit in abuses perpetrated by governments. The unavailability of foreign sovereign immunity to companies does not mean that U.S. courts would have unfettered authority over foreign corporations, or any corporation for that matter. The rules of personal jurisdiction continue to circumscribe the reach of U.S. courts. *See* Fed. R. Civ. P. 4(k), 12(b)(2); *International Shoe Co. v. Washington*, 326 U.S. 310 (1945); *Licciardello v. Lovelady*, 544 F.3d 1280, 1284 (11th Cir. 2008) (discussing *International Shoe*). As do the required elements of any claim, from the Computer Fraud & Abuse Act, with its requirement of "damage" or "loss," 18 U.S.C. §1030(g); to the Alien Tort Statute, 28 U.S.C. §1350, which requires that any claim by a foreign plaintiff against an American corporation for aiding and abetting governmental human rights abuses have a sufficient nexus to the United States and meet the standard tort elements of *mens rea* and *actus reus*, among others. *Nestlé USA, Inc.*, 141 S. Ct. at 1937; *Kiobel*, 133 S. Ct. at 1669.[67]

III. Foreign Sovereign Immunity Should Be Denied to Technology Companies Because Voluntary Mechanisms for Holding Them Accountable for Human Rights Abuses Are Inadequate

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

[66] *Id.* at 29.

[67] *See, e.g.*, Khakurel, *supra* n.36.

rights abuses have proven inadequate. The Ruggie Report recognizes that "companies can affect virtually all internationally recognized rights."[68] 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."[69]

The Ruggie Report argues that companies, therefore, must practice "due diligence," which involves taking steps "to become aware of, prevent and address adverse human rights impacts."[70] Due diligence[71] 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."[72] 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.[73]

---

[68] Ruggie, *supra* n.57, at 9.

[69] *Id.* at 20.

[70] *Id.* at 17.

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

[72] Ruggie, *supra* n.57, at 17.

[73] *Guiding Principles*, *supra* n.60, at 14-15.

However, the *Guiding Principles* expressly do not create any "new international law obligations."[74] Thus, the Ruggie Report's "due diligence" framework for companies is wholly voluntary. The report contemplates that voluntary mechanisms would play a significant role in corporate accountability for human rights violations.[75] The Ruggie Report and the UN's *Guiding Principles* helped spur progress in defining the right courses of action on business and human rights. Unfortunately, weakness of voluntary enforcement is evidenced by the fact that DarkMatter itself does not seem to have a due diligence or human rights policy, or at least not one that appears on its opaque online presence.[76] NSO Group does have a "due diligence" human rights program[77] yet governmental abuses continue.[78] Enforcement generally of human rights standards through voluntary corporate accountability mechanisms has been weak at best.

A. Limits of Multi-Stakeholder Initiatives

A report by MSI Integrity[79] concluded that multi-stakeholder initiatives (as a subset of voluntary human rights corporate accountability mechanisms) "are not effective tools for

---

[74] *Id.* at 1.

[75] Ruggie, *supra* n.57, at 26. *See also Guiding Principles*, *supra* n.60, at 28, 31.

[76] *See* DarkMatter, https://www.darkmatter.ae/.

[77] NSO Group, *Human Rights Policy*, https://www.nsogroup.com/governance/human-rights-policy/. *See also* Novalpina Capital, *NSO Group Announces New Human Rights Policy and Governance Framework* (Sept. 11, 2019), https://web.archive.org/web/20200418232001/https://www.novalpina.pe/nso-group-announces-new-human-rights-policy-and-governance-framework/.

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

[79] 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/.

holding corporations accountable for abuses, protecting rights holders against human rights violations, or providing survivors and victims with access to remedy."[80] This includes the leading technology-industry focused MSI, called the Global Network Initiative (GNI), discussed below. *See infra* Part III.C.[81]

The report correctly recognized that MSIs can only achieve "positive outcomes where there is genuine commitment on the part of corporate members to change."[82] The report emphasized that "MSIs do not eliminate the need to protect rights holders from corporate abuses through effective regulation and enforcement."[83] While supporting companies that are committed to avoiding human rights abuses is a useful role, the difference between these initiatives and law is clear: law ensures accountability for companies that do not care about—or are actively opposed to—respecting human rights.

This Court must recognize that denying companies like DarkMatter foreign sovereign immunity gives human rights victims a chance to enforce—through a binding judicial process—human rights standards against foreign and domestic 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)[84] wrote the

---

[80] 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.

[81] *Id.* at 24.

[82] *Id.* at 5.

[83] *Id*.

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

Guidelines for Multinational Enterprises that comprise recommendations for "responsible business conduct," which address the realm of human rights, among other areas.[85] 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.[86] The accountability mechanism for the *Guidelines* is the system of "National Contact Points" (NCPs), which are offices set up by participating countries to accept complaints—"Specific Instances"—that companies have violated the *Guidelines*.[87] Specific Instances can lead to mediation between the complainant and the company.[88] The National Contact Point for the United States is housed at the State Department.[89] The key shortcomings of the NCP/Specific Instance system are two-fold.[90] 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,[91] with only one relating to the telecommunications industry (involving T-Mobile

---

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

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

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

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

[89] 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/.

[90] *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/.

[91] 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.

and labor practices).[92] Second and more fundamentally, "the OECD Guidelines are non-binding on businesses and engagement in a Specific Instance process is voluntary."[93]

This latter shortcoming was on full display in the United Kingdom, providing a stark example for the technology industry.[94] Privacy International filed a complaint with the UK's NCP alleging that Gamma International UK Ltd.:

> supplied to the Bahrain authorities "malware" products which allowed them to hear/see and record private conversations, correspondence and other records (e.g. address books) of individuals involved in pro-democracy activities in Bahrain … [O]n the basis of information obtained by this surveillance, these individuals, who had not committed any criminal offences under Bahrain law, were subsequently detained and in some cases tortured by the Bahrain security forces.[95]
>
> 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 inthe Final Statement.[96] The UK NCP therefore sees no

---

[92] 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.

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

[94] 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 55-60%."), https://www.business-humanrights.org/en/from-us/company-response-mechanism/.

[95] 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.

[96] *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.

> 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.[97]

C. Global Network Initiative

GNI is a human rights corporate accountability program that focuses specifically on the information and communications technology (ICT) sector.[98] GNI was born out of the tragic case of Shi Tao, discussed above, where Yahoo! shared information from his email account with the Chinese government, which led to his arrest and imprisonment for nearly a decade. *See supra* Part I.C.

GNI is a voluntary program that follows a multi-stakeholder model, where its members include American and foreign technology companies, as well as civil society groups, academics, and investment firms.[99] Over two years of painstaking effort went into creating GNI,[100] including the foundational *Principles on Free Expression and Privacy*[101] and the related *Implementation Guidelines*, which require technology company members to submit to independent "assessments" or audits of their implementation of the *Principles*.[102]

While GNI should be credited for recruiting major technology companies and operationalizing human rights accountability for the ICT sector, the program has two major

---

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

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

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

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

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

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

shortcomings. First, not all technology companies are members—presently only 16 companies participate in GNI. Second and more importantly, the program's success hinges on the candor and cooperation of the member companies, which has been lacking.

Amicus was once a civil society member of GNI, until it resigned in 2013 from the organization after GNI members were implicated in mass Internet surveillance by the U.S. National Security Agency. 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.[103]

Additionally, the NYU Stern Center for Business & Human Rights resigned from GNI in 2016 due, in part, to the organization's board having removed the term "compliance" from the *Principles* and *Implementation Guidelines*, and added language stating that GNI would instead assess whether a company was "committed" to the *Principles* and was acting in "good faith" to implement them. As representatives for the Center wrote, "This is not a meaningful standard. Our assumption is that all member companies are committed to the principles and are making good faith efforts to implement them; the question is whether they are in compliance with a set of standards."[104]

CONCLUSION

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

---

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

[104] 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.

that have the sophistication and technical know-how that 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."[105]

Technology has the capacity to protect human rights, but it also can make violations ruthlessly efficient. We urge this Court to *deny* Defendant DarkMatter any form of foreign sovereign immunity. In so doing, this Court should craft a rule that denies foreign sovereign immunity to all private companies, especially those that facilitate violations of human rights. It is critical that U.S. courts remain a viable avenue for holding all technology companies accountable for their complicity in human rights abuses committed by repressive governments, especially when the U.S. judicial system may be the only available avenue of redress. This Court can help ensure that technological genius supports, rather than undermines, the rule of law.

Dated: October 19, 2021

Respectfully submitted,

SHULLMAN FUGATE PLLC

Deanna K. Shullman
Deanna K. Shullman (FBN 514462)
2101 Vista Parkway, Suite 4006
West Palm Beach, FL 33411
dshullman@shullmanfugate.com
Tel.: (561) 429-3619

and

Sophia Cope

[105] Kaye, *supra* n.13, at 6.

(*pro hac vice admission pending)*
Mukund Rathi
(*pro hac vice admission pending)*
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
sophia@eff.org
mukund@eff.org
Tel.: (415) 436-9333
Fax: (415) 436-9993

Counsel for Amicus Curiae
Electronic Frontier Foundation