Nos. 15-16909

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

DOE I, DOE II, Ivy HE, DOE III, DOE IV, DOE V, DOE VI, ROE VII, Charles LEE, ROE VIII, DOE IX, LIU Guifu, WANG Weiyu, individually and on behalf of proposed class members,

Plaintiffs-Appellants,

v.

CISCO SYSTEMS, INC., John CHAMBERS, Fredy CHEUNG, and Does 1-100,

Defendants and Appellees,

Appeal from United States District Court
for the Northern District of California
No. 5:11-cv-02449-EJD
The Honorable Edward J. Davila, United States District Judge

APPELLANTS' OPENING BRIEF

Terri E. Marsh (SB #447125)
Human Rights Law Foundation
1615 L Street, NW
Suite 1100
Washington, D.C. 20036
Telephone: (202) 697-3858
Facsimile: (202) 355-6701

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND REGULATIONS

OTHER AUTHORITIES

INTRODUCTION

This case is brought on behalf of individuals who were persecuted and abused based on their religion, with a U.S. corporation designing, building, implementing, and profiting from the system that led to their abuse – actions that substantially took place on U.S. soil, involving U.S. employees, accruing profits to a U.S. entity, which knew all the time how its products were assisting in the persecution. Yet the court below ruled that the U.S. corporation cannot be held accountable, for a variety of reasons, none of which stand up under applicable law.

U.S. corporation Cisco Systems, Inc. and its executives ("Cisco"), operating largely from the United States, committed torts central to the Chinese Communist Party's ("Communist Party") fifteen year-long campaign of violent religious persecution, torture, and other abuses targeted against Falun Gong believers in regions across China. Through their tailored technology designs, services, and implementation of the Orwellian surveillance network known as the Golden Shield and its anti-Falun Gong systems, Cisco furthered the widespread religious persecution and torture of Plaintiffs and similarly situated individuals. Falun Gong's special status in China as the most recent target of Stalinist-style violent purges was well known within the technology community, as was the peaceful character of the religious practice. Despite its knowledge of the Communist Party's persecutory goals, Cisco recommended first-of-a-kind, essential anti-Falun Gong systems to further these goals. Cisco, for considerable profit and self-serving benefit, designed and developed applications, system "solutions," and a sophisticated webbed architecture – all customized to target and further the alleged abuses against Falun Gong believers across China.

STATEMENT OF JURISDICTION

This appeal is taken from a final judgment entered on August 31, 2015. Appellants filed a timely Notice of Appeal on September 24, 2015, in response to the district court's orders of dismissal. The district court had subject matter jurisdiction over Appellants' claims pursuant to 28 U.S.C. §§ 1331 and 1350.

ISSUES PRESENTED FOR REVIEW

1. Do Plaintiffs' allegations establish aiding and abetting liability under the Alien Tort Statute (ATS)?
2. Are Plaintiffs' ATS claims barred under the presumption against extraterritoriality?
3. Does the Torture Victims Protection Act (TVPA) provide for aiding and abetting liability?
4. Did the district court err in not considering Plaintiffs' claims that Defendants participated in a conspiracy or joint criminal enterprise?

STATEMENT OF THE CASE

I. Statement of Facts

As Cisco was well aware at the time it performed the relevant conduct set forth herein, the Communist Party launched a widespread persecutory campaign against Falun Gong in 1999. SAC ¶ 37. The term used historically by the Communist Party to refer to its campaigns of violent persecution is "*douzheng*." SAC ¶ 31. Such campaigns, including the campaign against Falun Gong, typically involve the identification of targets; the banning of their activities; their condemnation and demonization by Communist Party mouthpieces; widespread apprehension, isolation, or detention; "forced conversion" through acts of torture (referred to by the Chinese term "*zhuanhua*"); extrajudicial killings; and enforced disappearances. SAC ¶¶ 31, 45-46. This *douzheng* campaign was principally carried out by officials and agents of China's Ministry of Public Security and "Office 610," a subdivision of the Communist Party dedicated specifically to the persecution of Falun Gong believers (referred to collectively herein as "Chinese security"). SAC ¶¶ 41-42. Because Plaintiffs are members of a religious group, the term "religious persecution" is used along with "*douzheng*" throughout this brief to refer to this campaign. This Circuit has long recognized the persecutory nature of China's actions toward Falun Gong believers. *See, e.g., Zhou v. Gonzales*, 437 F.3d 860, 868 (9th Cir. 2006).

The Communist Party intended the "Golden Shield" project as an Orwellian apparatus to perform both routine crime control operations and violent forms of religious and political persecution targeted at dissidents. The religious persecution of Falun Gong believers, identified by the Communist Party as its "number one" enemy, was one of its most important goals. SAC ¶¶ 2, 5, 55. Because a technological system of this sophistication was beyond China's native

technological capacity at the time, the Communist Party and Chinese security turned to prominent Western technology companies, including Cisco, for assistance. SAC ¶¶ 54-55. In doing so, they made their objectives clear: they needed a 21st century bespoke apparatus to suppress dissidents, especially Falun Gong believers. SAC ¶¶ 2, 56. In order to win lucrative Golden Shield contracts, Cisco committed itself to meeting these persecutory objectives. SAC ¶¶ 58-61. As a result, Cisco was selected on successive occasions to design, implement, maintain, and service the Golden Shield project and especially its bespoke anti-Falun Gong systems.

Cisco's assistance took several forms. Cisco designed, tailored, and integrated its products and features to target Falun Gong believers and to facilitate persecution, torture, and other abuses. By integrating Falun Gong databases with an "Internet Surveillance System," which identifies and tracks Falun Gong believers' Internet activities, Cisco's technology fed sensitive and tailored information on detainees used during interrogation, forced conversion, and torture sessions to Chinese security. SAC ¶¶ 82-85, 88, 91. Cisco further integrated these Falun Gong databases into China's anti-Falun Gong security infrastructure, including its police detention centers, clandestine jails, Public Security mental hospitals devoted to political opponents, and other detention and torture sites. SAC ¶ 98(h). Cisco's designs show how to track, monitor and identify Falun Gong believers to further their religious persecution. SAC ¶¶ 82-83, 94, 97-98.

In line with their business model and corporate structure, Cisco's San Jose headquarters maintained sole control through the entirety of the project. SAC ¶ 144. As the public face of Cisco in China, Cisco's subsidiaries operated as satellite offices for San Jose headquarters, with executives reporting to Cisco in San Jose.

SAC ¶¶ 138-39. Cisco's San Jose headquarters supervised and directed the Golden Shield marketing strategy, handled all aspects of the design phases of the project, and managed and controlled implementation and optimization. SAC ¶¶ 65, 127, 129, 145. The benefits were not insignificant. According to its own reporting, China accounted for $900 million in earnings for 2008 and sought to reach $7 billion in earnings for 2013. *See* SAC ¶¶ 168, 196.

As Cisco profited from its design, maintenance, servicing, and implementation of the Golden Shield and its anti-Falun Gong systems, the decade-long use of the apparatus to subject Falun Gong believers to religious persecution, torture and other abuses was widely reported in the United States by the media, the U.S. State Department, the United Nations, and human rights organizations. SAC ¶ 51. Communist Party reports describing the use of anti-Falun Gong systems to facilitate torture and persecution were also transmitted to Cisco's San Jose headquarters by its own sales team. SAC ¶¶ 88-91. More generally, the torture and other abuses carried out against Falun Gong believers were widely reported by media outlets, international human rights organizations, the U.S. government, U.S. court opinions, the United Nations, and the European Parliament. SAC ¶¶ 48-50, 160-67, 173.

The anti-Falun Gong systems provided by Cisco were used to identify and locate Plaintiffs for apprehension, detention, and torture. *See* SAC ¶¶ 319, 235, 241, 252, 267-68, 277-78, 287-88, 295-97, 301-02, 311-12, 322-25, 334, 343, 347-51. These anti-Falun Gong systems were also used to assist specific acts of torture carried out against Plaintiffs. During Plaintiff Wang Weiyu's detention, for example, security officials threatened his wife and used her anonymous Internet communications with overseas Falun Gong believers to force Wang to renounce

his belief in Falun Gong. SAC ¶ 356. Similar examples related to the other named Plaintiffs are available at SAC ¶¶ 237, 243, 247, 256, 260, 269, 273, 279-81, 289, 299, 306, 313, 319, 327, 340, 343.

II. Procedural History

Plaintiffs filed their original Complaint on May 15, 2011, followed by a First Amended Complaint on September 2, 2011, and a Second Amended Complaint ("SAC"), filed with leave of the court, on September 18, 2013. Defendants filed a motion to dismiss ("MTD").

After briefings and a March 21, 2014 hearing, the district court granted Defendants' MTD on September 5, 2014. One day prior, on September 4, 2014, the Ninth Circuit handed down a decision in *Doe I v. Nestle USA, Inc.*, 766 F.3d 1013 (9th Cir. 2014) ("*Nestle*"), addressing claims under the ATS similar to Plaintiffs' claims here.

On October 3, 2014, Plaintiffs filed a Motion for Reconsideration ("MFR"), arguing that because the district court was unable to consider *Nestle* given the close time proximity between the two decisions, and because *Nestle* substantially affected the district court's analysis, the district court should reverse its grant of the MTD. Following briefings, on August 31, 2015, the district court denied Plaintiffs' MFR.

III. Summary of Argument

The district court erred in holding that Plaintiffs' allegations were not sufficient to establish aiding and abetting liability under customary international law. First, the district court applied an incorrect *actus reus* standard, requiring that the accused must have "planned" or "directed" the underlying violations, a requirement having no basis in customary international law. Plaintiffs' allegations

meet the correct standard. Second, the district court erred in finding that Plaintiffs' allegations do not show that Cisco knew its conduct would assist unlawful conduct as opposed to legitimate security operations in China. Plaintiffs' allegations show that Cisco not only knew its conduct would assist torture and crimes against humanity, but provided assistance specifically for this purpose.

The district court erred in holding that Plaintiffs' claims were barred under the presumption against extraterritoriality. Requiring that Cisco planned, directed, or executed the underlying violations in the United States, the district court applied an even more extreme version of Justice Alito's concurring opinion in *Kiobel v. Royal Dutch Petroleum Co.*, 133 S.Ct. 1659 (2013) ("*Kiobel*"), which the Ninth Circuit rejected in *Nestle*, 766 F.3d at 1028. Cisco's conduct touches and concerns the territory of the United States with sufficient force to overcome the presumption, because a number of factors establish a sufficient nexus to the United States and because Cisco aided and abetted the underlying violations from the United States.

The district court misapplied Ninth Circuit precedent in holding that claims of aiding and abetting liability cannot be brought under the TVPA, 28 U.S.C. § 1350. In addition, the district court failed to consider Plaintiffs' claims that Cisco participated in a conspiracy or joint criminal enterprise.

STANDARD OF REVIEW

A dismissal for failure to state a claim is reviewed de novo. *Abagninin v. AMVAC Chem. Corp.*, 545 F.3d 733 (9th Cir. 2008). All factual allegations in the complaint must be accepted as true, and the pleadings construed in the light most favorable to the nonmoving party. *Id*. Rule 8 of the Federal Rules of Civil Procedure require plaintiffs to provide a "short and plain" statement of the claim

showing that the pleader is entitled to relief. Fed. R. Civ. P. 8(a)(2). A complaint must state "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A complaint is facially plausible when the pleaded factual content allows a court to draw a reasonable inference that the defendant is liable for the misconduct alleged. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Though a court considers any "obvious alternative explanation" for defendant's behavior when considering plausibility, if there are two plausible alternative explanations, one advanced by defendant and the other advanced by plaintiff, plaintiff's complaint survives a motion to dismiss. *Eclectic Props E., LLC vs. Marcus & Millichap Co.*, 751 F.3d 990, 996 (9th Cir. 2014) (quoting *Starr v. Baca*, 652 F.3d 1202, 1215 (9th Cir. 2011)). A complaint cannot be dismissed due to an alternative explanation unless it is so convincing that plaintiff's explanation is rendered implausible. *Id*.

ARGUMENT

I. PLAINTIFFS ADEQUATELY ALLEGE AIDING & ABETTING.

The district court below held that Plaintiffs have not "sufficiently alleged that Defendants are liable under the ATS for aiding and abetting the alleged violations." Excerpts of Record ("ER") 26. In reaching this conclusion, the district court applied an *actus reus* standard that lacks any basis in customary international law, and misapplied the appropriate *mens rea* standard.

A. Cisco's Alleged Conduct Meets the Required *Actus Reus* Standard.

Under *Sosa v. Alvarez-Machain*, 542 U.S. 692 (2004) ("*Sosa*"), and its progeny, courts looks to customary international law to determine the aiding and abetting liability standard. The district court below failed to apply the proper *actus reus* standard as set forth under this body of law, misstating the standard by

requiring that a defendant plan or direct the abuses committed against Plaintiffs. *See* ER 23-24, 26. In addition, the district court appears to require that an aider and abettor tailor his or her conduct to further the alleged abuses. *Id*. at 27. However, under customary international law, the *actus reus* element is met where the accused provides assistance that has a substantial effect on the commission of the crime, even if the conduct, standing alone, is neutral or not inherently unlawful, and even if the accused did not have control or authority over the principal perpetrator. *Prosecutor v. Taylor*, Case No. SCSL-03-01-A, Appeal Judgment, ¶¶ 362, 370, 395 (SCSL September 26, 2013) ("*Taylor*").

As demonstrated below, Plaintiffs' well-pled allegations meet the *actus reus* standard under three independent grounds: (1) Cisco provided the essential means by which the underlying violations were carried out; (2) Cisco's conduct supported, sustained, and enhanced the capacity of the Communist Party and Chinese security to carry out the underlying violations; and (3) Cisco's conduct maintained a widespread system of crimes.

1. The *actus reus* standard under customary international law requires only the provision of assistance, whether neutral or inherently unlawful, that has a substantial effect on the commission of the crimes.

The district court erred in holding that aiding and abetting liability under the ATS requires that the underlying crimes be "planned" or "directed" by a defendant. ER 23-24, 26.[1] This test has no basis in customary international law. Virtually all

[1] The district court drew this standard from *dicta* in *Sexual Minorities Uganda v. Lively*, 960 F.Supp.2d 304, 322 (D. Mass. 2013) ("*Sexual Minorities Uganda*"). As a factual matter, that case considered in part allegations that the defendant "plann[ed] and manag[ed] a campaign of repression," but nowhere were such allegations *required* to establish *actus reus*. *Id*. The court stated that the "relevant question" is whether the plaintiff alleged that "substantial practical assistance was afforded to the commission of the crime." *Id*. at 322-23.

sources of customary international law agree that the *actus reus* of aiding and abetting liability is met where "an accused's acts and conduct of assistance, encouragement and/or moral support had a substantial effect on the commission of each charged crime." *Taylor*, ¶ 362; *see Nestle* 766 F.3d at 1026. The assistance need not be provided to the physical actor or be used in the commission of the specific crime. *Id*. Nor is "[i]t . . . necessary as a matter of law to establish whether [the accused] had any power to control those who committed the offenses." *Taylor*, ¶ 370 (quoting *Prosecutor v. Simic*, Case No. IT-95-9-A, Appeal Judgment, ¶ 541 (ICTY November 28, 2006) ("*Simic*")). The question is whether the assistance had a substantial effect, not the "particular manner in which such assistance was provided." *Id*. at ¶ 368. There is no support for the district court's "planning or directing" requirement. As a result of its adoption of the wrong standard, the district court reached the wrong conclusion.

If a substantial effect has been demonstrated, assistance that is not inherently criminal in the abstract can lead to liability. *See Taylor*, ¶ 395; *Prosecutor v. Furundzija*, Case No. IT-95-17/1-T, Trial Judgment, ¶ 243 (ICTR December 10, 1998); *see also In re Tesch*, 13 Int'l L. Rep. 250 (Brit. Mil. Ct., Hamburg, 1946) ("*Zyklon B*") (defendants convicted for providing large quantities of poisonous gas which could have been used for pest control); *The Flick Case*, 6 Trials of War Criminals (T.W.C.) 1194 (civilian industrialist convicted for contributing money to Nazis). The accused's conduct need not be a "condition precedent" to the underlying violation. *Doe v. Exxon Mobil Corp.*, Case No. 01-1357, Slip Op. at 17 (D.D.C. 2015) ("*Exxon*") (citing *Prosecutor v. Ndahimana*, Case No. ICTR-01-68-A, Appeal Judgment, ¶ 149 (ICTR December 16, 2013)); *see also* Van Schaack, Beth, "The Many Faces of Complicity in International Law," Stanford Public Law

Working Paper No. 2705086 (December 17, 2015) ("…proof of a strict 'but for' causation is unnecessary. Rather, causation has a scalar quality: what must be shown is that the accomplice's assistance made a substantial contribution to the commission of the crime")[2].

Acts of complicity can exert a substantial effect on unlawful behavior "in an infinite variety of ways." *Taylor*, ¶ 369. "An accused's acts and conduct can have a substantial effect by providing financial support to an organization committing crimes, weapons and ammunition, or by standing guard, transporting perpetrators to the crime site, establishing roadblocks," and so on. *Id*. "The acts and conduct of an accountant, architect or dentist in their respective professional roles can have a substantial effect . . . as can those of prosecutors, judges and religious officials." *Id*. Thus, various forms of conduct which would not necessarily be unlawful in and of themselves ("standing guard," "establishing roadblocks," etc.) may have a substantial effect on the commission of crimes in a particular context. It is therefore essential to place Cisco's conduct in the context of the violent religious persecution being waged by its Communist Party and Chinese security clients against Falun Gong believers, and particularly in the context of the use of Orwellian controls of the Internet and other high-tech systems to carry it out.

Both domestic courts and international tribunals provide guidance as to the application of the *actus reus* standard for complicity liability. Circumstances in which the standard is met fall into at least three categories. ***First***, in "provision of means cases," the accused provides the essential means by which the underlying violations were carried out. *See, e.g., In re South African Apartheid Litigation*, 617

[2] Available at SSRN: http://ssrn.com/abstract=2705086: or http://dx.doi.org/10.2139/ssrn.2705086.

F.Supp.2d 228, 268 (S.D.N.Y. 2009) (allegations describing "provision of the means by which the South African Government carried out" apartheid "meet the *actus reus* requirement") ("*South African Apart.*"); *Zyklon B*, 13 Int'l L. Rep. 250 (defendants convicted for providing large quantities of poisonous gas used to exterminate inmates in concentration camps); *Taylor*, ¶ 160; *Public Prosecutor v. Van Anraat*, Case No. 2200050906-2, Judgment of the Court of Appeal of the Hague, ¶ 12.5(e) (May 9, 2007) (war crimes "depended to a decisive extent if not totally on" supplies of chemicals provided by the accused) ("*Van Anraat*").

Second, in "perpetrator assistance cases," the accused's conduct supports, sustains, and enhances the capacity of the principal perpetrator to carry out the underlying violations. *See, e.g., Taylor*, ¶ 520 (the accused provided assistance which "enhanced the capacity" of the principal perpetrators to plan and facilitate military operations, obtain arms and ammunition); *Prosecutor v. Bagaragaza*, Case No. ICTR-05-86-S, Sentencing Judgment, ¶ 25 (ICTR November 17, 2009) (accused provided money for purpose of buying alcohol to motivate principal perpetrators to continue with killings) ("*Bagaragaza*"); *Prosecutor v. Rukundo*, Case No. ICTR-2001-70-A, Appeal Judgment, ¶ 176 (ICTR October 20, 2010) (defendant identified Tutsi refugees to principal perpetrators who subsequently removed and killed them) ("*Rukundo*").

Third, in "system of crimes cases," the accused provides assistance that maintains a widespread system of crimes. *See, e.g., Simic*, ¶ 116 (imposing liability where accused "worked together with" police and paramilitaries "to maintain the system of arrests and detention of non-Serb civilians"); *Prosecutor v. Brđanin*, Case No. IT-99-36-T, Trial Judgment, ¶¶ 1069, 1073-74 (ICTR September 1, 2004) (accused "aid[ed] and abet[ted] the maintenance of a system" of religious

persecution) ("*Brđanin*").[3]

Although Plaintiffs need only prevail under one of these frameworks, for the reasons provided below, Cisco's assistance had a substantial effect on the underlying violations under all of them. As a result, the district court erred in finding that Cisco's alleged conduct did not meet the required *actus reus* standard.

2. Cisco's anti-Falun Gong systems provided the essential means by which the Communist Party and Chinese security's persecutory campaign was carried out.

Cisco provided essential high-tech tools to the Communist Party and Chinese security that were used directly to carry out the widespread identification, apprehension, detention, and torture of Falun Gong believers. Where an accused provides essential means by which the underlying violations are carried out, the accused's conduct has a substantial effect on the violations. *See, e.g., South African Apart.*, 617 F.Supp.2d at 268; *Zyklon B*, 13 Int'l L. Rep. 250; *Taylor*, ¶ 160; *Van Anraat*, ¶ 12.5(e). The means provided can have dual or neutral uses. "[P]erfectly innocuous items, such as satellite phones, could be used to assist the commission of the crimes, while instruments of violence could be used lawfully. The distinction between criminal and non-criminal acts of assistance is not drawn on the basis of the act in the abstract, but on its effect in fact." *Taylor*, ¶ 395. For this reason, the district court's finding that the "product produced by Defendants – even as specifically customized – can be used for many crime-control purposes in China without permitting torture or other human rights abuses," ER 27, is not relevant and misstates the operative law.

In the landmark post-World War II *Zyklon B Case*, private economic actors

[3] The same conduct may meet one or more of these tests.

were convicted for providing large quantities of poisonous gas used to exterminate concentration camp inmates. *Zyklon B*, 13 Int'l L. Rep. 250. Plaintiffs here plausibly allege that Cisco likewise provided and tailored the anti-Falun Gong systems by which the Communist Party and Chinese security subjected Falun Gong believers in China, solely on the basis of their religious beliefs, to forced conversion through torture. These systems included an array of Falun Gong-specific features, such as "Falun Gong databases," explicitly designated as such in Cisco's designs, that store and share sensitive information about detained Falun Gong believers used directly during forced conversion (i.e. torture) sessions—their personal Internet usage, their social and economic circumstances, the leverage that can be exerted through information about family members and fellow believers, and so on. SAC ¶¶ 85, 86, 106, 111, 114, 122, 131. Cisco designed these anti-Falun Gong systems such that the Falun Gong databases were integrated into China's security infrastructure, including its police detention centers, clandestine jails, Public Security mental hospitals devoted to political opponents, and other detention and torture sites. SAC ¶ 98(h). The integration of these Falun Gong features was essential to the Communist Party's program of religious persecution and was deployed directly to carry out the specific abuses suffered by Plaintiffs. For example, during Plaintiff Wang Weiyu's detention, security officials threatened his wife and used her anonymous Internet communications with overseas Falun Gong believers to forcibly convert Wang to renounce his belief in Falun Gong. SAC ¶ 356.[4]

Cisco's anti-Falun Gong systems were used directly not only in the

[4] Similar examples related to the other named Plaintiffs are enumerated *supra* at Statement of Facts, p. 5-6.

commission of torture but also in the commission of widespread acts of religious persecution as a crime against humanity.[5] In *South African Apartheid*, the district court found that defendant technology companies substantially assisted a system of apartheid by supplying "computer equipment *designed to track and monitor civilians* with the purpose of enforcing . . . apartheid" as well as the software and hardware to run the system "used to track racial classification and movement for security purposes." 617 F.Supp.2d at 268 (emphasis added). These acts constituted the "means by which the South African Government carried out both racial segregation and discrimination." *Id*. Cisco similarly designed, implemented, and maintained anti-Falun Gong systems that were used by Communist Party and Chinese security to identify, "track and monitor" Falun Gong believers with the purpose of enforcing a widespread campaign of religious persecution. Anti-Falun Gong systems and features—unique "signatures" of Falun Gong activity, a Falun Gong Web Announcement Interface, the National Information System for Falun Gong Key Personnel—were used to identify, track, and monitor Falun Gong believers as well as to house information on the activities of this particular religious group. SAC ¶¶ 82-83, 97, 192. Chinese security used these systems to enforce the religious persecution of Falun Gong believers. For example, these systems were used directly to monitor Plaintiff Doe IX's use of the software Dongtaiwang, which allows users to evade normal Internet controls, and to track her IP address such that even her anonymous Internet activity was logged. Doe

[5] To constitute a crime against humanity, persecution must be committed as part of a "widespread or systematic attack directed against any civilian population." *Sexual Minorities Uganda*, 960 F.Supp.2d at 316. Plaintiffs plainly allege that they were targeted for widespread persecution on the basis of their religious beliefs. *See* SAC ¶¶ 36-37, 404-08.

IX's Internet use at her workplace, including the use of multiple, unconnected devices, was tracked to her specific identity. SAC ¶ 319.[6]

Cisco not only provided goods used directly to carry out crimes against Plaintiffs, it tailored its goods to meet this goal. Although the district court in *South African Apartheid* required that automotive defendants tailor their vehicles to carry out war crimes (*see* 617 F.Supp.2d at 267), such a requirement does not exist under customary international law. *See Taylor*, ¶ 395. Nonetheless, even if tailoring were required, Plaintiffs' well-pled allegations demonstrate that Cisco tailored anti-Falun Gong systems to further forced conversion through torture ("*zhuanhua*") and religious persecution ("*douzheng*"). Cisco's technology fed information stored in the Falun Gong databases to physical locations where Falun Gong believers were subjected to detention and torture, and populated the Falun Gong databases via the Internet Surveillance System and other monitoring systems that collected the sensitive information used by Communist Party and Chinese security to forcibly convert Plaintiffs and persons similarly situated through torture. SAC ¶¶ 82-86, 88, 91. Cisco tailored other features to further the religious persecution of Falun Gong believers through their identification and apprehension. SAC ¶ 97(c). In addition, customer support teams located in San Jose provided tailored services in the form of localized configuration, systems architecture and integration, troubleshooting, and training to enable Chinese security to use the anti-Falun Gong systems to subject Falun Gong believers to forced conversion and religious persecution. SAC ¶¶ 134, 143.

---

[6] Similar examples related to the other named Plaintiffs are available at SAC ¶¶ 235 (Doe I); 241 (Doe II); 252 (Ivy He); 267-68 (Doe III); 277-78 (Doe IV); 287-88 (Doe V); 295-97 (Doe VI); 301-02 (Doe VII); 311-12 (Doe VIII); 322-25 (Charles Lee); 334, 343 (Liu Guifu); 347-51 (Wang Weiyu).

Some domestic courts have suggested that the ATS should not be used to impose liability on private companies for engaging in ordinary, arms-length commercial transactions with human rights abusers. *See, e.g., Nestle*, 766 F.3d at 1025 ("[d]oing business with child slave owners, however morally reprehensible," is not sufficient); *South African Apart.*, 617 F.Supp.2d at 269 ("merely doing business with a bad actor" not sufficient). But such concerns are not present here. In an arms-length commercial transaction, a buyer places an order for a standard product, which the seller ships out, concluding the transaction.

This arrangement is legally distinct from the present case in several ways. First, Cisco went through a lengthy bidding process to persuade its clients that it was the best company to meet the Communist Party and Chinese security's specific goals, thus requiring extensive research by Cisco into these goals, as well as a massive marketing campaign to convince them that Cisco could offer an effective hardware and software solution. *See* SAC ¶¶ 58-74. Second, Cisco did not simply ship out a few devices. It designed an end-to-end custom architectural solution to meet the Communist Party's and Chinese security's goals. *See* SAC ¶¶ 3-4, 75-95. Third, as noted directly above, this solution includes features and devices tailored to target Falun Gong believers. *See* SAC ¶¶ 83, 97(a). Fourth, Cisco did not passively fill orders placed by its clients. It recommended features and services to facilitate its clients' anti-Falun Gong goals, including first-of-its-kind designs, and provided training and customer service on how to use its anti-Falun Gong features. *See* SAC ¶¶ 76, 97(b)-(c), 134, 143, 181. Fifth, Cisco's work on the Golden Shield was such a major priority for Cisco that its top executives developed personal relationships with high-ranking Communist Party officials built upon Cisco's commitment to meeting anti-Falun Gong objectives to advance

its business. *See* SAC ¶¶ 58, 133. And sixth, this multifaceted business relationship between Cisco and the Communist Party and Chinese security went on for many years. *See* SAC ¶¶ 103, 107. Together, these allegations make clear that Cisco's conduct went well beyond an ordinary, arms-length commercial transaction in which a company simply does business with a known human rights violator.

3. Cisco's conduct supported, sustained, and enhanced the Communist Party's and Chinese security's capacity to carry out its violent persecutory campaign against Falun Gong.

The *actus reus* of complicity liability is also established where the accused's conduct supported, sustained, and enhanced the capacity of the principal perpetrator to carry out the underlying violations. *See Taylor*, ¶ 520; *Bagaragaza*, ¶ 25; *Rukundo*, ¶ 176. Such an approach dates back to the post-World War II tribunals. *See The Einsatzgruppen Case*, 4 T.W.C. 569 (1948); *United States v. Pohl*, 5 T.W.C. 958 (1947). Together, these cases make clear that even if the accused did not provide material used directly in the commission of the crimes, and even if the alleged conduct would be lawful in a different context, assistance that enhances the capacity of the principal perpetrator to carry out the underlying violations has the required substantial effect to ascribe liability as an accomplice.

Cisco's assistance here was of the sort international tribunals have found to constitute aiding and abetting. For example, in *Einsatzgruppen*, defendant Klingelhofer was convicted for "locating, evaluating and turning over lists of Communist party functionaries to the executive department of his organization." 4 T.W.C. 569. And in *Rukundo*, the defendant identified Tutsi refugees to soldiers and others, thus enhancing the capacity of the soldiers to remove and kill the refugees. *Rukundo*, ¶ 176. Similarly, Cisco, acting in San Jose, designed and

managed the implementation of a high-tech system to identify the targets of the Communist Party and Chinese security's violent religious persecution. SAC ¶¶ 80, 97(c), 98-101. If turning over a list of specific individuals to be targeted for abuse has a substantial effect on the crimes, then surely designing and implementing a high-tech system that identifies massive numbers of Falun Gong believers for abuse by scouring the Internet for their Falun Gong-related activity also has a substantial effect on the subsequent abuse of the individuals identified.

In *Taylor*, the accused provided "sustained and significant communications support," such as satellite phones, to "enhance [the] communications capability" of the principal perpetrators, as well as the "capacity to plan, facilitate and order" military operations during which crimes were committed. *Taylor*, ¶¶ 326, 332. Similarly, Cisco conceived and created a system that enabled the Communist Party and Chinese security to share, analyze, and use information on Falun Gong believers efficiently and securely throughout China's security infrastructure, including police detention centers, clandestine jails, Public Security mental hospitals devoted to political opponents, and other detention and torture sites. SAC ¶¶ 85, 86. Thus, even apart from the demonstrated direct connection between the anti-Falun Gong systems and the torture of Plaintiffs, Cisco provided technological solutions—in the form of hardware and software—and assistance that enhanced the capacity of the Communist Party and Chinese security to carry out widespread prolonged and arbitrary detention and torture, thus having a substantial effect on the commission of these and other human rights abuses.[7]

[7] Moreover, in *Taylor*, the SCSL emphasized that the accused provided assistance at a "critical time" in the principal perpetrators' military effort. *Id*. ¶ 514. Similarly, Cisco here provided its assistance at a critical time, when the Communist Party otherwise lacked the technological sophistication to develop these anti-Falun Gong

4. Cisco's conduct undergirded and maintained the Communist Party and Chinese security's widespread system of crimes.

The required *actus reus* for complicity liability can also be established where the accused provides assistance which maintains a system of crimes. *See Simic*, ¶ 116; *Brđanin*, ¶ 1073-74. "In terms of the effect of an accused's acts and conduct on the commission of the crime through his assistance to a group or organization, there is a readily apparent difference between an isolated crime and a crime committed in furtherance of a widespread and systematic attack on the civilian population." *Taylor*, ¶ 391. The substantial effect that Cisco's conduct had here on the underlying violations is particularly clear when viewed in the context of the Communist Party and Chinese security's widespread *system* of violent religious persecution against Falun Gong believers.

In *Simic*, the accused "worked together with the police [and] paramilitaries" to "maintain the system of arrests and detention of non-Serb civilians," thus lending substantial assistance to these unlawful acts. *Simic*, ¶ 116.[8] The Tribunal reached this conclusion despite the fact that the accused "had no authority over the police" who committed the crimes. *Id*. at ¶ 114. Similarly, Cisco deliberately

---

systems and when Falun Gong believers in the country were using their own technology tools to circumvent Communist Party and Chinese security controls on the Internet. *See* SAC ¶¶ 3, 76, 94. Without Cisco's systems in place at this time, the Communist Party could not have profiled, investigated, located, apprehended, detained, or forcibly converted and tortured Plaintiffs or other Falun Gong believers on a widespread basis.

[8] This analysis pertained to the accused's liability for the crime against humanity of persecution, specifically the unlawful arrest and detention of Bosnian Muslim and Bosnian Croat civilians. *Simic*, ¶ 4. Thus, liability should be imposed not only for torture but for Cisco's role in maintaining a widespread system of wrongful arrest and detention of Falun Gong believers on the basis of their religion.

entered into collaboration with Communist Party and Chinese security leaders to carry out the religious persecution and forced conversion of Falun Gong believers in China. SAC ¶ 150. Cisco acknowledged on its website that it constructed the Golden Shield in "full collaboration" and "partnership" with Chinese security in provinces and regions across China, and that its Golden Shield designs are tailored to their specific needs and requests. SAC ¶¶ 153-55. For over a decade, Cisco's American executives and engineers worked together with Chinese security to design anti-Falun Gong systems in a manner that would maintain the system of violent religious persecution waged against Falun Gong believers in China. *See also* SAC ¶¶ 58, 107, 133, 196-200.

In *Brđanin*, the accused issued decisions that non-Serbs should disarm, which made non-Serb civilians more vulnerable. *Brđanin*, ¶¶ 469, 528, 663, 673, 1056. Similarly, Cisco provided upgrades to the Golden Shield to "'catch' Falun Gong believers who were themselves using ever more advanced methods to escape detection and persecution" and in other ways furthered their round up and widespread wrongful detention. SAC ¶¶ 9-21, 94-97. In the same way that Brđanin's actions left the civilian population vulnerable to crimes carried out by others, Cisco provided features that stripped Falun Gong believers of any significant protection against the Communist Party and Chinese security's Orwellian Internet surveillance and left them exposed to more severe abuse.

Importantly, Cisco's conduct need not have "played a direct role in each crime." *Taylor*, ¶ 374. The *Brđanin* Trial Chamber focused on "the cumulative effect" of the accused's acts on "the ability" of the principal perpetrators' to carry out the crimes. *Id*. (citing *Brđanin*, ¶ 476). Here, the cumulative effect of Cisco's conduct is clear. "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 [Plaintiffs] in the same manner, or at all." SAC ¶ 225. This effect on the ability of the Communist Party and Chinese security to wrongfully arrest, detain, and torture Falun Gong believers in large numbers is further established by the circumstances in which the specific Plaintiffs were identified and tracked through use of the Golden Shield. *See* SAC ¶¶ 235, 241, 252, 267-68, 277-78, 287-88, 295-97, 301-02, 311-12, 319, 322-25, 334, 343, 347-51.

For all of the reasons stated above, Plaintiffs' allegations permit the plausible inference that Cisco's conduct had a substantial effect on the underlying abuses.

B. Cisco Possessed the Requisite *Mens Rea* for Aiding & Abetting Liability.

In evaluating whether Cisco possessed the necessary *mens rea* for complicity liability, the district court adopted the correct legal standard, but then misapplied it to the facts. In finding that the requisite *mens rea* for aiding and abetting liability was not established by Plaintiffs' allegations because they did not show that Cisco "knew that [its] product would be used beyond its security purpose – the apprehension of individuals suspected of violating Chinese law," ER 27, the court ignored or misunderstood Plaintiffs' well-pled allegations, which permit a plausible inference that Cisco knew that its conduct would specifically facilitate the Communist Party's campaign of violent religious persecution against Falun Gong believers, including their widespread torture.

This Court, in assessing Plaintiffs' claims, should first determine that a *mens rea* of "knowledge" is required for aiding and abetting liability under customary international law, an issue that this Court did not resolve in *Nestle*. But regardless

of whether the Court applies a standard of "knowledge" or "purpose," Plaintiffs' allegations are sufficient to establish the requisite *mens rea*.

1. Customary international law requires a *mens rea* of "knowledge" for aiding and abetting liability.

When choosing between competing legal standards for an ATS claim, courts "consider which one best reflects a consensus of the well-developed democracies of the world." *Nestle*, 766 F.3d at 1023 (citing *Sosa*, 542 U.S. at 732). This Circuit has declined to decide whether aiding and abetting liability requires a showing of "knowledge" or "purpose." *Id*. at 1024. Importantly, however, the Court noted that a knowledge standard "dates back to the Nuremberg tribunals" and has been "embraced by contemporary international tribunals." *Id*. at 1023. Indeed, all international tribunals, from Nuremberg to the Special Court of Sierra Leone, have applied a knowledge standard. *See, e.g., Zyklon B*, 13 Int'l L. Rep. 250; *Prosecutor v. Tadic*, Case No. IT-94-1-A, Appeal Judgment, ¶ 229 (ICTY July 15, 1999); *Prosecutor v. Stanisic and Simatovic*, Case No. IT-03-69-A, Appeal Judgment, ¶ 104 (ICTY December 9, 2015); *Prosecutor v. Kayishema*, Case No. ICTR-95-1-T, Trial Judgment, ¶ 205 (ICTR May 21, 1999); *Prosecutor v. Sesay*, Case No. SCSL-04-15-A, Appeal Judgment, ¶ 546 (SCSL October 26, 2009).

Article 25(3)(c) of the Rome Statute, which states that a person shall be liable if that person "[f]or the purpose of facilitating the commission of such a crime, aids, abets, or otherwise assists in its commission," does not dictate otherwise. Much of the Rome Statute, particularly Article 25(3)(c), "was not intended to codify existing customary rules." *See* David Scheffer and Caroline Kaeb, *The Five Levels of CSR Compliance: The Resiliency of Corporate Liability under the Alien Tort Statute and the Case for a Counterattack Strategy in Compliance Theory*, 29 Berkeley J. Int'l L. 334 (2011). *See also Prosecutor v.*

Oric, Case No. IT-03-68-A, Appeal Judgment, Judge Schomburg Opinion, ¶ 20 (ICTY July 3, 2008). Even if it were, such codification is "not dispositive and do[es] not override the cumulative weight of other evidentiary sources." Chimene I. Keitner, *Conceptualizing Complicity in Alien Tort Cases*, 60 HASTINGS L.J. 61, 88 (Nov. 2008). Thus, a knowledge standard "best reflects a consensus of the well-developed democracies of the world." *Nestle*, 766 F.3d at 1023.

2. The *mens rea* standard requires well-pled allegations that the defendant was aware of the likely consequences of his conduct, not proof that he specifically intended those consequences.

Customary international law dictates that a defendant is liable for aiding and abetting if he or she was aware of the "substantial likelihood that his acts would assist the commission of a crime." *Sesay*, ¶ 546. It is not required that the defendant intended, willed, or desired those consequences. *Id*.

Nor must a defendant have certain knowledge that a particular crime will be committed as a result of his assistance. *Id*. A defendant need only be "aware that one of a number of crimes will probably be committed, and one of those crimes is committed." *Exxon*, Slip Op. at 19 (citing *Prosecutor v. Popovic*, Case No. IT-05-88-A, Appeal Judgment, ¶ 1732 (ICTY January 30, 2015); *Prosecutor v. Karera*, Case No. ICTR-01-74-A, Appeal Judgment, ¶ 321 (ICTR February 2, 2009)). A defendant does not need to know "every detail of the crime that was eventually committed." *Exxon*, Slip Op. at 19 (citing *Prosecutor v. Sainovic*, Case No. IT-05-87-A, Appeal Judgment, ¶ 1773 (ICTY January 23, 2014)). "Knowledge of the same or similar actions in the past by the principal perpetrator is sufficient" to establish this knowledge. *Id*. (citing *Popovic*, ¶ 1734). The accused need not know that the effect his acts would have on the commission of the crimes would be substantial. *Taylor*, ¶ 439. Constructive knowledge is also sufficient. *Doe I v.*

Unocal Corp., 395 F.3d 932, 953 (9th Cir. 2002) (*vacated on other grounds*); *see also Prosecutor v. Furundzija*, Case No. IT-95-17/1-T, Trial Judgment, ¶ 245 (ICTY December 10, 1998) (determinative question is whether "a driver would reasonably have known that the purpose of the trip was an unlawful execution").

3. Plaintiffs' allegations plausibly demonstrate that Cisco knew that its conduct would further objectives beyond legitimate law enforcement.

Plaintiffs' allegations adequately support a plausible inference that Cisco knew that its conduct would assist the crimes committed against Plaintiffs by Cisco's clients. Such an inference may be drawn on the basis of (1) the nature of the assistance Cisco provided; (2) Cisco's own admissions of its knowledge of religious persecution against Falun Gong believers; (3) widespread publicity and news coverage of the widespread human rights abuses against Falun Gong believers; and (4) Cisco's management structure and business model.

First, the nature and scope of Cisco's assistance permits a plausible inference of the required knowledge. Knowledge has been proven in this way since the jurisprudence of the World War II tribunals. For example, in *Pohl*, defendant Kiefer, an architect who planned and supervised the construction of concentration camps, was found to have possessed the requisite knowledge because "the very nature of such installations and their continued maintenance constituted knowledge of the purposes for which they were used." 5 T.W.C. 995, 1019. Here, Cisco's work on the anti-Falun Gong systems required an intimate knowledge of its intended end use. SAC ¶ 77. The Golden Shield is unlike other security operations in China or elsewhere. It is "not an ordinary crime control apparatus;" it differs "from all previous crime control initiatives in scale, complexity, intelligence, and technological sophistication," and contains a unique "system of Falun Gong specific features." SAC ¶¶ 2, 5. This is made clear by Cisco's designs, developed

and created in San Jose. SAC ¶¶ 95, 127, 129. These designs explicitly diagram and discuss features and systems such as an "Internet Surveillance System" developed and used to persecute (*douzheng*) Falun Gong; and Falun Gong databases developed and used to subject believers to forced conversion (*zhuanhua*). Other anti-Falun Gong systems were developed and used specifically to enable *douzheng* through surveillance, tracking, and identification of Falun Gong believers. SAC ¶¶ 82-85, 88, 91, 134, 143.

The designs further support a plausible inference of Cisco's awareness of the substantial likelihood that its conduct would specifically assist torture. Cisco's designs featured customized digital "Falun Gong" signatures. These signatures, marketed by Cisco as the best in the industry, are able to identify pictorial information unique to Falun Gong believers which depict the persecutory nature of the campaign, as distinct from propaganda and other information promulgated about Falun Gong by Party media and others. SAC ¶¶ 80, 97(c). Cisco could not develop these "signatures" without an in-depth analysis of their content, including graphic depictions of the torture and religious persecution of believers. SAC ¶¶ 97(c), 127, 131. Cisco also tailor-designed the Falun Gong systems to comprise such Falun Gong-specific features as the Falun Gong databases that store and share sensitive information about detained Falun Gong believers—their personal Internet usage, their social and economic circumstances, the leverage that could be exerted through information about family members and fellow believers—which was used directly during forced conversion (i.e. torture) sessions. SAC ¶¶ 85, 86, 106, 111, 114, 122, 131. Hosting an array of information that extends beyond that collected by ordinary criminal justice systems of the Golden Shield, these databases store a "lifetime profile" of each identified Falun Gong believer, which is used to

psychologically intimidate them, extract false confessions, and devise strategies for successive rounds of forced conversion based on past behavior. SAC ¶ 100-01. By integrating the Falun Gong databases to the "Internet Surveillance System," which identifies and tracks Falun Gong believers' Internet activities, Cisco's technology fed sensitive and tailored information on detainees used during interrogation, forced conversion, and torture sessions to Chinese security. SAC ¶¶ 82-85, 88, 91. Cisco further integrated these Falun Gong databases into China's anti-Falun Gong security infrastructure, including its police detention centers, clandestine jails, Public Security mental hospitals devoted to political opponents, and other detention and torture sites. SAC ¶ 98(h). Communist Party reports transmitted to Cisco specifically state that these features enable the forced conversion through torture of Falun Gong believers. *See* SAC ¶¶ 88-91, 117-22. For example, one report states that Falun Gong databases help "solve the problem of [Falun Gong's] forced conversion [*zhuanhua*] easily." SAC ¶ 88. Cisco's Public Security sales team deployed to China was tasked with transmitting such reports to San Jose headquarters. SAC ¶¶ 59, 145-46, 172.[9]

In *Zyklon B*, knowledge was established in part due to the sheer volume of poisonous gas provided by the accused: "the accused must have known that the large deliveries of Zyklon B could not have been made for the purpose of disinfecting the buildings." 13 Int'l L. Rep. 250. Similarly, Cisco's anti-Falun Gong systems required an unprecedented "scale", capacity", and "complexity" to

[9] Another report describes Falun Gong databases as an essential part of the system used to "deepen the *douzheng* against Falun Gong . . . to unearth all Falun Gong online information to firmly control [Falun Gong] . . . and when necessary to implement compulsory ideological conversion measures to prevent a return to their practice of their religion." SAC ¶ 117.

violently suppress Falun Gong believers across China, far more than would be needed to perform legitimate security operations. *See* SAC ¶¶ 2, 3, 99, 129. Due to the complexity and scale of the project, Cisco designed the apparatus in San Jose, sent their Advanced Service Team from San Jose to China to oversee the implementation of the apparatus, and in other ways maintained and controlled the project from San Jose. SAC ¶¶ 145-46. It is simply inconceivable that Cisco could have engaged in this conduct without awareness of the substantial likelihood that such features would facilitate the violent persecution and torture of Falun Gong believers. At the very least, a plausible inference of such knowledge can be drawn from these allegations.

Second, an accused's own admissions of knowledge of the underlying crimes can establish the required *mens rea*. *See Taylor*, ¶ 538 (defendant admitted "that by April 1998 anyone providing support to [rebel groups] 'would be supporting a group engaged in a campaign of atrocities'"). Here, Cisco has repeatedly admitted they knew that their products would further their clients' objectives, and that these objectives included religious persecution. For example, an internal Cisco PowerPoint sales presentation acknowledged in 2002 that a primary objective of the Golden Shield is to facilitate the "ongoing crackdown or *douzheng* [violent persecution] against Falun Gong." SAC ¶¶ 62, 185, 216. In May 2008, during a hearing before a U.S. Senate Committee, Cisco Senior Vice President Mark Chandler admitted that this language, which he acknowledged referred to "combat" against "hostile elements, including religious organizations," was included "by way of explaining the Chinese Government's goals." *See* U.S. Senate, Committee on the Judiciary, *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, Hearing, p. 13, May 20, 2008 (Serial No. J-

110-93); SAC ¶ 216. Cisco internal files describe this objective "as a lucrative business opportunity for the company." SAC ¶ 187. Defendants' marketing literature "reiterated Cisco's commitment to customize all their products to meet security's objectives." SAC ¶ 65. Cisco marketing at security trade shows in China similarly express their commitment to persecutory objectives. *See* SAC ¶¶ 68, 70. Another Cisco report, posted to Cisco's U.S.-based website, characterized the capacity to ensure "social stability," a coded phrase used in Cisco internal documentation to refer to the suppression of targeted groups, as a major selling point of Cisco technology. SAC ¶¶ 63, 190, 215. It can therefore be reasonably and plausibly inferred that Cisco was aware of the substantial likelihood that its conduct would assist the religious persecution of Falun Gong believers.

Third, the systematic persecution and torture of Falun Gong believers in China has been widely reported in the United States at all relevant times. A reasonable inference that Cisco knew that its conduct would have a substantial effect on the underlying crimes may be drawn on this basis. In *Nestle*, the Ninth Circuit easily concluded that the defendants were "well aware of the child slavery problem in the Ivory Coast . . . due to the many reports issued by domestic and international organizations." 766 F.3d at 1017. And in *Flick*, the tribunal convicted a businessman who contributed money to Himmler at a time when the criminal activities of the SS were "common knowledge." 6 T.W.C. 1194. Common knowledge is similarly established here on the basis of widespread reports from a variety of sources. Each year from 1999 to present, the U.S. State Department, in reports submitted to Congress, has documented and condemned the widespread religious persecution of Falun Gong believers in China. SAC ¶ 164. The State Department estimated as early as 2001 that several hundreds of thousands of Falun

Gong believers have been persecuted on the basis of their religious beliefs. SAC ¶ 48. Similar reports have been issued by the UN, the European Parliament, and international human rights organizations. SAC ¶ 165. Such reports document the widespread practice of arbitrary arrest and wrongful detention, including the ongoing practice of holding detainees in "Re-education Through Labor" camps. *Id*. U.S. new media have similarly documented this persecution. SAC ¶¶ 160-163.

Much early reporting on the crackdown focused on the severity and ubiquity of torture and other forms of severe abuse against Falun Gong. SAC ¶ 160. The widespread use of torture to forcibly convert Falun Gong believers was well documented by survivors' public statements and prominent media coverage from 1999 through the present day. SAC ¶ 173. Media reports provided graphic depictions of the torture of Falun Gong believers. Ian Johnson won a Pulitzer Prize for his 2001 coverage in the *Wall Street Journal* of the murder of a Falun Gong believer by her Communist Party jailers through "repeated jolts from a cattle prod as part of two days of torture that left her legs bruised and her short black hair matted with pus and blood." SAC ¶ 160. In "Torture is Breaking Falun Gong," the *Washington Post* provided similarly disturbing illustrations of the widespread use of forced conversion through torture practices. *Id*. Other reports have similarly provided widespread graphic documentation of the torture of Falun Gong believers in China. SAC ¶¶ 49, 159-65, 167, 173.[10]

The use of the Golden Shield apparatus in particular to further these abuses

[10] Most of these reports emphasize the alleged application of these unlawful practices in Re-education Through Labor (RTL) camps, clandestine jails, prisons, and other detention facilities in China. *See, e.g.,* SAC ¶ 173. If the Defendants were aware that apprehended Falun Gong believers were subsequently detained, they were also, *ipso facto*, aware that they would be subjected to torture and other crimes against humanity.

has also been reported widely by western media outlets, the U.S. government, the UN, and international human rights organizations since 1999. SAC ¶ 51. *See, e.g.,* Reporters Without Borders, "Living dangerously on the Net," *Censorship and Surveillance of Internet forums* (May 12, 2003)[11]; Amnesty International, "People's Republic of China: Controls tighten as Internet activism grows" (January 28, 2004)[12]; Richard C. Morais, "Cracks in the Wall," *Forbes* (January 27, 2006)[13].

In addition, U.S. courts regularly grant asylum claims on behalf of Falun Gong believers in light of the system of religious persecution against them in China. *See, e.g., Yun Wang v. Holder*, 493 Fed.Appx. 476, 480 (4th Cir. 2012); *Shan Zhu Qiu v. Holder*, 611 F.3d 403, 407 (7th Cir. 2010). And from 2003-04, in San Jose and northern California more generally, there were media reports about an ongoing lawsuit in the Northern District of California against former Beijing mayor Liu Qi, who was found liable for the torture and prolonged wrongful detention of several Falun Gong plaintiffs in that case. SAC ¶ 167.

Fourth, Defendants' management structure and business model permit the plausible inference that Defendants possessed the required knowledge. In *Zyklon B*, the tribunal concluded that "the real strength of the Prosecution in this case . . . rests upon the general proposition that, when you realize what kind of man [the defendant] was, it inevitably follows that he must have known every little thing about his business." 13 Int'l L. Rep. 250. Similarly, as alleged in the SAC, Cisco's management structure and business model plausibly support the inference that

[11] Available at URL: http://en.rsf.org/china-living-dangerously-on-the-net-12-05-2003,06793.html.
[12] Available at URL: http://www.amnesty.nl/nieuwsportaal/pers/controls-tighten-internet-activism-grows.
[13] Available at URL: http://www.forbes.com/global/2006/0227/018A.html.

Cisco knew the Golden Shield would assist violent religious persecution and torture of the targets of their clients' surveillance. Cisco's entire business model is based on providing end-to-end "solutions" for its client, a term it uses to describe "a comprehensive, well-integrated set of products and services designed specifically to eliminate their customers' specific 'problem.'" SAC ¶ 4. Cisco assigned its "Advanced Services Team," a specialized service provided by its San Jose headquarters for large-scale projects and important clients, to work on the Golden Shield in China, conducting assessments and planning based on the clients' goals, post-product maintenance, testing and verification, and training and support. SAC ¶¶ 145-46. Cisco set up a Cisco Public Security sales team "specifically to ascertain and help Cisco meet Chinese security objectives," including hiring consulting agencies to research these objectives. SAC ¶ 59. This team "was tasked with accessing and sharing with company superiors" all information about the Golden Shield, including reports on its persecutory objectives and the use of features to assist torture. SAC ¶¶ 88-91. More generally, the apparatus could not be designed, implemented, and serviced by Cisco without a deep understanding of the purposes for which it would be used. SAC ¶¶ 77, 87, 134, 182. The intensive, end-to-end nature of Cisco's work on this project renders it virtually impossible that Cisco did not know its violent persecutory purposes.

Plaintiffs' allegations, taken together, permit a plausible inference that Cisco knew its conduct would assist the religious persecution and torture of Plaintiffs.

4. If applied, the purpose standard only requires that the accused act with the purpose of facilitating a crime, not that the accused desired the crime's commission.

As noted *supra* at I(B)(1), much of the Rome Statute, particularly Article 25(3)(c), does not reflect customary international law. *See Oric*, ¶ 20. Even if this

Circuit were to reject the existing jurisprudence in favor of a knowledge standard and instead apply a purpose standard drawn from the Rome Statute, this standard does not require specific intent to bring about a particular consequence. Rather, the Rome Statute would only require that the accused act with the purpose of *facilitating* the underlying violation.

Nothing in the Rome Statute can be read to require that the defendant act with specific intent or that the defendant share the same intent as the principal perpetrator. *See Doe I v. Nestle USA, Inc.*, 738 F.3d 1048, 1049 (9th Cir. 2013) (*vacated by* 766 F.3d 1013); *South African Apart.*, 617 F.Supp.2d at 262. Article 25(3)(c) of the Rome Statute merely requires that a person act "[f]or the purpose of facilitating the commission" of a crime. Rome Statute, art. 25(3)(c). Even under the Rome Statute, "'intent' does not require that an aider or abettor share the primary actor's purpose." *South African Apart.*, 617 F.Supp.2d at 262. Notably, while the Ninth Circuit in *Nestle* held that the plaintiffs' allegations met a purpose standard, nowhere did the Court require or find that the defendants acted with the same intent as the principal perpetrators, or with a specific intent to further child slavery. The plaintiffs there "conceded that the defendants did not have the subjective motive to harm children." 766 F.3d at 1025.

Rather than requiring what is known as "specific intent" at common law, the reference to "purpose" in Article 25(3)(c) of the Rome Statute is explicitly attached to the accused's "facilitation" of the commission of a crime. Rome Statute, art. 25(3)(c). In this context, purpose refers to the act of the accused that would facilitate the crime. For example, if an arms trader sells arms to a dictator, "purpose to facilitate" refers to the purpose to sell arms, not a purpose to achieve the consequences the dictator intends to achieve with those arms. While Article

25(3)(c) is silent as to the *mens rea* required for the consequences or outcome of the crime, such a standard is found in Article 30 and requires only "aware[ness] that [the consequence] will occur in the ordinary course of events." Rome Statute, art. 30.[14] Thus, even ignoring Art. 25(3)(d)(ii)'s "knowledge" standard, the Rome Statute at most constructs a "dual intent" doctrine: the accused must act with the purpose to facilitate the crime and be aware the crime will be committed in the ordinary course of events, but need not intend for the crime to be committed or desire the victims be harmed. The drafting history of the Rome Statute confirms this reading. *See* James G. Stewart, "An Important New Orthodoxy on Complicity in the ICC Statute?", January 21, 2015.[15] This reading is preferred by the vast majority of international law scholars, and is consistent with customary international law. *See id*.; *Sesay*, ¶ 546; Scheffer and Kaeb, 29 Berkeley J. Int'l L. at 357.

5. Plaintiffs' allegations plausibly demonstrate that Cisco acted with the purpose of facilitating the religious persecution of Falun Gong.

Plaintiffs' allegations are easily sufficient to allow a plausible inference of purpose under the Rome Statute, if that is the standard required by this Court. First, there is no dispute that Cisco intentionally carried out the acts that Plaintiffs allege facilitated the underlying violations: providing high-tech devices, features, and designs for the Golden Shield. Second, for the reasons noted above at I(B)(2), Cisco knew the consequence of these actions would be the violent religious persecution, i.e., *douzheng*, of Falun Gong believers in China and their subjection

[14] Courts must look to the "text of the treaty as a whole in order to interpret its meaning." *South African Apart.*, 617 F.Supp.2d at 262 n. 180.
[15] Available at URL: http://jamesgstewart.com/the-important-new-orthodoxy-on-complicity-in-the-icc-statute/.

to torture and other crimes against humanity.

This conclusion is consistent with the Ninth Circuit's analysis in *Nestle*. There, the Court held that a plausible inference of purpose could be drawn because the defendants "obtained a direct benefit" from the use of child slavery, namely products at drastically reduced cost. 766 F.3d at 1024. Here, gaining a stronghold in the Golden Shield market "required the design, development, and promotion of technology specifically tailored for" persecutory purposes. SAC ¶ 56. Cisco therefore obtained the direct benefit of a new and lucrative client base in China based solely on the marketing, design, servicing, and implementation of goods and services that could be and were used to further torture and religious persecution. *See* SAC ¶¶ 55, 58, 126, 135, 187, 193. According to its own reporting, Cisco China accounted for $900 million in earnings for 2008 and sought to reach $7 billion in earnings for 2013. *See* SAC ¶¶ 168, 196. As in *Nestle*, Cisco "placed increased revenues before basic human welfare." 766 F.3d at 1024. Thus, it can be plausibly inferred that Cisco acted with the purpose of facilitating violent religious persecution and torture in order to win Golden Shield contracts and gain a profit, heedless of the consequences for thousands of Falun Gong believers in China.[16]

Moreover, Plaintiffs' allegations here are distinct from, and more fulsome than, cases in which a purpose standard was not met. In *Presbyterian Church of Sudan v. Talisman Energy, Inc.*, 582 F.3d 244 (2d Cir. 2009), for example, the underlying violations "ran contrary to the defendant's goals in the area, and even

[16] While the Ninth Circuit in *Nestle* found that the defendants' "control over the Ivory Coast cocoa market further supports" a showing of purpose, nowhere did it suggest that such a showing was required. Indeed, customary international law makes clear that "it is not necessary as a matter of law to establish whether [the accused] had any power to control those who committed the offenses." *Taylor*, ¶ 370 (quoting *Sesay*, ¶ 541).

forced the defendant to abandon its operations." *Nestle*, 766 F.3d at 1024 (citing *Talisman*, 582 F.3d at 262). And in *Aziz v. Alcolac, Inc.*, 658 F.3d 388 (4th Cir. 2011), the defendants had nothing "to gain from the use of chemical weapons." *Nestle*, 766 F.3d at 1024 (citing *Aziz*, 658 F.3d at 394, 401). Here, by contrast, Cisco benefitted from the persecutory campaign against Falun Gong believers, as noted immediately above.[17]

For these reasons, Plaintiffs' allegations permit a plausible inference that Cisco possessed the required *mens rea*.

II. PLAINTIFFS' CLAIMS ARE NOT BARRED BY THE PRESUMPTION AGAINST EXTRATERRITORIALITY.

Cisco is a U.S. company whose U.S. employees carried out essential conduct in the United States. Cisco deployed agents from the United States to implement the Golden Shield's anti-Falun Gong features. The company and its leadership were in constant contact with its agents and instrumentalities in China, and developed close relationships with the ultimate client, the Communist Party and Chinese security. Dismissal on extraterritoriality grounds would run counter to the purpose of the doctrine as established in *Kiobel*. It would also directly conflict with U.S. foreign policy, because all three branches of the U.S. government have consistently condemned the abuses at issue here.

Nevertheless, the district court held that Plaintiffs' claims were barred under the presumption against extraterritoriality because there was "not a sufficient

[17] In addition, the plaintiffs in *Aziz* set forth only a single allegation pertaining to purpose: that the defendant placed a chemical "into the stream of international commerce with the purpose of facilitating the use of said chemicals" to be used, among other things, against civilians. 658 F.3d at 401. This stands in sharp contrast to the plethora of factual allegations showing that Cisco benefitted from its ongoing involvement in the Golden Shield market. *See* SAC ¶¶ 55, 58, 126, 187.

showing" that Plaintiffs' claims sufficiently "'touch and concern' the United States'" ER 24 (quoting *Kiobel*, 133 S.Ct. at 1669). In so ruling, the district court erroneously adopted in large part an approach advanced in Justice Alito's *Kiobel* concurrence, even though Justice Alito himself recognized his concurrence advocated a "broader" bar than the majority actually adopted. 133 S.Ct. at 1669 (Alito, J., concurring). The district court went even further than Justice Alito, requiring that all of the underlying violations be "planned, directed, or executed in the United States." ER 25. The district court's stringent requirements are inconsistent with the majority in *Kiobel* and conflict with this Circuit's decision in *Nestle*, which explicitly rejected Justice Alito's approach and did not require those plaintiffs to prove domestic "planning or directing" on the part of the defendants. 766 F.3d at 1028.

While this Circuit has not yet adopted a precise standard, existing precedent indicates that courts should examine all of the surrounding facts and circumstances and undertake a multi-factor analysis of relevant connections to the United States to determine whether a claim touches and concerns the United States with sufficient force to displace the presumption against extraterritoriality. *See Mujica v. AirScan Inc.*, 771 F.3d 580, 594 (9th Cir. 2014); *Al Shimari v. CACI Premier Technology, Inc.*, 758 F.3d 516, 527 (4th Cir. 2014). Alternatively, even if this Court were to reverse course, adopt Justice Alito's approach, and require that the Defendants' domestic conduct by itself be sufficient to aid and abet the underlying violations, it should reject the district court's unduly circumscribed version of Justice Alito's test. Plaintiffs' claims would satisfy Justice Alito's test because the Defendants aided and abetted abuses from the United States. Plaintiffs' claims are therefore not barred by the presumption against extraterritoriality.

A. The District Court's Extraterritoriality Analysis Is Inconsistent with Both *Kiobel* and This Circuit's Analysis.

The Supreme Court in *Kiobel* held that the "principles underlying the presumption against extraterritoriality" constrain courts exercising their power under the ATS. 133 S.Ct. at 1665. But the Court left room for claims to proceed where "some of the activity underlying [an] ATS claim took place in the United States." *Nestle*, 766 F.3d at 1028; *see Mujica*, 771 F.3d at 594 (9th Cir. 2014); *Kaplan v. Central Bank of Islamic Republic of Iran*, 961 F.Supp.2d 185, 205 (D.D.C. 2013).

The Supreme Court did not purport to determine the precise circumstances when ATS claims for violations occurring abroad are actionable. At least seven Justices made clear that the Court was intentionally leaving open important questions about when violations arising abroad sufficiently "touch and concern" the United States. *See Kiobel*, 133 S.Ct. at 1669 (Kennedy, J., concurring) (opinion "is careful to leave open a number of significant questions"); *id*. (Alito, J., concurring) (the majority's "formulation obviously leaves much unanswered"); *id*. at 1673 (Breyer, J., concurring) (decision "leaves for another day the determination of just when the presumption against extraterritoriality might be 'overcome'"). The Court ruled only under what circumstances "a court may *not* recognize a cause of action under the ATS – that is, when the claim involves a foreign plaintiff suing a foreign defendant where 'all relevant conduct' occurred on foreign soil." *Doe v. Drummond Co., Inc.*, 782 F.3d 576, 585 (11th Cir. 2015) (emphasis in original) (citing *Kiobel*, 133 S.Ct. at 1669).

Only Justices Alito and Thomas concluded that the ATS's reach should be limited to domestic tortious conduct, advocating for a stricter standard than the majority adopted. *See Kiobel*, 133 S.Ct. at 1169-70 (Alito, J., concurring). "[T]he

standard proposed by Justice Alito . . . is far more circumscribed than the majority opinion's." *Al Shimari*, 758 F. 3d at 527.[18] According to Justices Alito and Thomas, courts should apply a stringently circumscribed version of the "focus" test from in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 130 S.Ct. 2869 (2010), in which the presumption against extraterritoriality is displaced "if the event or relationship that was 'the "focus" of congressional concern' under the relevant statute takes place within the United States." *Kiobel*, 133 S.Ct. at 1670 (Alito, J., concurring) (quoting *Morrison*, 130 S.Ct. at 2884). Applied in the ATS context, a putative cause of action would in their estimation be barred "unless the domestic conduct is sufficient to violate an international law norm." *Id*.

The district court explicitly followed the approach advocated by Justices Alito and Thomas in Justice Alito's concurring opinion in *Kiobel*. *See* ER 24 ("[t]he domestic conduct of the Defendants is not, as set forth by Justices Alito and Thomas, 'sufficient to violate an international law norm'") (quoting *Kiobel*, 133 S.Ct. at 1670 (Alito, J., concurring)). But such an approach is not consistent with the majority's view in *Kiobel* and this Circuit's decision in *Nestle*. In *Nestle*, this Circuit held that *Kiobel* "did not incorporate" the "focus" test on which Justices Alito and Thomas relied, and that such a test "cannot sensibly be applied to ATS claims." 766 F.3d at 1028. In doing so, the Ninth Circuit rejected the entire rationale for the Alito-Thomas approach. Thus, the district court's grounds for holding that the claims were barred – that the "domestic conduct" is not "sufficient

[18] *Kiobel* did not adopt any bright-line rule that the underlying *Sosa* violation must occur within U.S. territory, giving no indication that it intended to overturn *Filartiga v. Pena-Irala*, 630 F.2d 876 (2d Cir. 1980), and its progeny, which the Court had previously endorsed and which involved torture committed entirely abroad. *See Sosa*, 542 U.S. at 732.

to violate an international law norm," ER 24 – fatally undermines its analysis.

Moreover, the district court applied an extreme version of the Alito-Thomas concurrence, requiring that a defendant "plan, direct, or commit" the alleged human rights violations in the United States to meet *Kiobel's* "touch and concern" test, drawing from an incorrect reading of dicta in *Sexual Minorities Uganda*, 960 F.Supp.2d at 322.[19] ER at 23-24. The "relevant conduct" of a defendant under the "focus" test includes conduct "aiding and abetting" a violation. *Balintulo*, 796 F.3d at 166. There is no basis for concluding that aiding and abetting requires that the accused "plan" or "direct" the underlying violation. *See supra* at I(A)(1). Nor would the Ninth Circuit have remanded in *Nestle* to allow plaintiffs to amend their complaint if the Court had a "planning or directing" requirement in mind.[20] Thus, the district court's analysis below is not even a consistent application of the Alito-Thomas concurrence.

---

[19] In looking to answer the "relevant question" of "whether Plaintiff has alleged that substantial practical assistance was afforded to the commission of the crime . . . from the United States," the district court in *Sexual Minorities Uganda* considered in part allegations showing that the defendant "plann[ed] and manag[ed] a campaign of repression" from the United States. 960 F.Supp.2d at 322-23. But nowhere did the court hold that such facts are *required* to establish that defendants offered "substantial practical assistance" or for the claims to sufficiently "touch and concern" the United States. Accordingly, this district court's reliance on this language to *require* a stronger showing of domestic planning, direction, or execution in the United States is erroneous.

[20] Amendment would have been futile in *Nestle* under a "planning or directing" requirement. Defendants in *Nestle* "do not own cocoa farms themselves;" they buy and sell cocoa through agreements with intermediate suppliers. 766 F.3d at 1017. None of plaintiffs' allegations there comes close to suggesting that the defendants dictated, planned, or directed a policy of child slavery. Plaintiffs' amendment of their claims is not likely to alter the basic facts. Thus, if this Circuit had wished to impose a planning or directing requirement, it would have simply dismissed the case outright.

For these reasons, the district court's extraterritoriality holding is fatally flawed.

B. The *Kiobel* Presumption Is Displaced Here Under A Fact-Intensive Inquiry And Because Cisco Aided And Abetted The Underlying Violations From The United States.

Plaintiffs' claims touch and concern the territory of the United States with sufficient force to overcome the presumption against extraterritoriality as required by *Kiobel*. First, the Ninth Circuit should, consistent with its opinions in *Nestle* and *Mujica*, undertake the fact-intensive inquiry set forth in *Al Shimari*, 758 F.3d at 527. Under such an inquiry, Plaintiffs allege many facts showing a sufficient nexus between Plaintiffs' claims and the United States. Alternatively, even if this Court were to reverse course and require that Cisco's domestic conduct by itself be sufficient to aid and abet the underlying violations, Plaintiffs' claims would meet this test.

1. The *Kiobel* presumption is displaced under a fact-intensive inquiry.

Kiobel's holding was limited only to "foreign-cubed" cases where a foreign plaintiff makes claims against a foreign defendant for conduct committed on foreign soil. 133 S.Ct. at 1669. Because this case involves American defendants who committed relevant conduct on U.S. soil, the Court should engage in a more intensive analysis to determine whether Plaintiffs' claims touch and concern the United States with sufficient force. *Id*. In making this determination, the Fourth Circuit has held that courts should evaluate the broad factual circumstances surrounding the claim to determine if there is a sufficient nexus between the claim and the United States. *See Al Shimari*, 758 F.3d at 527. District courts have undertaken a similar analysis. *See Kaplan*, 961 F.Supp.2d at 205; *Mwani v. Bin*

Laden, 947 F.Supp.2d 1, 5 (D.D.C. 2013). Moreover, this Circuit has suggested a similar approach. *See Mujica*, 771 F.3d at 594 (a defendant's U.S. citizenship or corporate status may be "one factor that, in conjunction with other factors, can establish a sufficient connection between an ATS claim and the territory of the United States"). Thus, there is broad support for this Court to look at the totality of facts surrounding Plaintiffs' claims to determine if they sufficiently touch and concern the United States, rather than applying the erroneous and needlessly strict requirements imposed by the district court.

In applying a fact-intensive inquiry, a variety of factual circumstances are relevant. In *Al Shimari*, the Fourth Circuit weighed factors including: the defendant's status as a U.S. corporation; the defendant's employees, upon whose conduct the ATS claims were based, being U.S. citizens; the fact that managers in the U.S. gave tacit approval to the conduct underlying the claims; and the interest of the United States in regulating the conduct at issue. 758 F.3d at 530-31. Similar facts carry equal weight here.

First, just as in *Al Shimari*, 758 F.3d at 530, Defendants' status ties them to the United States. Defendant Cisco is an American corporation headquartered in California. SAC ¶ 22.[21] The conduct underlying the violations was performed

[21] As the Fourth Circuit has noted, this factor is especially important, because it means the case does not present any "problems associated with bringing foreign nationals into United States courts." *Al Shimari*, 758 F.3d at 530. This was one of the central concerns underlying the Supreme Court's decision in *Kiobel*, which involved foreign corporations. *See* 133 S.Ct. at 1669. Moreover, the United States has an international duty to provide a remedy when a U.S. citizen violates international law. *See* Emmerich de Vattel, *The Law of Nations* 162 (1797) (nations "ought not to suffer their citizens to do an injury to the subjects of another state"); Curtis Bradley, *Agora: Kiobel, Attorney General Bradford's Opinion and the Alien Tort Statute*, 106 AM. J. INT'L L. 509, 526 & n.112 (2012) (collecting

primarily by executives, engineers, and other employees of Cisco's San Jose headquarters in the United States. Cisco's San Jose-based Advanced Service Team controlled and managed the planning and preparation, marketing, design, implementation, and optimization phases of the Golden Shield project from the United States. *See* SAC ¶¶ 126-35 (detailing the extensive role played by executives, managers, and employees at Cisco's San Jose headquarters office), 145-46. Cisco engineers designed the entire apparatus from the United States, including its Falun Gong systems. SAC ¶¶ 95, 127. Cisco provided trouble shooting and other tailored customer services for Chinese security utilizing the Falun Gong systems in addition to the rest of the apparatus from the United States. SAC ¶ 102.

Moreover, Cisco's San Jose executives frequently met with Communist Party leaders in China, building relationships on the basis of its anti-Falun Gong contributions that were crucial to Cisco's efforts to penetrate and capture the lucrative Chinese technology market. *See* SAC ¶¶ 58-59, 69. Cisco's China Strategy Board, which "develops and drives the vision and strategy for China,"

---

authorities) ("[T]he United States would have had a duty to ensure that certain torts in violation of international law, especially those committed by its citizens, were punished and redressed."). For this reason, another of the concerns underpinning the *Kiobel* decision—that courts should be "wary of impinging on the discretion of the Legislative and Executive branches in managing foreign affairs," 133 S.Ct. at 1664 (internal citation omitted)—cuts in precisely the opposite direction where the defendant is a U.S. citizen, because the Legislature specifically enacted the ATS to fulfill the obligations of the United States under international law. *See Tel-Oren v. Libyan Arab Republic*, 726 F.2d 774, 783 (D.C. Cir. 1984) (Edwards, J., concurring) ("If the court's decision constitutes a denial of justice, or if it appears to condone the original wrongful act, under the law of nations the United States would become responsible for the failure of its courts and be answerable not to the injured alien but to his home state.").

including its design and development of the Golden Shield and its anti-Falun Gong systems, is composed mostly of San Jose executives and is overseen by Defendant Chambers. SAC ¶¶ 149, 206. San Jose executives sit at the top of the reporting structure of Cisco's China Research Development Center, which manufactures Cisco products in China, "including Golden Shield parts and other technology used to 'douzheng' Falun Gong [believers] in China." SAC ¶¶ 148, 205.[22]

Second, while managers in the U.S. in *Al Shimari* gave tacit approval to the conduct underlying the claims, 758 F.3d at 531, the Cisco Defendants actually carried out most of the key anti-Falun Gong conduct underlying the claims in the United States. "Cisco headquarters planned and engaged in a step-by-step process essential to establishing successful use of the Golden Shield to enact '*douzheng*' of Falun Gong." SAC ¶ 129. Defendants in San Jose "supervised and directed a marketing strategy"; "handled all aspects of the high-level design phases including those enabling the *douzheng* of Falun Gong"; and managed and controlled the implementation, integration, and optimization of anti-Falun Gong features. SAC ¶¶ 65, 127, 129, 145. "San Jose's procedures required that headquarters controlled all decision-making and related management over the project." SAC ¶ 108. Cisco's "decision-making rubric" dictated that for large and complex projects like the Golden Shield, Cisco's policy is to "maintain sole control throughout the entirety of the project." SAC ¶ 144. Customer support "was managed by the parent corporation from San Jose at least through 2008." SAC ¶ 143.

Third, just as in *Al Shimari*, 758 F.3d at 531, the United States maintains a strong interest in regulating the conduct at issue here. All three branches of the

[22] Jurisdictional discovery would disclose the extent of Cisco's control over its subsidiaries and degree to which the Chinese subsidiaries acted as a proxy for Cisco.

United States government have repeatedly condemned the widespread human rights abuses committed against the Falun Gong community and characterized Falun Gong believers as a peaceful religious group. *See* SAC ¶¶ 28, 48, 51, 164, 167, 173. Cisco representatives were called before the U.S. Senate Judiciary Committee to testify regarding their potential complicity in Chinese human rights abuses. A major part of the hearing was devoted to a discussion of internal Cisco documents revealing Cisco's knowledge of the persecutory purposes of the Golden Shield and its intended use to further of the persecution of Falun Gong members. *See* U.S. Senate, Committee on the Judiciary, *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, Hearing, May 20, 2008 (Serial No. J-110-93). The Department of Commerce's Bureau of Industry and Security (BIS) recently proposed new rules to specifically regulate the export of network security technology, including network surveillance instruments. Under these proposed rules, licensure of such products will take into account "the foreign policy interest of promoting the observance of human rights around the world." Federal Register, Vol. 80, No. 97, Proposed Rules (May 20, 2015). Further, U.S. courts hearing asylum claims have frequently held that Falun Gong believers are subject to persecution in China. *See, e.g., Yun Wang*, 493 Fed.Appx. at 480; *Shan Zhu Qiu*, 611 F.3d at 407.

Thus, these facts taken together reveal a strong nexus between the Plaintiffs' claims and the United States.

2. The *Kiobel* presumption is displaced because Cisco's domestic conduct is sufficient by itself to aid and abet the underlying violations.

Alternatively, even if this Court were to disregard the majority's opinion in *Kiobel* in favor of Justice Alito's more stringent territoriality test, the Defendants'

domestic conduct alone is sufficient to displace the extraterritoriality presumption because it constitutes aiding and abetting in and of itself.

Plaintiffs' allegations meet this approach as well. Here, the conduct alleged to have aided and abetted the underlying violations – the planning, marketing, design, and implementation of the Golden Shield's anti-Falun Gong features and the support, oversight, and management of their implementation – all occurred in the United States. *See supra* at I(A)(2)-(4) *and* I(B)(2), (4); *see also* SAC 126-35 (detailing Cisco's conduct in San Jose). While the physical implementation of the Golden Shield's anti-Falun Gong systems occurred in China, the "fact that the impact of Defendant's conduct was felt [abroad] cannot deprive Plaintiff of a claim." *Sexual Minorities Uganda*, 960 F.Supp.2d at 321-22. Much like *Sexual Minorities Uganda*, the Defendants' orchestration and management of its work from the United States is "analogous to a terrorist designing and manufacturing a bomb in this country, which he then mails [abroad] with the intent that it explode there." *Id*. at 322. Given the quality and quantity of the Defendants' activity in the United States, and its essential contributions to the system of religious persecution in China, the Defendants' domestic conduct alone was sufficient to aid and abet the underlying violations for the purposes of satisfying Justice Alito's alternative test in *Kiobel*.

In short, an American corporation, acting in the United States, designed and oversaw the implementation of a high-tech instrument that had a substantial effect on the violent persecution of Falun Gong in China, a subject of significant foreign policy concern on the part of all branches of the U.S. government. Plaintiffs' claims therefore "touch and concern" the United States with "sufficient force" to displace the presumption against extraterritoriality.

III. OTHER LEGAL ERRORS.

In addition to the errors discussed above, the district court below (1) wrongly dismissed Plaintiffs' claims under the TVPA, and (2) entirely ignored Plaintiffs' arguments that Defendants, in addition to aiding and abetting the underlying violations, participated in a conspiracy or joint criminal enterprise to carry out the underlying violations.

First, the district court below wrongly held that Plaintiffs' claims under the TVPA must be dismissed because "claims for vicarious liability, including aiding and abetting, cannot be brought under the TVPA." ER 25. But the TVPA "contemplates liability against those who did not '*personally* execute the torture or extrajudicial killing,'" *Drummond*, 782 F.3d at 607-08 (quoting *Mohamed v. Palestinian Authority*, 566 U.S. __, 132 S.Ct. 1702, 1709 (2012) (emphasis in *Drummond*), including those who aid and abet. *Id*. This is so because "domestic law sets the standards for the TVPA," *id*., and because Congress specifically contemplated "lawsuits against persons who ordered, aided, or assisted in the torture." S. Rep. No. 102-249, at 8 (1991). The district court relied on the Ninth Circuit's language in *Bowoto v. Chevron Corp.*, 621 F.3d 1116, 1128 (9th Cir. 2010), in which the Court stated that the TVPA "limits liability to an individual who subjects another to torture." But the Ninth Circuit in *Bowoto* was addressing only the issue of corporate liability under the TVPA, explicitly leaving open the question of aiding and abetting liability: "*Even assuming the TVPA permits some form of vicarious liability*, the text limits such liability to . . . natural persons." *Id*. (emphasis added). The availability of aiding and abetting liability under the TVPA was not presented or argued in *Bowoto*, and the Ninth Circuit's holding was strictly limited to the issue of corporate liability. *See id*. at 1126-28. Thus, Plaintiffs' TVPA claims against the individual Defendants should not have been dismissed.

Second, the district court failed to even address Plaintiffs' claims that Defendants participated in a conspiracy or joint criminal enterprise to carry out the underlying violations. SAC ¶¶ 385, 390, 396, 399, 403, 408, 412, 416. Instead, the district court focused only on Plaintiffs' aiding and abetting claims. *See* ER 25-27. Thus, notwithstanding this Court's other findings, it should remand the case to the district court to address the question of conspiracy and joint criminal enterprise.

CONCLUSION

For the reasons stated above, the district court's grant of Defendants' motion to dismiss should be reversed.

Dated: January 4, 2016

Respectfully submitted,

/s/

Terri E. Marsh
HUMAN RIGHTS LAW FOUNDATION
Attorney for Plaintiffs

STATEMENT OF RELATED CASES

There are no known related cases pending in this Court.

Signed,
_____/s Terri Marsh_____
Terri Marsh

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 13,999 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). 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 version 14.5.6 in Times New Roman font size 14.

Dated: January 4, 2016

s/ Terri E. Marsh
Terri E. Marsh
Attorney for Plaintiffs/Appellants

CERTIFICATE OF SERVICE

I hereby certify that on January 4, 2016, I electronically filed the foregoing Appellants' Opening Brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that none of the participants in the case is not a registered CM/ECF user.

Dated: January 4, 2016

By: _____s/ Terri E. Marsh_____
Terri E. Marsh