CINDY COHN (SBN 145997)
cindy@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333 x108
Fax: (415) 436-9993

*Counsel for Amicus Curiae*
*Electronic Frontier Foundation*

**UNITED STATES DISTRICT COURT**

**FOR THE NORTHERN DISTRICT OF CALIFORNIA**

**SAN JOSE DIVISION**

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, and those individuals similarly situated,

Plaintiffs,

v.

CISCO SYSTEMS, INC., JOHN CHAMBERS, FREDY CHEUNG, and DOES 1-100,

Defendants.

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

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

Date: March 21, 2014
Time: 9:00 a.m.
Judge: Hon. Edward J. Davila
Courtroom 4, 5th Floor

Action Filed: May 19, 2011

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

### FEDERAL CASES



### FEDERAL RULES



### OTHER AUTHORITIES

## INTRODUCTION

Amicus curiae the Electronic Frontier Foundation ("EFF"), having observed the oral argument held on March 21, 2014, addresses three points that we hope will assist the Court in its determination of whether this case has been pled sufficiently to survive a motion to dismiss.

1) Whether the Second Amended Complaint ("Complaint" or "SAC") sufficiently alleges acts by Defendant, Cisco Systems, Inc., that, if proven, would be sufficient to create liability for Cisco for assisting the Chinese government in violating the human rights of Plaintiffs, practitioners of the Falun Gong religion;

2) Whether the SAC sufficiently alleges a U.S. nexus, if such a showing is required after *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659 (2013); and

3) Whether the District of Maryland's "political question" or "act of state" analyses in *Du v. Cisco* are correct.

Although the parties also disagree about the specific applicable legal standards, some of which are currently pending before the Ninth Circuit, under any standard this exhaustively pled Complaint should survive the Defendant's Motion to Dismiss ("MTD").

EFF especially hopes to assist the Court in response to Cisco's claim that other technology companies will face unwarranted liability if this case is allowed to proceed to discovery. EFF is broadly supportive of innovation and proud of the role that technology companies, many of whom are based in this District, have played in spreading the benefits of the digital age around the world. As a result, we are sensitive to the issues that would arise from holding technology companies liable for violations of international law under the Alien Tort Statute ("ATS") based solely on their provision of general-purpose technologies to others who then misuse them.

However, the Complaint alleges much more. Plaintiffs offer specific, nonconclusory factual allegations that, if proven, would demonstrate direct, purposeful actions taken by Cisco to facilitate the human rights abuses suffered by Plaintiffs, including: 1) specific technical customization of their products to help the Chinese authorities locate and target Falun Gong practitioners for human rights abuses including detention, torture and forced religious conversion; 2) sales, marketing and support of their products toward that end; and 3) knowledge that the Chinese authorities planned to and

actually are in fact using their products to facilitate gross human rights abuses. Taken together, these allegations take Cisco's actions far beyond the culpability of a standard sale of general-purpose technologies or services and state a claim for facilitation of human rights abuses sufficient to survive to discovery.[1]

## INTEREST OF AMICUS

EFF is a San Francisco-based non-profit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges industry, government and the courts to support free expression, privacy, and openness in the information society. Founded in 1990, EFF has over 27,000 dues-paying members domestically and internationally, with over 5,700 in California. EFF has over 280,000 newsletter subscribers, and a social media reach of well over 2.5 million followers across different social networks.

EFF seeks to participate as amicus because the allegations against Cisco here fit into a pattern EFF has tracked around the world: a growing industry of U.S. and European technology companies that knowingly sell state-of-the-art, customized electronic surveillance equipment to governments that then use them to violate human rights.[2] These surveillance technologies have been linked to harassment, arrests, and even torture of journalists, human rights advocates, and democratic activists.[3]

For instance, Bloomberg reported: "a monitoring system sold and maintained by European companies had generated text-message transcripts used in the interrogation of a human rights

[1] All websites cited in this brief were last accessed April 9, 2014.
[2] Jennifer Valentin-Devries, Julia Angwin and Steve Stecklow, *Document Trove Exposes Surveillance Methods,* Wall St. J., Nov. 11, 2011, http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html; *Wired for Repression*, Bloomberg, http://topics.bloomberg.com/wired-for-repression/.
[3] Vernon Silver, *Post-Revolt Tunisia Can Alter E-Mail with 'Big Brother' Software*, Bloomberg, Dec. 12, 2011, http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html ("Tunisia Big Brother").

activist tortured in Bahrain."[4] Other reports show that the Syrian regime restricts speech and online activities using Western surveillance and censorship technology.[5]

Similarly, Silicon Valley-based Narus provided Egypt Telecom with a tracking and content-filtering technology that allows network managers to inspect, track and target content from users of the Internet and mobile phones.[6] Although Narus' involvement in Egypt caught the attention of the press, Narus' other customers include national telecommunications authorities in Pakistan and Saudi Arabia, both of which share Egypt's poor track record for human rights abuses.[7] News reports of the Tunisian revolution explain how the Tunisian government purchased technology products developed and sold by western companies to intercept and monitor mobile and online communications and activity.[8]

Nor does these surveillance technologies only affect foreigners abroad. An American citizen in the United States was recently targeted by the Ethiopian government using technology provided by a UK and German company called Gamma International.[9] The technology infiltrated his computer and engaged in illegal wiretapping and access to his saved information and online activities.[10]

---

[4] Vernon Silver, *EU May Probe Bahrain Spy Gear Abuses*, Bloomberg, Aug. 24, 2011, http://www.bloomberg.com/news/2011-08-24/eu-legislators-ask-for-inquiry-into-spy-gear-abuses-in-bahrain.html.

[5] Hamed Aleaziz, *Syria Uses US Technology in Cyber Crackdown*, Mother Jones, Oct. 19, 2011, http://www.motherjones.com/politics/2011/10/blue-coat-systems-internet-blocking-syria; *see also* Leila Nachawati, *BlueCoat: US Technology Surveilling Syrian Citizens Online*, GlobalVoices, Oct. 10, 2011, http://advocacy.globalvoicesonline.org/2011/10/10/bluecoat-us-technology-surveilling-syrian-citizens-online.

[6] Jenn Ettinger, *Questions Raised About U.S. Firm's Role in Egypt Internet Crackdown*, FreePress, Jan. 28, 2011, http://www.freepress.net/press-release/2011/1/28/questions-raised-about-us-firms-role-egypt-internet-crackdown.

[7] *Narus: Security Through Surveillance*, Berkman Ctr. for Internet & Soc. At Harv. Univ., Nov. 11, 2008, http://blogs.law.harvard.edu/surveillance/2008/11/11/narus-security-through-surveillance/.

[8] Tunisia Big Brother, *supra*.

[9] Craig Timberg, *U.S. Citizen Sues Ethiopia for Allegedly Using Computer Spyware Against Him*, Washington Post, Feb. 18, 2014, http://www.washingtonpost.com/business/technology/us-citizen-sues-ethiopia-for-allegedly-using-computer-spyware-against-him/2014/02/18/b17409c6-98aa-11e3-80ac-63a8ba7f7942_story.html. EFF serves as counsel to the citizen in a wiretapping and invasion of privacy lawsuit filed in the Federal District Court for the District of Columbia.

[10] *Id*.

## DISCUSSION

### A. Plaintiffs' Factual Allegations Meet Even the ATS Liability Standards Urged by the Defense.

Plaintiffs' factual allegations must only be "enough to raise a right to relief above the speculative level . . . on the assumption that all the allegations in the complaint are true . . ." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citations omitted).

As this Court is aware, the Ninth Circuit recently rejected the requirement that a plaintiff allege specific intent in order to satisfy the standard for liability under the ATS. *See Doe I v. Nestle USA, Inc.*, 738 F.3d 1048 (9th Cir. 2013). Defendants in that case have sought en banc review. Cisco urges this Court to assume that the Ninth Circuit en banc will reject the panel opinion and asks, among other things, that it apply the Fourth Circuit's test articulated in *Aziz v. Alcolac*, *Inc.,* 658 F.3d 388 (4th Cir. 2011). Reply MTD 6, ECF No. 131**.**

For purposes of deciding this Motion, however, the Court need not take a position on which test will prevail, because Plaintiffs have sufficiently pled both mens rea and actus rea, even assuming the stricter *Aziz* formulation for ATS liability applies. According to the *Aziz* formulation, ATS liability for aiding and abetting is available when a defendant "1) provides practical assistance to the principal which has a substantial effect on the perpetration of the crime, and 2) does so with the purpose of facilitating the commission of that crime." *Aziz,* 658 F.3d at 396 (emphasis added).

In the alternative, a corporation may be liable if it has conspired to commit a human rights violation. *See Bowoto v. Chevron Corp.*, No. C 99-02506 SI, 2006 WL 2455752, at *8 n.13 (N.D. Cal. Aug. 22, 2006) (accepting the theory of joint criminal enterprise as an alternate basis for civil liability in ATS/TVPA cases). Defendants assert (and Plaintiffs disagree) that the proper test was articulated by *Presbyterian Church of Sudan v. Talisman Energy, Inc.*: "The analog to a conspiracy as a completed offense in international law is the concept of a joint criminal enterprise," and that "without deciding, that plaintiffs could assert such a theory in an ATS action, an essential element of a joint criminal enterprise is a criminal intention to participate in a common design." 582 F.3d 244, 260 (2d Cir. 2009) (emphasis added) (internal quotation marks omitted).

Plaintiffs' Complaint presents factual allegations that, taken together, state a claim for relief under aiding and abetting or conspiracy theories even under Defendants' formulations. These

allegations are neither implausible nor conclusory. They allege actions far beyond mere negligence or even willful blindness – they allege purposeful, knowing activity that actually assisted in gross human rights abuses perpetrated against the Falun Gong, a religious minority. That is all that is required at this stage.

In response, Cisco makes several factual claims about Plaintiffs' Complaint that are simply incorrect. First, Cisco claims that the Complaint seeks liability "solely because Cisco sold Internet equipment and services—the same goods and services that Cisco sells throughout the world—to Chinese entities." MTD 1:5-6, ECF No. 49. But, as detailed below, the Complaint alleges that Cisco specifically customized the products it sold to the Chinese authorities to target the Falun Gong, unlike the goods and services it sells elsewhere around the world.

Second, Cisco claims that "[t]he Complaint nowhere alleges any facts suggesting that Cisco . . . knew or intended that its technology would be used by Chinese authorities to injure Plaintiffs." MTD at 13:15-18. But, as also detailed below, the Complaint is rife with such assertions and with factual support for them, ranging from Cisco's marketing to its support and continued development of the technologies. Finally, Cisco alleges that the Complaint fails to allege "that Cisco knew of, or participated in, Chinese authorities' alleged detention or persecution of Plaintiffs or the 'many thousands' of other Falun Gong practitioners located throughout China." MTD at 13:18-20. Yet, the Complaint absolutely does allege both knowledge and participation in the detention through providing customized tools to allow the Chinese to identify and locate Falun Gong practitioners for detention.

Specifically, the Complaint alleges:

1. Practical Assistance: Cisco's Customization of Technological Tools that Facilitate China's Human Rights Violations Against Falun Gong.

The Complaint alleges specific and articulable facts that supporting the conclusion that Cisco created Falun Gong-specific targeting software and technologies for use by the Chinese authorities. It alleges that the tools were designed to work in an integrated fashion with public security torture sites and detention centers to facilitate the identification, apprehension and detention of Falun Gong. The specific and detailed allegations include:

**Identification and Location of Falun Gong:** Cisco created a library of carefully analyzed patterns of Falun Gong Internet activity (or "signatures") that enable the Chinese government to uniquely identify Falun Gong Internet users. SAC ¶ 80.

**Databases to Centralize Information About Falun Gong:** Cisco created several log/alert systems that provide the Chinese government with real time monitoring and notifications based on Falun Gong Internet traffic patterns. SAC ¶¶ 80, 82, 83.

**Integration with General Security:** Cisco integrated the Falun Gong-specific databases alleged above with the rest of the Internet Surveillance System it built for general law enforcement purposes. SAC ¶ 80.

**Forced Conversion Information:** Cisco created systems for storing data profiles on Falun Gong practitioners for use during interrogation and "forced conversion" (*i.e.*, torture), as well as a system for storing and sharing of "effective forced conversion sessions with other security to enable them to learn how best to force the Falun Gong adherent to renounce his religious belief." SAC ¶¶ 84-86, 98-99.

Cisco also created a system for categorizing individual Falun Gong adherents by their likely susceptibility to different methods of "forced conversion." SAC ¶¶ 88-89.

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

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

The Complaint then traces the practical application and development of the system after deployment, detailing how Cisco further honed the product toward the goal of assisting the Chinese in locating Falun Gong. SAC ¶ 92. Specifically:

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

**Falun Gong Blocking and Logging Engine:** Cisco's "Service Control Engine" detects and blocks Falun Gong web content and logs the data about such web presence. SAC ¶ 97(d). Cisco's promotional materials for the Service Control Engine included specific warnings about four 'Current Threats' online – all of

which were Falun Gong-related and promised to increase the efficiency of persecuting Falun Gong adherents. *Id.*

The Complaint also ties these customized technologies to the specific arrest, detention and torture of the Plaintiffs. ¶¶ 227, 229. In short, far from being general-purpose routers and equipment, the Complaint alleges that Cisco sold products customized specifically to assist in the Chinese government's persecution of the Falun Gong. *See also* SAC ¶¶ 35, 39, 51-52, 65, 68, 101, 109, 125, 128, 131, 155, 217.

2. Purpose or Intent: Marketing, Sale and Support of the Product for Uses That Violate Human Rights.

The Complaint also sufficiently alleges Cisco's purpose or intent to facilitate targeting of the Falun Gong. First, it alleges that Cisco intentionally vied for a lucrative contract to create a surveillance apparatus that it knew would contribute to violating the human rights of Falun Gong believers. SAC ¶¶ 54-56. The Complaint directly alleges that: "Cisco's marketing materials in China repeatedly boasted that Cisco's technology solutions could guard against Falun Gong, block and track Falun Gong, monitor and profile Falun Gong, and in other ways persecute Falun Gong." SAC ¶ 176.[11]

But the Complaint does not rest on general assertions: it specifically asserts that Cisco "knew that the most important goal of the Golden Shield apparatus was to 'stop' the Falun Gong" at the time it marketed its products. SAC ¶ 56. Well before Cisco attended any trade technology shows in China, Cisco "was already aware . . . that eliminating Falun Gong was the primary concern of [the Chinese Security officers]" *Id.* ¶ 182. It alleges that Cisco's booth brochures at a technology trade show in Beijing in the early 2000s claimed that its technology could be used to *douzheng*

[11] Cisco confirmed its knowledge of the Chinese government's goal to violate human rights. In a press release issued after an English-language presentation by Cisco Systems, Inc. became public, Cisco's Director of Corporate Communications, Terry Alberstein, stated: "those statements [to Combat Falun Gong evil religion and other hostilities] were included in the presentation to reflect the **Chinese government's position** . . . They were merely inserted in that presentation to capture the **goals of the Chinese government** in that specific project, which was one of many discussed in that 2002 presentation." Brad Rees, *PowerPoint Presentation Appears to Implicate Cisco in China Censorship*, May 20, 2008, https://www.networkworld.com/community/node/27957 (emphasis added).

Falun Gong.[12] SAC ¶ 64. Such booth brochures were used to compete with other companies for the contract to create the Golden Shield, which was awarded to Cisco in late 2001. SAC ¶¶ 72-74.

Plaintiffs further allege the existence of internal files wherein Cisco acknowledged the repressive anti-Falun Gong purpose of the Golden Shield and committed to this goal. SAC ¶¶ 61, 78, 84, 94 (indicating "even more explicitly Cisco's compliance with Communist Party ideological objectives including the suppression of the Falun Gong"). Plaintiffs allege that as early as 2002, and until at least 2006, "Cisco provided private training and marketing sessions for . . . employees . . . across China with PowerPoint presentations that specifically reference the ongoing crackdown or *douzheng* against Falun Gong and illustrate how Cisco's products are tailored to meet the stated goal of persecuting and suppressing the Falun Gong practitioners in China." *Id.* ¶ 185. Cisco's solutions and security features "cemented Cisco's place as one of the top foreign technology providers in the Chinese market." SAC ¶ 108.

Finally, Plaintiffs' assert that Cisco promoted its repressive technology on its U.S.-based website, using coded language to boast of its proficiency in combating the Falon Gong in a way that would be understood by its Chinese customers but not readily apparent to its Western customers. "The website, Cisco.com, included 'success stories' demonstrating the company's familiarity with and deliberate attempts to further the repressive purposes of the apparatus. In one website entry, for example, Cisco touts the company's enhancement of multi-tiered networked features, designed to enhance 'social stability' and so-called 'Strike Hard campaigns,' that are described in Cisco literature, Chinese law expert reports (and elsewhere) as a key component of the Chinese persecutory crackdown against Falun Gong." SAC ¶¶ 60, 63.

Discovery can confirm these specific allegations as well as ensure their admissibility, but they are more than sufficiently specific, factual and nonconclusory to survive a motion to dismiss.

[12] "Douzheng" is defined in the Complaint as a violent persecutory campaign designed to "convert through torture, murder and in other ways suppress Falun Gong" SAC ¶¶ 34, 37, 43

3. Specific Knowledge: China's Well-Documented Practice of Engaging in Gross Human Rights Violations Using Surveillance Technologies Like Those Provided by Defendant

The Complaint highlights the Chinese Communist Party ("CCP") and Chinese security's well-documented practice of engaging in gross human rights violations against Falun Gong believers. As noted above, the Plaintiffs sufficiently allege that Cisco in San Jose had specific knowledge that persecution of the Falun Gong was a driving purpose for the Golden Shield prior to entering into contract with the CCP. *See also* SAC ¶¶ 1, 53-108, 127-29, 132, 159-65, 168 ("Defendants knew that a central purpose of the Golden Shield's Internet Control and Monitor System was the facilitation and advancement of the persecution of Falun Gong, and that this persecution routinely included widespread acts of torture.").

Again, this is not surprising. China's record of human rights abuses against Falun Gong practitioners is notorious and widely recognized as violating "universal and obligatory norms" of human rights law, as required for ATS liability.[13] Nor is it subject to reasonable dispute that the surveillance facilitated by Cisco leads directly to the torture, arbitrary arrest and detention and other human rights abuses against this religious minority.

The Complaint specifically notes that "Falun Gong believers have been subjected to human rights abuses" by the CCP "[s]ince the late 1990s." SAC ¶ 29. "[I]n June of 1999, the Party published a document calling for the implementation of a widespread persecutory '*douzheng*' campaign against the Falun Gong in China to ideologically convert through torture, murder and in other ways suppress Falun Gong believers in China based solely on their spiritual or religious belief." SAC ¶¶ 37, 41.

Plaintiffs support their assertion that Cisco knew of these human rights violations not only as noted in Section 2 above, but by citing the public documentation and condemnation of these abuses by the "U.S. Department of State, the United Nations, and a number of international human rights organizations, including Amnesty International and Freedom House." SAC ¶ 51. They also cite voluminous concurrent reporting on the campaign. The torture of Falun Gong believers was the

[13] *See Sosa v. Alvarez-Machain,* 542 U.S. 692, 732 (2004) (*quoting In re Estate of Marcos, Human Rights Litig.,* 25 F.3d 1467, 1475 (9th Cir. 1994)).

subject of Ian Johnson's 2001 Pulitzer Prize-winning coverage for the Wall Street Journal, as well as a host of other prominent reports. SAC ¶ 160.[14] Plaintiffs further cite a "prominent 2001 article" from the *Washington Post*, "Torture is Breaking Falun Gong," SAC ¶ 160,[15] as well as several *Associated Press* reports covering the Chinese detention and torture of Falun Gong believers in 1999, SAC ¶ 161, a *New York Times* article reporting that over 35,000 Falun Gong practitioners had been detained in 1999. SAC ¶ 162.[16]

Throughout China, the CCP openly announces its anti-Falun Gong objectives. The Complaint states that "[H]undreds of reports and announcements publicly and conspicuously displayed by Communist Party agents throughout China," including "notices by official Communist Party media" and local government website announcements reiterated "Communist Party orders to use the Golden Shield to suppress Falun Gong." SAC ¶ 88. Plaintiffs allege that "[m]any of these reports specifically emphasized the need to develop features that would facilitate serious human rights violations of Falun Gong adherents," such as databases that would "enable the categorization of Falun Gong believers according to their susceptibility to forced conversion tactics . . .." *Id*. As noted above, Cisco built such features into the technologies it provided to the Chinese authorities.

The Complaint connects this widespread coverage to Cisco's actual awareness of the abuses. *Id.* ¶ 52. Indeed, as early as 2002, "Cisco's shareholders had . . . accused Cisco of aiding and abetting human rights abuses perpetrated in China via the Golden Shield project" and demanded investigation into those issues. ¶¶ 166, 174.

(a) U.S. State Department Publicly Confirms Human Right Abuses Against Falun Gong.

Nor are the allegations of Cisco's knowledge surprising. As noted above, the U.S. State Department has long documented both the Chinese persecution of the Falun Gong, and their use of

[14] *See, e.g.,* Ian Johnson, *A Deadly Exercise*, Wall St. J., April 20, 2000, http://www.pulitzer.org/archives/6463? (listing the series of articles about Chinese abuses against the Falun Gon that won the 2001 Pulitzer Prize).

[15] John Pomfret & Philip P. Pan, Wash. Post, "Torture is Breaking Falun Gong; China Systematically Eradicating Group" at A.01 (Aug. 5, 2011).

[16] Elisabeth Rosenthal, N.Y. Times, "Few Members of Large Sect to Face Trial, Beijing Says" (Dec. 2, 1999), available at http://www.nytimes.com/1999/12/02/world/few-members-of-large-sect-to-face-trial-beijing-says.html (last accessed April 4, 2014).

surveillance technologies to facilitate that persecution.[17] For example, the 2013 U.S. State Department report on China generally describes how Chinese authorities used surveillance to assist in these abuses, noting that the government "monitored telephone conversations, fax transmissions, e-mail, text messaging, and Internet communications [and also] opened and censored domestic and international mail." *Id.* at 20. The State Department also provides:

- "Family members of activists, dissidents, Falun Gong practitioners, journalists, unregistered religious figures, and former political prisoners were targeted for arbitrary arrest, detention, and harassment"
- In May authorities in Sichuan Province detained and beat lawyers Tang Jitian and Jiang Tianyong as they attempted to visit a black jail in Ziyang that reportedly holds followers of the banned Falun Gong movement.
- There were widespread reports of activists and petitioners being committed to mental-health facilities and involuntarily subjected to psychiatric treatment for political reasons. . . . Falun Gong practitioners were among those housed in these institutions.
- Human rights lawyers reported that authorities did not permit them to defend certain clients or threatened them with punishment if they chose to do so. The government suspended or revoked the licenses of lawyers or their firms to stop them from taking sensitive cases, such as defending prodemocracy dissidents, house-church activists, Falun Gong practitioners, or government critics.[18]

This formal recognition by the State Department is important for two reasons. First, it confirms that the allegations contained in news reports had been officially confirmed by the United States government, making it not credible for Cisco to claim that it did not have sufficient knowledge of the abuses. Second, as described further below, the State Department's longstanding and unequivocal recognition of these abuses belies Cisco's claim (mistakenly adopted by the Maryland court) that the question of China's human rights violations against Falun Gong practitioners is a "political question" so irretrievably assigned to the export decisionmaking such that no liability can ever attach to Cisco's assistance of those violations.

[17] While the report is not attached to the Complaint, this Court can take judicial notice of it should it wish.

[18] *See* more at: http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?year=2013&dlid=220186.#section1darbitrary.

**B. Finding for Plaintiffs on this Motion Will Not Create Human Rights Liability Merely for Selling a General-Purpose or Dual-Purpose Device.**

To be clear, EFF believes that it is unwise to assign liability to companies for selling general-purpose or dual-purpose products to the general public that are later misused. The law does not and should not so hold. However, the facts of this case, plus the ATS and international law, already carefully cabin liability here in several key ways.

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

Second, as noted above, liability under the ATS only attaches to specific, universal, and obligatory violations of international law.[19] *Sosa*, 542 U.S. at 732 (*quoting In re Estate of Marcos,* 25 F.3d at 1475); *see also Kiobel*, at 1665. Thus, liability under the ATS under aiding and abetting or conspiracy theories is also limited to situations in which the underlying acts are gross human rights abuses like torture and arbitrary arrest and detention. Liability under the ATS simply does not arise from garden-variety offenses or crimes.

Third, in this specific case the factors noted above plainly differentiate this situation from one in which a company sells a dual-purpose product that is subsequently misused. Most important

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

of these, from a technologist's perspective, is the difference between a dual-purpose tool and a customized one. While on the margins it may be difficult to recognize the difference between a dual-purpose tool and a customized one, this difference is not conceptually difficult. For example, a hammer is a dual-purpose tool. A person can use a hammer to pound nails into wood or to bludgeon. The hammer manufacturer designs the hammer to transfer substantial force to the object it hits regardless of how it's used. In this sense, the hammer is dual-purpose, and although it can effectuate a crime, it was not customized and sold to the customer for that particular purpose.

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

**C. The Complaint Sufficiently Alleges a U.S. Nexus.**

The Complaint sufficiently pleads a U.S. nexus for Plaintiffs' claims brought under the ATS. The defense disingenuously argues that the Complaint alleges "purely extraterritorial conduct" "lacking any nexus to United States territory, citizens, or interests" MTD at 3, 20; however, the Complaint centrally implicates the conduct of a U.S. company on United States soil.

In *Kiobel*, the Court concluded that cases brought under the ATS must "touch and concern" the United States. *Kiobel* at 1669. That is, a nexus must exist between the torts committed and the United States in order to rebut the presumption against extraterritoriality which would otherwise apply. Under the facts of *Kiobel* the necessary nexus did not exist because the defendant companies were all foreign, all of the relevant conduct took place outside the U.S., and the only company presence in the U.S. consisted of a single office in New York City that existed merely to help "explain their business to potential investors." *Kiobel* at 1677.

It is important to note that the Majority opinion in *Kiobel* provided little guidance about what conduct would "touch and concern" the U.S. with sufficient force to displace the presumption against extraterritoriality. All three concurring opinions highlight the Majority's lack of clarity about what behavior satisfies the Majority's "touch and concern" test. For instance, Justice Kennedy stated in his concurrence:

> Other cases may arise with allegations of serious violations of international law principles protecting persons, cases covered neither by the TVPA nor by the reasoning and holding of today's case; and in those disputes the proper implementation of the presumption against extraterritorial application may require some further elaboration and explanation.

*Kiobel* at 1669 (Kennedy, J., concurring). Similarly, Justice Breyer noted that the decision "leaves for another day the determination of just when the presumption against extraterritoriality might be 'overcome.'" *Kiobel* at 1673 (Breyer, J. concurring) (citation omitted). Justice Alito commented that the requirement that ATS claims that "touch and concern the territory of the United States . . . must do so with sufficient force to displace the presumption against extraterritorial application" obviously "leaves much unanswered . . . " *Kiobel* at 1669 (Alito, J., concurring) (quotation omitted).

Thus, although the Supreme Court found no extraterritorial application of the ATS based on the specific facts of *Kiobel*, the Court made clear that extraterritorial application may apply to cases in which there is a sufficient connection between the United States and the tort committed.

Few courts have had the opportunity to analyze *Kiobel*'s "touch and concern" test since the case's decision in April of 2013. However, in *Mwani v. Bin Laden*, the court found that a bombing of the United States embassy in Nairobi, Kenya "touched and concerned" the United States because it served "not only to kill both American and Kenyan employees inside the building, but to cause pain and sow terror in the embassy's home country, the United States." 947 F. Supp. 2d 1, 5 (D.D.C. 2013) (citations omitted). The court further found that the Plaintiffs in the case "presented evidence that the attackers were involved in an ongoing conspiracy to attack the United States, and overt acts in furtherance of that conspiracy took place within the United States." *Id.*

Plaintiffs here have sufficiently alleged a U.S. nexus to withstand a motion to dismiss:

1. Specific Customization, Marketing Management and Support from the U.S.:

**Marketing Materials** Cisco's San Jose office largely managed Cisco's marketing campaign aimed at China. SAC ¶ 74. It created marketing materials referring to the "Strike Hard" campaign against "evil cults," echoing the rhetoric used in connection with the persecution of the Falun Gong. SAC ¶ 62.[20] "The anti-Falun Gong purpose of the apparatus, known to Defendants in San Jose, played a significant role in Cisco's marketing of the Golden Shield designs and products in China." SAC ¶ 58, ¶ 183.

**Refinement and Customization:** Cisco's San Jose office was centrally involved in the refinement of the Golden Shield's ability to track and identify dissidents such as the Falun Gong. "The Golden Shield [] required post-product maintenance, testing and verification, training and support, . . . [a]ll of the above required intensive and ongoing involvement by Cisco employees in San Jose." SAC ¶ 102. Plaintiffs allege that the existing uses of the technology were "carefully analyzed . . . made more efficient [and increased] in scope by Cisco engineers in San Jose." SAC ¶ 92.

**Decision-making and Management:** "San Jose's procedures required that headquarters controlled all decision-making and related management over the project." *Id.* ¶ 108.

**Advanced Services Team:** "For technologically advanced important overseas projects like the Golden Shield," Cisco "routinely assigns its own engineering resources to design and implement the project in its entirety and in particular through its Advanced Services Team, a specialized service offered [Cisco] that employs experts and engineers in network technology for large-scale overseas projects or important clients." SAC ¶ 145.

2. U.S. Nexus for Cisco's Business in China:

**China Strategy Board:** Cisco has a China Strategy Board ("CSB"), which has controlled Cisco's Chinese operations since 2008. *Id.*, SAC ¶ 206 The CSB is composed of high-level executives working at Cisco's San Jose headquarters and at its Chinese subsidiaries, and is chaired by Cisco Senior Vice President Jim Sheriff. SAC ¶ 139. It is also overseen by Defendant John Chambers. SAC ¶ 206

**Corporate Structure Oversight:** Furthermore, the Complaint includes extensive discussion of the corporate structure and oversight of Cisco's operations in China. *See, e.g.,* SAC ¶¶ 137-139. "During the period relevant

[20] This is also confirmed by a leaked presentation that is identified on every page as being the product of the American company, Cisco Systems, Inc. Sarah Stirland, *Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers,* http://www.wired.com/threatlevel/2008/05/leaked-cisco-do.

to this complaint, Defendants in San Jose directly oversaw the operations of Cisco China . . . indicating a clear chain of command in which all operations in China were reported to and major decisions were directed by executives in San Jose." *Id.* ¶ 138.

**Executive Overlap:** "San Jose Defendants exercised unusual control over Cisco China's day-to-day and other operations. Many of the high-ranking Cisco China executives held equally high-level sales and marketing positions in Defendant Cisco's San Jose headquarters . . ." *Id.* ¶ 139.

3. Cisco's General U.S. Nexus:

**Principle Place of Business and U.S. Employees:** Cisco is an American company incorporated in California with its principal place of business in San Jose, California. SAC ¶ 22. In fact, Cisco has over 37,000 U.S. employees (out of a total of over 75,000) according to its 2013 10-K report to the Securities and Exchange Commission.[21]

**Real Property:** Cisco also owns a significant amount of real property in the United States, including its headquarters in San Jose, California and facilities in the surrounding areas of San Jose, California; Boston, Massachusetts; Richardson, Texas; Lawrenceville, Georgia; and Research Triangle Park, North Carolina.[22]

**Defendant John Chambers**: A resident of California and as CEO of Cisco, Chambers directs and supervises Cisco's operations in China, as he did at all relevant times. SAC ¶ 23

## D. Maryland Decision of *Du v. Cisco* Was Incorrect and Should Not be Followed by This Court

As this Court is aware, the United States District Court for the District of Maryland recently dismissed *Du Daobin v. Cisco Systems*, ___ F. Supp. 2d ____, 2014 WL 769095 (D. Md. Feb. 24, 2014), a case brought by Chinese democracy advocates against Cisco. As an initial matter, the Maryland court did not accept Cisco's claim that the mere fact that it is a corporation makes it immune from liability. *Id.* at *8. The Maryland then court largely side-stepped the issue of when corporations can be held to account for building technologies that are customized for repressive

[21] Cisco Systems, Inc., *United States Securities and Exchange Commission, Form 10-K,* http://investor.cisco.com/sec.cfm?NavSection=SEC&DocType=Annual&Year=2013. While also not yet formally in the record, Cisco's annual report is a party admission under Fed. R. Evid. 801(d)(2)(A).

[22] *Id*.

governments, instead ruling incorrectly on two other grounds: political question and act of state. This Court should decline to follow that analysis.

First, the court in *Du Daobin* held that export laws and regulations create a "political question" rendering Cisco's liability here nonjusticiable. *Id*. at *6. Yet neither Cisco nor the Maryland court pointed to any statement by Congress that it intended for export control authorities to have sole discretion over questions of subsequent liability for the use of the American technologies abroad. Thus, the situation plainly fails the *Baker v. Carr* requirement of a "textually demonstrable constitutional commitment of the issue to a coordinate political department." *Baker v. Carr,* 369 U.S. 186, 217 (1962).

This is not surprising: the export question is up or down – exports are either allowed or they are not. This level of decisionmaking may be appropriate for items that are single use, such as the instruments of physical torture which were subjected to severe export controls after the Tiananmen Square protests of 1989. It is *not* an appropriate decision-making method for dual-use items like surveillance equipment, which can be used for legitimate law enforcement purposes as well as gross human rights abuses. Congress' decision to allow these exports says absolutely nothing about whether subsequent liability should attach to a company that knowingly customizes, sells and supports a dual-use item intended for human rights abuses. Nor is it even clear from this record that the customizations and knowledge of Cisco about the end uses of its technology were even presented to the Commerce Department as part of the export process. Moreover, liability for a product is simply not determined by a decision to export – were it so, the export determinations could be used as a shield against product liability, breach of contract or other civil claims. Additionally, as noted above, relying solely on the export review processes also overlooks the State Department's clear and unequivocal assertions that human rights abuses are occurring against Falun Gong practitioners and that those abuses are facilitated by surveillance.

Second, the *Du Daobin* court held that the "act of state" doctrine forbade it from ruling on whether China had abused the plaintiffs' human rights. The "act of state" doctrine stipulates that, in general, one country should not sit in judgment on another government's official acts within its own territory. But this doctrine only applies to public, *official* policies of another country. The Chinese

government has repeatedly denied that human rights abuses are its official policies. This should end the matter.

In an attempt to revitalize the argument, Cisco relies upon ten-year-old letters from the U.S. State Department and the Chinese government raising concerns about a different case, brought directly against Chinese officials who resided in China. MTD at 14:9-15:23. Not only are the circumstances here significantly different – this case is against an American company based in San Jose – but quite plainly, if either the U.S. government or the Chinese government had similar concerns about this case, they could have sent similar letters to this Court. They did not and it is not appropriate for this court to rely, for "act of state" purposes, on statements made over a decade ago to a different court about a very different case.

Finally, Cisco seemed to assert at oral argument that the fact that China had passed a discriminatory law banning the Falun Gong religion renders all human rights abuses it conducts subsequently, and any efforts Cisco makes to facilitate those abuses, "acts of state." But this is not the law. The relevant "acts" here are the human rights abuses themselves – the unlawful detention, torture and other abuses – which are inconsistent with China's international law obligations, and as noted above, denied by China.[23]

## CONCLUSION

Amici respectfully request that the Motion to Dismiss be denied and this case allowed to proceed to discovery.

DATED: April 10, 2014

Respectfully submitted

By: *s/ Cindy Cohn*
CINDY COHN
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
*Counsel for Amicus Curiae*
*Electronic Frontier Foundation*

[23] An interpretation of the "act of state" doctrine as prohibiting any human rights claims arising out of discriminatory laws would undermine the very foundation of human rights law. Quite obviously, modern international human rights law arose out of the Nazi atrocities that were largely carried out under such discriminatory laws.