NO. 15-16909

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

DOE I, DOE II, IVY HE, DOE III, DOE IV, DOE V, DOE VI, CHARLES LEE, ROE VII, ROE VIII, LIU GUIFU, DOE IX, WEIYU WANG, and those individuals similarly situated,

PLAINTIFFS-APPELLANTS,

v.

CISCO SYSTEMS, INC.,
JOHN CHAMBERS, FREDY CHEUNG AKA ZHANG SIHUA, DOES 1-100,

DEFENDANTS-APPELLEES.

On Appeal from the United States District Court
for the Northern District of California

Case No. 5:11-cv-02449-EJD

The Honorable Edward J. Davila, District Court Judge

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, ARTICLE 19, AND PRIVACY INTERNATIONAL IN SUPPORT OF PLAINTIFFS-APPELLANTS AND REVERSAL

Sophia Cope
Cindy Cohn
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: sophia@eff.org
Telephone: (415) 436-9333

Counsel for Amici Curiae

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amici Curiae* Electronic Frontier Foundation, ARTICLE 19 and Privacy International state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION i

STATEMENT OF INTEREST 1

INTRODUCTION 3

ARGUMENT 5

I. THE DISTRICT COURT'S "TOUCH AND CONCERN" ANALYSIS IS FLAWED 5

A. The District Court's "Touch and Concern" Analysis Is Inconsistent with Permitting Aiding and Abetting Claims Under the ATS 5

B. Designing and Customizing a Technology Product in the United States that Facilitates Human Rights Abuses Abroad Is Sufficient for an ATS Claim to "Touch and Concern" the U.S. 7

II. THE DISTRICT COURT'S ANALYSIS OF *MENS REA* FOR AN "AIDING AND ABETTING" ATS CLAIM IS FLAWED 9

A. Plaintiffs' Allegations Are Sufficient to Reasonably Infer That Defendants Had the *Mens Rea* of "Purpose" to Facilitate Human Rights Abuses 9

B. The District Court Misapplied the *Nestle* Factors 14

III. THE DISTRICT COURT'S ANALYSIS OF *ACTUS REUS* FOR AN "AIDING AND ABETTING" ATS CLAIM IS FLAWED: CISCO'S GOLDEN SHIELD "SUBSTANTIALLY ASSISTED" CHINA IN PERSECUTING THE FALUN GONG 19

IV. FINDING FOR PLAINTIFFS WILL NOT CREATE HUMAN RIGHTS LIABILITY MERELY FOR SELLING GENERAL-PURPOSE OR DUAL-PURPOSE PRODUCTS 23

V. TECHNOLOGY COMPANIES FACILITATING GOVERNMENTAL HUMAN RIGHTS ABUSES IS A GLOBAL PROBLEM 25

CONCLUSION 28

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(A)(7)(C) 29

CERTIFICATE OF SERVICE 30

TABLE OF AUTHORITIES

Cases

Balintulo v. Ford Motor Co.,
796 F.3d 160 (2d Cir. 2015) 6, 7, 8, 13

Doe I v. Cisco Systems, Inc.,
66 F. Supp. 3d 1239 (N.D. Cal. 2014) ("Cisco I") ..... *passim*

Doe I v. Cisco Systems, Inc.,
No. 5:11-02449, 2015 WL 5118004
(N.D. Cal. Aug. 31, 2015) ("Cisco II") ..... *passim*

Doe I v. Nestle USA, Inc.,
766 F.3d 1013 (9th Cir. 2014) ..... *passim*

Du v. Cisco Systems,
No. 11-cv-01538 (D. Md. Aug. 15, 2013)
opinion reported at 2 F. Supp 3d 717 (D. Md. 2014) 3

In re Estate of Marcos, Human Rights Litig.,
25 F.3d 1467 (9th Cir. 1994) 24

Kadic v. Karadzic,
70 F.3d 232 (2nd Cir. 1995) 23

Kiobel v. Royal Dutch Petroleum Co.,
133 S. Ct. 1659 (2013) 4, 5, 24

Rosemond v. United States,
134 S. Ct. 1240 (2014) 6

Sosa v. Alvarez-Machain,
542 U.S. 692 (2004) 24

Other Authorities

Beth Van Schaack, *China's Golden Shield—Is Cisco Systems Complicit?*, Just Security (March 24, 2015) 4

Black's Law Dictionary (5th. ed.) 6

Boeing Completes Acquisition of Narus, Boeing News Releases/Statements (July 29, 2010) 26

Electronic Frontier Foundation, *A Warning to Know Your Customer: Computerlinks Fined for Dealing Blue Coat Surveillance Technology to Syria*, (May 28, 2013)..... 26

Electronic Frontier Foundation, *Kidane v. Ethiopia* 26

Electronic Frontier Foundation, *Mass Surveillance Technologies*..... 25

Electronic Frontier Foundation, *Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA* (Feb. 21, 2012) 26

Global Internet Freedom: Corporate Responsibility and the Rule of Law: Hearing before Subcomm. on Human Rights and the Law of the S. Comm. on the Judiciary, 110th Cong. (2008) 18

Global Online Freedom Act of 2007, H.R. 275, 110th Cong..... 18

Hal Roberts, *Narus: Security Through Surveillance*, Berkman Center for Internet & Society at Harvard University (Nov. 11, 2008) 27

Hamed Aleaziz, *Syria Uses US Technology in Cyber Crackdown*, Mother Jones (Oct. 19, 2011)..... 26

Jennifer Valentin-Devries, Julia Angwin & Steve Stecklow, *Document Trove Exposes Surveillance Methods*, Wall Street Journal (Nov. 19, 2011) 25

Morgan Marquis-Boire et al., *You Only Click Twice: FinFisher's Global Proliferation*, Citizen Lab (March 13, 2013)..... 27

Sarah Stirland, *Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers*, Wired (May 20, 2008) 13

Timothy Karr, *One U.S. Corporation's Role in Egypt's Brutal Crackdown*, Huffington Post Blog (Jan. 28. 2011) 27

U.S. State Dep't, *China Country Report on Human Rights Practices for 1999* (Feb. 23, 2000) 12, 24

U.S. State Dep't, *Syria Sanctions*..... 26

Universal Declaration of Human Rights, art. 18 (Dec. 10, 1948)..... 13

Vernon Silver, *EU May Probe Bahrain Spy Gear Abuses*, Bloomberg (Aug. 24, 2011) 27

Vernon Silver, *Post-Revolt Tunisia Can Alter E-Mail with 'Big Brother' Software*, Bloomberg (Dec. 12, 2011) 27

Wired for Repression, Bloomberg 26

STATEMENT OF INTEREST[1]

Amici curiae Electronic Frontier Foundation, ARTICLE 19 and Privacy International submit this brief pursuant to Federal Rule of Appellate Procedure 29. *Amici* are non-governmental organizations that advocate for civil liberties and human rights around the world. We have a strong interest in ensuring that the law discourages companies from providing customized technologies that have the clear purpose of assisting governments in violating human rights.

The Electronic Frontier Foundation ("EFF"), founded in 1990 and based in San Francisco, works to protect individual rights in the digital world. EFF has participated as *amicus curiae* in cases focusing on corporate complicity in governmental human rights abuses. We submitted an *amicus* brief to the Fourth Circuit in an ATS case where black South Africans accused IBM of building a customized computer-based national identification system that facilitated human rights abuses under the apartheid regime.[2]

ARTICLE 19 was founded in 1987 and has an international office in London, UK, and regional offices in Brazil, Mexico, Senegal, Kenya, Bangladesh and Myanmar. The organization, named for the corresponding article of the Universal Declaration of Human Rights, advocates for freedom of expression as a

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than *amicus*, its members, or its counsel contributed money that was intended to fund preparing or submitting this brief.

[2] *Balintulo v. Ford Motor Co.*, No. 14-4104-cv, Amicus Brief of Electronic Frontier Foundation, ECF No. 57 (2d. Cir. Feb. 11, 2015), opinion reported at 796 F.3d 160 (2d. Cir. 2015).

fundamental human right, including in the digital environment. The organization has participated as *amicus curiae* in free expression cases around the world, including in the United States.

Privacy International was founded in 1990 and is based in London. It was the first organization to campaign at an international level on privacy issues. It is committed to fighting for the right to privacy across the globe, including through research, litigation and advocacy.

INTRODUCTION[3]

This is the second Alien Tort Statute ("ATS") case in which plaintiffs allege that the technology giant Cisco specially built surveillance, censorship, and other repressive products for the Chinese government that targeted disfavored groups—here, a religious minority called the Falun Gong, and in the other, prominent democracy activists—who were then subjected to torture and other recognized human rights abuses.[4]

As experts focusing on the intersection of civil liberties, human rights and technology, *amici* promote innovation while also calling for the responsible deployment of technology. We applaud the role technology companies play in spreading the benefits of the digital age around the world. We believe it is inappropriate to hold technology companies liable for violations of international law under the ATS based *solely* on their provision of general-purpose or dual-purpose technologies to governments or others who misuse them to commit human rights violations.

However, it is also important to ensure that liability is preserved for companies that intentionally build and provide ongoing support for customized technologies that have the clear purpose of facilitating governmental human rights abuses. Plaintiffs have presented allegations and evidence in this case that, if substantiated through discovery, would be sufficient to support such liability for

[3] All websites were last accessed Jan. 11, 2016.

[4] *Du v. Cisco Systems*, No. 11-cv-01538, Amicus Brief of Electronic Frontier Foundation, ECF No. 52-1 (D. Md. Aug. 15, 2013), opinion reported at 2 F. Supp. 3d 717 (D. Md. 2014)

Cisco's customization of the "Golden Shield" (also known as "The Great Firewall").[5]

The district court should not have granted Defendants' motion to dismiss Plaintiffs' Second Amended Complaint ("Complaint"). First, the district court's "touch and concern" analysis is inconsistent with the settled existence of "aiding and abetting" ATS claims. Actions taken in the United States to design and customize hardware and software technologies to facilitate human rights abuses abroad are sufficient for an ATS claim to "touch and concern" the U.S. *See Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1669 (2013). Second, Plaintiffs sufficiently pled aiding and abetting because the allegations in the Complaint—that Cisco knew about and specifically marketed its technologies to assist in the human rights violations its customer was notoriously committing—support a reasonable inference that Defendants also had the necessary *mens rea* of "purpose" to facilitate torture, forced conversion, and other human rights abuses by the Chinese government. Additionally, the Complaint sufficiently alleges that Defendants exhibited the necessary *actus reus* because Cisco developed specific portions of the Golden Shield in the U.S. to assist in the identification and location of Falun Gong practitioners, and those portions substantially assisted the Chinese government in efficiently and expansively persecuting the Falun Gong.

Third, finding for Plaintiffs will not create human rights liability for

[5] *See* Beth Van Schaack, *China's Golden Shield—Is Cisco Systems Complicit?*, Just Security (March 24, 2015), https://www.justsecurity.org/21397/chinas-golden-shield-is-cisco-systems-complicit/.

companies that merely sell general-purpose or dual-purpose products.

Finally, this Court must provide guidance for when technology companies may be held liable for stepping over the line into aiding and abetting human rights abuses, because Cisco is not alone in developing technologies that are being used to facilitate violations of human rights.

ARGUMENT

I. The District Court's "Touch and Concern" Analysis is Flawed

A. The District Court's "Touch and Concern" Analysis Is Inconsistent with Permitting Aiding and Abetting Claims Under the ATS

An ATS claim must "touch and concern" the United States "with sufficient force to displace the presumption against extraterritorial application" of the statute. *Kiobel*, 133 S. Ct. at 1669. Although the Supreme Court declined to articulate exactly what facts would meet the "touch and concern" test, something more is needed beyond "mere corporate presence" in the United States. *Id.*

Although the district court acknowledged the long-settled law that "Plaintiffs may bring claims for aiding and abetting under the ATS," *Doe I v. Cisco Systems, Inc.*, 66 F. Supp. 3d 1239, 1247 (N.D. Cal. 2014) ("Cisco I"), the court's interpretation of the "touch and concern" element effectively forecloses aiding and abetting liability. In holding that Plaintiffs did not meet the "touch and concern" test, the district court stated, "Plaintiffs have not shown that the alleged human rights abuses committed against them in China, including torture and forced conversion, were *planned, directed, or committed* in the United States." *Cisco I*, 66

F. Supp. 3d at 1246 (emphasis added). *See also Doe I v. Cisco Systems, Inc.*, No. 5:11-02449, 2015 WL 5118004, at *5 (N.D. Cal. Aug. 31, 2015) ("Cisco II").

"Aiding and abetting" presumes that there was a principal perpetrator and that the accomplice took steps "to help, assist, or facilitate the commission of a crime, promote the accomplishment thereof, help in advancing or bringing it about, or encourage, counsel, or incite as to its commission" by the principal perpetrator. *Black's Law Dictionary* (5th. ed.). "A person may be responsible for a crime he has not personally carried out if he helps another to complete its commission." *Rosemond v. United States*, 134 S. Ct. 1240, 1245 (2014).[6] But to the district court, allegations of assistance were not sufficient: "meetings with Party members, shareholders' complaints, and acknowledgment that the system was to be used to 'stop' or apprehend Falun Gong still do not establish Defendants' planning, direction, or *participation* in the human rights abuses committed against Plaintiffs." *Cisco I*, 66 F. Supp. 3d at 1246 (emphasis added).

To say that Defendants must have "committed" or "participated" in the torture and forced conversion of Plaintiffs is to say that Defendants had to have been the principal perpetrators in order for the ATS claim to "touch and concern" the United States. The district court's reliance on direct participation in human rights abuses is inconsistent with its own correct finding that aiding and abetting liability is available here.

[6] The Second Circuit also agrees that aiding and abetting is an acceptable theory of liability under the ATS. See *Balintulo v. Ford Motor Co.*, 796 F.3d 160, 166-67 (2d Cir. 2015).

B. Designing and Customizing a Technology Product in the United States that Facilitates Human Rights Abuses Abroad Is Sufficient for an ATS Claim to "Touch and Concern" the U.S.

The district court acknowledged that "Plaintiffs have properly pled that Defendants"—based in the United States—"customized, marketed, designed, and implemented the Golden Shield system for use by Chinese law enforcement." *Cisco I*, 66 F. Supp. 3d at 1246. These allegations are sufficient to show that Plaintiffs' ATS claim—based on an aiding and abetting theory of liability—"touches and concerns" the United States.

The Second Circuit's recent decision in *Balintulo* illustrates that designing and customizing a technology product in the United States that is then used abroad to facilitate human rights abuses supports a finding that an aiding and abetting ATS claim "touches and concerns" the U.S. with sufficient force to displace the presumption against the extraterritorial application of the statute. *Balintulo*, 796 F.3d at 169.

In that case, the plaintiffs were victims of apartheid. They brought ATS claims alleging that both Ford and IBM aided and abetted the human rights abuses suffered by the plaintiffs at the hands of the South African government. The Second Circuit found sufficient the plaintiffs' allegation that IBM created a customized computer-based national identification system that was then transferred to the South African government and facilitated the "denationalization" of country's black population. *Id.* The Second Circuit concluded:

> Identity documents … were an *essential component* of the system of racial separation in South Africa. And so, designing *particular*

> *technologies* in the United States that would facilitate South African racial separation would appear to be both 'specific and domestic' conduct that would satisfy the first of the two steps of our jurisdictional analysis.

Id. (citations omitted) (emphasis added).[7]

As in *Balintulo*, Plaintiffs here allege that Cisco developed hardware and software in the United States—"particular technologies"—that facilitate human rights abuses by specifically identifying and locating Falun Gong practitioners. The customized features of the Golden Shield designed in the U.S. were an "essential component" of the Chinese government's vast program of persecution against the Falun Gong, which included—once practitioners were identified and located—torture, forced conversion, and other human rights abuses. As Plaintiffs allege:

> The Golden Shield provided the essential means by which the Plaintiffs and similarly situated persons were tracked, detained, and tortured. Without the information collected and assembled through the Golden Shield, it would not have been possible to carry out the human rights and other violations against them in the same manner, or at all.

ER 77-78, Second Am. Compl. ("SAC") ¶ 225.

Thus the district court's other "touch and concern" benchmarks are also inappropriately limited and inconsistent with an aiding and abetting theory of liability. To say that Defendants must have "planned" or "directed" the torture and

[7] The Second Circuit ultimately rejected plaintiffs' aiding and abetting 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. *Balintulo*, 796 F.3d at 170. However, *Balintulo* is distinguishable because there was no allegation, as here, that IBM specifically *marketed* its technology as being able to help the South African government persecute the country's black population. *See infra* Section II.A.

forced conversion of Plaintiffs dismisses the other legally sufficient ways—short of being the masterminds—Defendants could have acted in the United States as accomplices to the human rights abuses perpetrated by the Chinese government against Plaintiffs.

II. The District Court's Analysis of *Mens Rea* for an "Aiding and Abetting" ATS Claim is Flawed

The district court erroneously applied this Court's decision in *Doe I v. Nestle USA, Inc.*, 766 F.3d 1013 (9th Cir. 2014), which was issued one day before the district court issued *Cisco I*. This error occurred in *Cisco II*, in which the district court denied Plaintiffs' Motion for Reconsideration. *Cisco II*, 2015 WL 5118004, at *5.

A. Plaintiffs' Allegations Are Sufficient to Reasonably Infer That Defendants Had the *Mens Rea* of "Purpose" to Facilitate Human Rights Abuses

Although this Court in *Nestle* chose not to decide whether a "knowledge" or "purpose" standard applies to a claim of aiding and abetting under the ATS, it leaned toward the "the more stringent purpose standard," stating that factual allegations must support a "reasonable inference" that "an aiding and abetting ATS defendant act[ed] with the *purpose* of facilitating the criminal act." *Nestle*, 766 F.3d at 1023-25 (emphasis in original). In this case, Plaintiffs' allegations support the reasonable inference that Defendants designed and built the Golden Shield with the purpose to facilitate the human rights abuses perpetrated by the Chinese government against Falun Gong practitioners, including Plaintiffs.

In *Cisco II* the district court followed *Nestle* and accepted "purpose" as the *mens rea* standard for an aiding and abetting ATS claim. The district court stated, referring to its opinion in *Cisco I*:

> This court … already applied the more lenient knowledge standard and held that Plaintiffs failed to sufficiently plead that *Defendants knew their product would be used beyond its security purposes to commit human rights violations*. … Since Plaintiffs fail to satisfy the lenient knowledge standard, they also fail to satisfy the heightened purpose standard.

Cisco II, 2015 WL 5118004, at *3-4 (emphasis added). However, the Complaint supports the reasonable inference that Cisco should have known—and surely did know—*not* that the Chinese government would use the Golden Shield *beyond* its security purposes, but that to the Chinese government "security purposes" *included* violating international human rights law by brutally suppressing a disfavored religious minority. As Plaintiffs allege:

> In the company's internal marketing literature, a high-level Cisco engineer reiterated Cisco's commitment to customize all of their products to meet security's objectives, which the same engineer described elsewhere as inclusive of—indeed devoted to—the *douzheng* of Falun Gong and other dissident groups in China.

ER 43, SAC ¶ 65. As Plaintiffs explain, *douzheng* is "the term of art used to describe persecutory campaigns comprising persecution and torture." ER 43, SAC ¶ 61.

Two types of factual allegations support the finding of sufficient *mens rea* of "purpose" to facilitate human rights abuses: Defendants knew that the Chinese

government was already persecuting practitioners of Falun Gong, and knew that the Chinese government was seeking a surveillance tool to target the Falun Gong specifically, as evidenced by the fact that Cisco *marketed* its technology for that specific purpose. It is inconceivable that Defendants did not know that the Golden Shield would be the *critical first step* in a sophisticated system of repression that included torture and forced conversion.

First, the record strongly supports the conclusion that the Chinese government's "widespread human rights abuse against Falun Gong adherents and its ongoing nature were well known to Cisco at the time that they began to market their technology for the Golden Shield project in China." ER 41, SAC ¶ 52. The district court in *Cisco I* acknowledged allegations that Defendants knew of the campaign of persecution and torture against Falun Gong believers and knew that the Chinese government considered them to be "hostile elements" that needed to be "stopped." *Cisco I*, 66 F. Supp. 3d at 1242-43 (citing ER 69, 75, 76, SAC ¶¶ 174-5, 212, 217-18).

Specifically, Defendants knew or should have known at the time they sought the initial Golden Shield contract in 1999 that the Chinese government viewed practitioners of Falun Gong as a disfavored minority and had commenced a campaign of persecution against them that same year that included torture, forced conversion, and other human rights abuses. Plaintiffs highlight several newspaper articles and reports from the United Nations and human rights groups beginning in 1999. ER 66-67, SAC ¶¶ 158-65. Additionally, in 2000, the State Department's annual human rights report for China specifically discussed the Falun Gong

repression. ER 41, 67, 69, SAC ¶¶ 51, 164, 173. Cisco had already built the core network of the Golden Shield in 1999, but designed the specific anti-Falun Gong features in 2001, meaning that the State Department report was available to the company (and broadly publicized) prior to customization. ER 65, 45, SAC ¶¶ 151, 73-74. Indeed, the Complaint specifically alleges that defendant Chambers, CEO of Cisco, as early as 1998 began "cultivat[ing] a personal relationship" with the very Chinese government official who founded the 1999 campaign of persecution against the Falun Gong. ER 72-73, SAC ¶ 197. The State Department report discussed how the Chinese "government launched a crackdown against the Falun Gong spiritual movement" during the summer of 1999, banning the "cult" and calling it "evil" in an anti-Falun Gong propaganda campaign.[8] The State Department also discussed how several Falun Gong practitioners died after being beaten while in police custody, and others were "detained in outdoor stadiums and forced to sign statements disavowing Falun Gong before being released" or sent to "reeducation-through-labor" prisons. *Id.*

Second, the record strongly supports the conclusion that Defendants knew that the Chinese government wanted Cisco's Golden Shield to include the ability to identify and locate Falun Gong believers specifically as part of a broader persecutory campaign. This is evidenced, most damningly, by Cisco's aggressive *marketing* of the company's unique capability of building a surveillance tool with customized features to target the Falun Gong. ER 42-45, SAC ¶¶ 58-74. Plaintiffs

[8] U.S. State Dep't, *China Country Report on Human Rights Practices for 1999* (Feb. 23, 2000), http://www.state.gov/j/drl/rls/hrrpt/1999/284.htm.

allege:

> The term *douzheng* was used by Cisco in internal power point presentation files to define a key purpose of the Golden Shield project as a whole, and in defining "opportunities" Cisco was pursuing in the fields of Design, Construction, Training, Security, and Maintenance. This statement of the purposes of the Golden Shield was also echoed in Cisco reports referring to the "Strike Hard" campaign against "evil cults," which the Golden Shield assisted in furthering, as equivalent to and connected to the *douzheng* of Falun Gong. All of these materials were identified as emanating from Cisco San Jose.

ER 43, SAC ¶ 62.[9] And, of course, formal governmental repression of a religious group is unequivocally a violation of long-settled human rights law.[10]

Balintulo is plainly distinguishable on this key fact—how Cisco wooed the Chinese government. The Second Circuit rejected the plaintiffs' aiding and abetting ATS claim against IBM for failure to sufficiently plead "purpose." *Balintulo*, 796 F.3d at 170. Although *amici* strongly disagree with the Second Circuit's analysis of the *mens rea* element, there was no allegation in that case—as there is here—that IBM specifically *marketed* its technology as being able to help the South African government persecute the country's black population. Given Plaintiffs' factual allegations, the district court plainly erred in concluding that

[9] *See also* Sarah Stirland, *Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers*, Wired (May 20, 2008), http://www.wired.com/threatlevel/2008/05/leaked-cisco-do.

[10] *See* Universal Declaration of Human Rights, art. 18 (Dec. 10, 1948), http://www.un.org/en/universal-declaration-human-rights/ ("Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.").

Defendants did not build and customize the Golden Shield with the purpose of ultimately facilitating torture and other human rights abuses of Falun Gong believers.

This is not to say, however, that Cisco necessarily has personal ill will toward practitioners of Falun Gong. Just as this Court noted in *Nestle*, those companies' purposeful support of child slavery did not necessarily mean that they had the subjective intent to harm children in West Africa. *Nestle*, 766 F.3d at 1025. Rather, "factual allegations concerning the defendants' goals and business operations give rise to a reasonable inference that the defendants acted with purpose" to support child slavery. *Id.* In this case, as in *Nestle*, Defendants had "a myopic focus on profit over human welfare," even if that meant facilitating human rights abuses. *Id.*

B. The District Court Misapplied the *Nestle* Factors

This Court in *Nestle* discussed three factors that may be considered when analyzing whether the defendants had the *mens rea* of "purpose" to aid and abet human rights abuses: 1) whether the defendants directly benefited from the human rights abuses committed by the principal perpetrators; 2) whether the defendants had sufficient control or leverage in the marketplace to stop the human rights abuses; and 3) whether the defendants engaged in lobbying in the United States that corroborated the inference that they supported the human rights abuses. *See Nestle*, 766 F.3d at 1024-25; *Cisco II*, 2015 WL 5118004, at *3.

The district court's application of the *Nestle* factors here was flawed in

several ways.

First, Defendants directly benefitted from the Chinese government's human rights abuses. Plaintiffs allege that the Golden Shield was highly customized to identify and locate Falun Gong practitioners specifically. ER 46-38, SAC ¶¶ 80-85. The district court erroneously inferred that this significant customization was done with no additional charge by Cisco. *Cisco II*, 2015 WL 5118004, at *4. But it is far more reasonable to infer that if the Golden Shield had been designed as a simpler, less customized, general law enforcement tool, then Cisco's fee would have been smaller. The defendants in *Nestle* benefited financially from child slavery because it ensured that they could purchase the cheapest cocoa possible due to the virtually non-existent labor costs. *Nestle*, 766 F.3d at 1024. Similarly, by being compensated for providing the Chinese government with an essential means of achieving its ambitious persecutory goals, Cisco directly benefited from the Chinese government's campaign of persecution against the Falun Gong. If additional allegations are necessary to support this direct-benefit factor, then Plaintiffs should be permitted to amend their complaint and conduct any necessary discovery. Certainly there is no allegation or evidence in the current record to support the district court's counterintuitive conclusion that:

> [T]here are insufficient allegations that Defendants obtained a direct benefit from the persecution of Falun Gong practitioners. While Plaintiffs allege that anti-Falun Gong features in the Golden Shield are lucrative to Defendants and appealing to the Chinese Government, there is no indication that Defendants would earn a reduced profit if those features were absent from the Golden Shield system.

Cisco II, 2015 WL 5118004, at *4.

Second, because Defendants had the power *not* to provide China with sophisticated surveillance and other repressive technologies, they could have at least significantly limited the Chinese government's ultimate ability to persecute and torture Falun Gong practitioners, including Plaintiffs. The district court erred by concluding that Cisco did not have sufficient control over the market in this way:

> [T]here are insufficient allegations that Defendants have ample control over the Chinese security system market such that it can stop or limit the persecution of Falun Gong practitioners. The alleged human rights violator is the Chinese Government, thus it is far-reaching to conclude that Defendants—an American private company and its executives specializing in internet networking—can have sufficient influence or leverage over the Chinese Government so as to dictate its policies regarding Falun Gong.

Id. Plaintiffs allege that Defendant Chambers, the CEO of Cisco, "was in a position to prevent Cisco's tortious conduct in relation to the Golden Shield …." ER 74, SAC ¶ 208. Similarly, "Defendant Cheung knew of the campaign of torture and persecution of Falun Gong practitioners in China [and] was in a position to influence Cisco's tortious conduct during the development of the Golden Shield …." ER 76, SAC ¶ 219.

Additionally, the district court applied this second factor in a way that does not take into account the different context of this case. In *Nestle*, the defendants were *purchasers* of cocoa produced by Ivory Coast farmers who enslaved child laborers. The defendants "dominate[d]" the Ivory Coast cocoa market "by forming

exclusive buyer/seller relationships" with the farmers. *Nestle*, 766 F.3d at 1017. Thus, it was reasonable for this Court to conclude that the "defendants had the means to stop or limit the use of child slavery, and had they wanted the slave labor to end, they could have used their leverage"—as exclusive buyers—"in the cocoa market to stop it." *Id.* at 1025.

By contrast, Cisco is a *seller* of technology. Thus the district court should have applied the control-leverage factor by discussing how it may be shown that a company *sold* its technology with the purpose of facilitating human rights abuses by its customer. The allegation that Cisco specifically marketed tools to facilitate human rights abuses and touted its ability to better track Falun Gong believers than its competitors supports the conclusion that Cisco leveraged its position in the marketplace to better assist China in its campaign to persecute the Falun Gong. It is no secret that Cisco was eager to enter the "lucrative security technology market in China." ER 41, SAC ¶ 55. As Plaintiffs allege, "In 2002, in internal files Cisco acknowledged that the purpose of the Golden Shield was to *douzheng* Falun Gong and described this goal as a lucrative business opportunity for the company." ER 71, SAC ¶ 187.

Thus Defendants engaged in an aggressive marketing campaign—which included building relationships with Communist Party officials—to convince the Chinese government that Cisco could build a sophisticated system to best meet the Chinese government's well-documented goal and practice of persecuting the Falun Gong. ER 42-45, 72-73, SAC ¶¶ 58-72, 196-99. It is readily inferable that since Cisco had already built foundations of the Golden Shield for China before it

engaged in the specific customizations aimed at targeting Falun Gong practitioners, had Cisco chosen *not* to build the specific customization package, the company could have reduced the human rights violations the Chinese government was able to carry out against the Falun Gong.

Third, Defendants attempted to shape U.S. policy to support the Chinese government's human rights violations. Cisco testified before Congress denying any involvement in the Chinese "Great Firewall" (i.e., Golden Shield)[11] as Congress considered legislation that would control how U.S. companies sell technologies to repressive governments in order to prevent U.S. complicity in Internet surveillance and censorship.[12] Additionally, Plaintiffs allege that "Senior Director of Corporate Communications at Cisco, Terry Alberstein, wrote a letter published in the *Taipei Times* responding to allegations of Cisco's contributions to human rights abuses in China." ER 69, SAC ¶ 177. It is reasonable to infer that Cisco did take steps to protect its ability to sell customized surveillance technology to China. If additional allegations are necessary to support this factor, which was embraced by this Court

---

[11] *See Global Internet Freedom: Corporate Responsibility and the Rule of Law: Hearing before Subcomm. on Human Rights and the Law of the S. Comm. on the Judiciary*, 110th Cong. (2008) (statement of Mark Chandler, Senior Vice President Legal Services, General Counsel and Secretary, Cisco Systems, Inc.), https://www.judiciary.senate.gov/imo/media/doc/08-05 20Mark_Chandler_Testimony.pdf at 3 ("Allegations that Cisco has built a 'great firewall' in China or elsewhere confuse the provision of the basic pipes of the Internet, which include basic security features that every network must have, with more specific technological mechanisms which may be implemented to achieve the invasive effects that have raised specific concerns.").

[12] *See, e.g.*, Global Online Freedom Act of 2007, H.R. 275, 110th Cong., https://www.congress.gov/bill/110th-congress/house-bill/275/.

long after the Complaint was filed, then Plaintiffs should be permitted to amend their Complaint. The district court erroneously concluded that:

> [T]here is no indication that Defendants have taken any action to shape American policy towards the Chinese Government and their laws regarding Falun Gong, such as lobbying the federal government to defeat legislation that would aid Falun Gong practitioners in China.

Cisco II, 2015 WL 5118004, at *4.

Therefore, all three *Nestle* factors, when appropriately analyzed in the context of this case, weigh in favor of concluding that Plaintiffs' Second Amended Complaint survives a motion to dismiss on whether Defendants created the Golden Shield for the purpose of facilitating the Chinese government's program of persecution against Plaintiffs and other Falun Gong believers.

III. The District Court's Analysis of *Actus Reus* for an "Aiding and Abetting" ATS Claim Is Flawed: Cisco's Golden Shield "Substantially Assisted" China in Persecuting the Falun Gong

In *Nestle*, this Court "decline[d] to adopt an *actus reus* standard for aiding and abetting liability under the ATS." *Nestle*, 766 F.3d at 1026. However, this Court stated that there must be a "causal link between the defendants and the commission of the crime." *Id.* Following *Nestle*, the district court accepted the *actus reus* standard that a defendant must have provided "substantial assistance or other forms of support to the commission of the crime." *Cisco II*, 2015 WL 5118004, at *4 (quoting *Nestle*, 766 F.3d at 1026). However, the district court failed to see the very obvious causal link between Cisco's Golden Shield and the human rights abuses suffered by Plaintiffs at the hands of the Chinese government.

Far from providing general-purpose equipment, the Complaint alleges that Cisco sold products customized specifically to assist in the Chinese government's persecution of the Falun Gong. Cisco designed the Golden Shield to work in an integrated fashion with public security torture activities and detention operations to facilitate the identification, apprehension and detention of Falun Gong practitioners. ER 44, 46, 48-49, 52-53, 54, 59, 60, SAC ¶¶ 68, 77-78, 84-86, 88-89, 98-99, 101, 125, 131.

The district court disregarded these allegations. In *Cisco I* the district court simply stated that "the allegations in the SAC do not show that Defendants' conduct had a substantial effect on the perpetration of alleged violations against Plaintiffs." *Cisco I*, 66 F. Supp. 3d at 1248. In *Cisco II* the district court stated only, "Plaintiffs have failed to provide a persuasive argument as to why this court's previous ruling should be changed." *Cisco II*, 2015 WL 5118004, at *4.

In each decision, the district court overlooked specific and detailed allegations that clearly show that Cisco's Golden Shield substantially assisted the Chinese government in its human rights abuses, including:

> **Identification and Location of Falun Gong:** Cisco created a library of carefully analyzed patterns of Falun Gong Internet activity (or "signatures") that enable the Chinese government to uniquely identify Falun Gong Internet users. ER 46-47, SAC ¶ 80.
>
> **Databases to Centralize Information About Falun Gong:** Cisco created several log/alert systems that provide the Chinese government with real-time monitoring and notifications based on Falun Gong Internet traffic patterns. ER 46-48, SAC ¶¶ 80, 82, 83.
>
> **Integration with General Security:** Cisco integrated the Falun Gong-specific databases alleged above with the rest of the Internet

Surveillance System it built for general law enforcement purposes. ER 47, SAC ¶ 80.

Forced Conversion Information: Cisco created systems for storing data profiles on Falun Gong practitioners for use during interrogation and "forced conversion" (*i.e.*, torture), as well as a system for storing and sharing of "effective forced conversion sessions with other security to enable them to learn how best to force the Falun Gong adherent to renounce his religious belief." ER 48, 52-53, SAC ¶¶ 84-86, 98-99. Cisco also created a system for categorizing individual Falun Gong adherents by their likely susceptibility to different methods of "forced conversion." ER 48-49, SAC ¶¶ 88-89.

Advanced video analyzers: Cisco created highly advanced video and image analyzers for the Chinese government, which it marketed as "the only product capable of recognizing over 90% of Falun Gong pictorial information." ER 51, SAC ¶ 97.

Nationwide Video Surveillance: Cisco created a networked video surveillance system, integrated across all Chinese provinces, which has been a primary means for the identification and detention of Falun Gong adherents. ER 52, SAC ¶ 97.

The Complaint further traces the practical application and development of the Golden Shield after deployment, detailing how Cisco further honed the product toward the goal of assisting the Chinese government in identifying and locating the Falun Gong. ER 50, SAC ¶ 92.

Ongoing Improvement in Identification and Location of Falun Gong Tool: Cisco's "Ironport" product, incorporated in the Golden Shield by 2007, was an email and website tracking and blocking system. ER 50, 51-52, SAC ¶¶ 93, 97(c). This allowed Chinese authorities to identify Falun Gong email communication as distinct from other communication about the Falun Gong, in order to facilitate the apprehension of Falun Gong believers who sent pictorial Falun Gong images to others in China. *Id.* Cisco drew on its "extensive and long-term identification and analysis of Internet activity unique to

> Falun Gong practitioners" in order to build this customized surveillance tool. ER 52, SAC ¶ 97(c).
>
> **Falun Gong Blocking and Logging Engine:** Cisco's "Service Control Engine" detects and blocks Falun Gong web content and logs the data about such web presence. ER 52, SAC ¶ 97(d). Cisco's promotional materials for the Service Control Engine included specific warnings about four 'Current Threats' online—all of which were Falun Gong-related. *Id.*

The Complaint also ties these customized technologies to the specific arrest, detention and torture of Plaintiffs. ER 78, SAC ¶¶ 227, 229.

The thrust of Plaintiffs' allegations focuses on how Cisco's customized technology substantially assisted the Chinese government by making its campaign against the Falun Gong highly efficient and capable of achieving a vast scale. As Plaintiffs allege:

> Without Cisco's networked technology (with first-of-their-kind features) and the Golden Shield's far wider scale, complexity and capacity, Public Security and Office 610 officers would not have been able to obtain sensitive information from almost anywhere in China such as home and work addresses, purchases, financial information, contact with other Falun Gong members, past Falun Gong activities, IP addresses, and family information (used for interrogation and forced conversion practices/purposes). Nor would it have been possible for security officers to coordinate large-scale investigations, locate, track, apprehend, interrogate, torture and persecute Falun Gong members from anywhere in China without having to search each and every home and office for evidence.

ER 54-55, SAC ¶ 106.

Technology can be customized not only to make violations possible, but also to make violations ruthlessly efficient. Thus, this Court should conclude that

Plaintiffs have sufficiently alleged that Cisco—through its customized Golden Shield system—substantially assisted the Chinese government's human rights abuses against Falun Gong believers.

IV. Finding for Plaintiffs Will Not Create Human Rights Liability Merely for Selling General-Purpose or Dual-Purpose Products

To be clear, *amici* believe that it is inappropriate to hold companies liable for selling general-purpose or dual-purpose products to the general public that are later misused. The law does not and should not so hold.

The facts of this case, plus the ATS and international law, already carefully cabin liability here in several key ways.

First, Cisco's liability under international law turns on the fact that it is selling technologies to the Chinese government. Unlike commercial sales to the public, international law attaches to actions taken by state actors or taken under color of law, with only minimal exceptions. *See*, *e.g.*, *Kadic v. Karadzic*, 70 F.3d 232, 245 (2nd Cir. 1995). Thus, the sale of technologies to private actors for private use generally cannot serve as the basis for vendor liability under international law. This limitation also means that the chances that a company would unwittingly provide technologies for use in human rights abuses are slim—government contracting is generally a sophisticated and eyes-open process. As noted above, even assuming that Cisco had been completely unaware of the Chinese goals, a cursory check of the U.S. State Department reports would have alerted Cisco to the strong likelihood that the technologies it was providing to the

Chinese government would be used to facilitate human rights abuses against the Falun Gong.[13]

Second, liability under the ATS only attaches to specific, universal, and obligatory violations of international law.[14] *Sosa v. Alvarez-Machain,* 542 U.S. 692, 732 (2004) (*quoting In re Estate of Marcos, Human Rights Litig.,* 25 F.3d 1467, 1475 (9th Cir. 1994)); *see also Kiobel*, 133 S. Ct. at 1665. Thus, liability under the ATS under aiding and abetting or conspiracy theories is also limited to situations in which the underlying acts are gross human rights abuses like torture and arbitrary arrest and detention. Liability under the ATS simply does not arise from garden-variety offenses or crimes.

Third, this case is plainly different from one in which a company sells a dual-purpose product that is subsequently misused. While on the margins it may be difficult to recognize the difference between a dual-purpose tool and a customized one, this difference is not conceptually difficult. For example, a hammer is a dual-purpose tool. A person can use a hammer to pound nails into wood or to bludgeon another person. The hammer manufacturer designs the hammer to transfer substantial force to the object it hits regardless of how it is used. In this sense, the hammer is dual-purpose, and although it can effectuate a crime, it was not customized and sold to the customer for that particular purpose.

---

[13] *See, e.g.*, U.S. State Dep't, *China Country Report on Human Rights Practices for 1999* (Feb. 23, 2000), http://www.state.gov/j/drl/rls/hrrpt/1999/284.htm.

[14] The Supreme Court also emphasized that this also "enabled federal courts to hear claims in a very limited category defined by the law of nations and recognized at common law." *Sosa,* 542 U.S. at 712.

The technologies that Defendants continue to provide and support appear at base to be routers, which by themselves are dual-purpose devices akin to hammers in that they can both facilitate communication and be used for surveillance and other state-sponsored abuses. Yet the facts alleged in the Complaint indicate that Defendants did far more than merely sell off-the-shelf routers to the Chinese government and far more than merely adapt their technology for Chinese language speakers, as suggested by counsel at the oral argument.[15] Instead, Plaintiffs allege specific facts that Defendants knowingly customized their router-based technologies specifically for the purpose of facilitating human rights abuses against the Falun Gong.

V. Technology Companies Facilitating Governmental Human Rights Abuses is a Global Problem

Cisco's complicity in persecuting the Falun Gong and other disfavored groups in China does not exist in a vacuum.[16] Cisco is simply one player in a growing trend of U.S. and European technology companies earning a profit by making the violation of human rights a highly efficient enterprise for governments. Western-provided surveillance and censorship technologies assist in the harassment, arrest, and torture of religious minorities, democratic activists, journalists, and human rights advocates.[17] *Amicus* EFF has even discovered the

[15] Oral Arg. Tr., Mar. 21, 2014, 23:14, ECF No. 144.
[16] *See, e.g.,* Electronic Frontier Foundation, *Mass Surveillance Technologies*, https://www.eff.org/issues/mass-surveillance-technologies.
[17] *See, e.g.*, Jennifer Valentin-Devries, Julia Angwin & Steve Stecklow, *Document Trove Exposes Surveillance Methods*, Wall Street Journal (Nov. 19, 2011), http://online.wsj.com/article/SB10001424052970203611404577044192607407780

abuse of surveillance technologies within the United States by the Ethiopian government.[18]

Oppressive regimes in the Middle East in particular have received surveillance and censorship tools originating from Western, often American, companies in recent years. The Syrian government uses technology originating from American company Blue Coat Systems to engage in surveillance and censorship of Internet communications.[19] As of May 2013, after the U.S. enacted sanctions in 2011,[20] evidence suggested that Syria was using 34 Blue Coat Systems servers,[21] as well as surveillance technology from the Italian company Area SpA.[22] Another American company, Narus, now owned by Boeing,[23] provided Telecom Egypt with technology that allows network managers to track and filter the

---

.html; *Wired for Repression*, Bloomberg, http://topics.bloomberg.com/wired-for-repression.

[18] *See* Electronic Frontier Foundation, *Kidane v. Ethiopia*, https://www.eff.org/cases/kidane-v-ethiopia.

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

[20] U.S. State Dep't, *Syria Sanctions*, http://www.state.gov/e/eb/tfs/spi/syria/.

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

[22] Electronic Frontier Foundation, *Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA* (Feb. 21, 2012), https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa.

[23] *Boeing Completes Acquisition of Narus*, Boeing News Releases/Statements (July 29, 2010), http://boeing.mediaroom.com/2010-07-29-Boeing-Completes-Acquisition-of-Narus.

communications of Internet and cell phone users.[24] Narus' other customers include Pakistan and Saudi Arabia, both of which share Egypt's poor track record on human rights.[25] United Kingdom company FinFisher also provided surveillance technology to the Egyptian government[26] and to the government of Ethiopia.[27] During the Tunisian revolution the government used technologies from Blue Coat Systems and NetApp, another U.S. company, to conduct surveillance and censorship against online and mobile users.[28] The German company Trovicor provided the Bahraini government with surveillance technology that led to the torture of democratic activists.[29] And the French company Amesys provided

[24] Timothy Karr, *One U.S. Corporation's Role in Egypt's Brutal Crackdown*, Huffington Post Blog (Jan. 28. 2011), http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html.
[25] Hal Roberts, *Narus: Security Through Surveillance*, Berkman Center for Internet & Society at Harvard University (Nov. 11, 2008), http://blogs.law.harvard.edu/surveillance/2008/11/11/narus-security-through-surveillance/.
[26] Electronic Frontier Foundation, *Spy Tech Companies & Their Authoritarian Customers, Part I: FinFisher And* Amesys (Feb. 16, 2012), https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys.
[27]Morgan Marquis-Boire et al., *You Only Click Twice: FinFisher's Global Proliferation*, Citizen Lab (March 13, 2013), https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.
[28] Vernon Silver, *Post-Revolt Tunisia Can Alter E-Mail with 'Big Brother' Software*, Bloomberg (Dec. 12, 2011), http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html.
[29] Vernon Silver, *EU May Probe Bahrain Spy Gear Abuses*, Bloomberg (Aug. 24, 2011), http://www.bloomberg.com/news/2011-08-24/eu-legislators-ask-for-inquiry-into-spy-gear-abuses-in-bahrain.html.

surveillance technology to the Libyan government under Muammar Qaddafi.[30]

CONCLUSION

In the digital age, repressive governments do not act alone to violate human rights. They have accomplices—including American technology companies like Cisco, as alleged by Plaintiffs—with the sophistication and technical know-how that those repressive governments lack. If aiding and abetting liability under the Alien Tort Statute is to mean anything, it must apply to cases like this—where an American company took knowing and purposeful steps in the United States to market to and provide a foreign government with customized technological tools to meet its specific persecutory goals. This Court should overturn the district court and reverse the granting of Defendants' motion to dismiss.

Dated: January 11, 2016

By: /s/ Sophia Cope
Sophia Cope

ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
sophia@eff.org

Counsel for Amici Curiae Electronic Frontier Foundation, ARTICLE 29, and Privacy International

[30] Electronic Frontier Foundation, *Spy Tech Companies & Their Authoritarian Customers, Part I: FinFisher And Amesys* (Feb. 16, 2012), https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys.

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(a)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amici Curiae Electronic Frontier Foundation In Support of Plaintiffs-Appellees complies with the type-volume limitation, because this brief contains 6,937 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: January 11, 2016

By: /s/ Sophia Cope
Sophia Cope

Counsel for Amici Curiae Electronic Frontier Foundation, ARTICLE 19, and Privacy International

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on January 11, 2016.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: January 11, 2016

By: /s/ Sophia Cope
Sophia Cope

Counsel for Amici Curiae Electronic Frontier Foundation, ARTICLE 19, and Privacy International