IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Greenbelt Division

DU DAOBIN, *et al.*,	)	
	)	Case No.: 8:11-cv-01538-PJM
Plaintiffs,	)	
	)	
v.	)	
	)	
CISCO SYSTEMS, INC., *et al.*,	)	
	)	
Defendants.	)	

MOTION FOR LEAVE TO FILE BRIEF AMICUS CURIAE

The Electronic Frontier Foundation ("EFF") submits this Motion for Leave to File a Brief as amicus curiae in support of Plaintiffs' Opposition to Defendants' Motion to Dismiss:

1. This Court has recognized that the aid of amici curiae is appropriate at the trial level when, among other reasons, they: 1) provide helpful analysis of the law and, 2) when they have a special interest in the subject matter of the suit. *Bryant v. Better Business Bureau of Greater Baltimore, Inc.*, 923 F. Supp. 720, 728 (D. Md. 1996). Here, EFF hopes to provide a helpful analysis of the law, especially on the issues of extraterritoriality and whether the complaint properly states a claim upon which relief can be granted. EFF has a special interest in the subject matter, as described further in paragraph 3 below.

2. EFF is a 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, the EFF has over two-decades of experience engaging with law related to digital technology, including either representing parties or filing amicus briefs in dozens of key cases

addressing the interaction of law and digital technology across the country. EFF believes this perspective can assist this Court in determining whether Defendants' Motion to Dismiss should be granted.

3. EFF has also been an international leader in raising concerns about the use of Western surveillance technologies to facilitate human rights abuses in repressive regimes. EFF has tracked the misuse of these technologies in a series of publications,[1] has testified about them before the European Parliament,[2] has assisted members of Congress in consideration and development of potential legislation addressing this issue and has written a white paper laying out voluntary tests that companies should adopt to prevent assisting in human rights violations, drawing on the standards for behavior by companies under the Foreign Corrupt Practices Act and Export Administration Act.[3]

4. EFF has contacted both the Plaintiffs and Defendants to seek consent to file this brief. The Plaintiffs have consented and the Defendants have taken no position on the filing of this brief.

---

[1] *See, e.g.* "Mass Surveillance Technologies," https://www.eff.org/issues/mass-surveillance-technologies; Jillian York, "Blue Coat: Concern for Criminal Penalties, Not Human Rights," (October 29, 2011) https://www.eff.org/deeplinks/2011/10/blue-coat-acknowledges-syrian-government-use-its-products; Trevor Timm, "Spy Tech Companies & Their Authoritarian Customers, Part 1: Fin FinFisher and Amesys" (February 16, 2012), https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys; Trevor Timm, "Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA," (February 21, 2012) https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa.

[2] Trevor Timm, "Time to Act on Companies Selling Mass Spy Gear to Authoritarian Regimes," (February 7, 2102) https://www.eff.org/deeplinks/2012/02/time-act-companies-selling-mass-spy-gear-authoritarian-regimes.

[3] Cindy Cohn & Jillian C. York, "'Know Your Customer'" Standards for Sales of Surveillance Equipment" (Oct. 24, 2011), https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment.

5. EFF thus seeks leave to file the accompanying amicus curiae brief, which is attached as Schedule 1.

Respectfully submitted,

/s/ Jan I. Berlage
Jan I. Berlage #23937
GOHN, HANKEY & STICHEL, LLP
201 North Charles Street
Baltimore, MD 21201
Phone: (410) 752-9300
Facsimile: (410) 752-2519
JBerlage@ghsllp.com

Cindy Cohn (*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
cindy@eff.org

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on the 15th day of August, 2013 a copy of Electronic Frontier Foundation's Motion for Leave to File Brief Amicus Curiae of in Support of Plaintiffs was served via first class mail, postage pre-paid and/or electronically via CM/ECF system, to the following:

Lincoln O. Bisbee
MORGAN, LEWIS & BOCKIUS
111 Pennsylvania Avenue, NW
Washington, DC 20004
(202) 739-3000
(202) 739-3001 fax
lbisbee@morganlewis.com

Kathleen M. Sullivan
Isaac Nesser
Faith E. Gay
QUINN EMANUAEL URQUHART & SULLIVAN
51 Madison Avenue, 22nd Floor
New York, New York 10010
(212) 849-7000
kathleensullivan@quinnemanuel.com
isaacnesser@quinnemanuel.com
faithgay@quinnemanuel.com

Counsel for Defendants

Daniel S. Ward
Taimur Rabbani
WARD & WARD, P.L.L.C.
2020 N Street, NW
Washington D.C. 20036
(202) 331-8160
dan@wardlawdc.com
trabbani@wardlawdc.com

Counsel for Plaintiffs

/s/ Jan I. Berlage
Jan I. Berlage

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Greenbelt Division

DU DAOBIN, *et al.*,	)	
	)	Case No.: 8:11-cv-01538-PJM
Plaintiffs,	)	
	)	
v.	)	
	)	
CISCO SYSTEMS, INC., *et al.*,	)	
	)	
Defendants.	)	

BRIEF AMICUS CURIAE OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS

Jan I. Berlage #23937
GOHN, HANKEY & STICHEL, LLP
201 North Charles Street
Baltimore, MD 21201
Phone: (410) 752-9300
Facsimile: (410) 752-2519
JBerlage@ghsllp.com

Cindy Cohn (*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
cindy@eff.org

Counsel for Amicus Curiae
Electronic Frontier Foundation

Dated: August 15, 2013

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Greenbelt Division

DU DAOBIN, *et al.*,	)	
	)	Case No.: 8:11-cv-01538-PJM
Plaintiffs,	)	
	)	
v.	)	
	)	
CISCO SYSTEMS, INC., *et al.*,	)	
	)	
Defendants.	)	

BRIEF AMICUS CURIAE OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS

Jan I. Berlage #23937
GOHN, HANKEY & STICHEL, LLP
201 North Charles Street
Baltimore, MD 21201
Phone: (410) 752-9300
Facsimile: (410) 752-2519
JBerlage@ghsllp.com

Cindy Cohn (*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
cindy@eff.org

Counsel for Amicus Curiae
Electronic Frontier Foundation

Dated: August 15, 2013

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

Federal Rules

Other Authorities

Jillian York, "Blue Coat: Concern for Criminal Penalties, Not Human Rights," (October 29, 2011) https://www.eff.org/deeplinks/2011/10/blue-coat-acknowledges-syrian-government-use-its-products 3

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/ 8

Liu Xianbin, http://www.bbc.co.uk/news/world-asia-pacific-12859050 4

"Mass Surveillance Technologies," https://www.eff.org/issues/mass-surveillance-technologies 3

Press Release, Congressman Chris Smith, Smith Bill Promoting Online Freedom Is Passed by Key House Subcommittee (Mar. 27, 2012) http://chrissmith.house.gov/news/documentsingle.aspx?DocumentID=287401 9

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/ 12

Steve Stecklow, Paul Sonne, & Matt Bradley, *Mideast Uses Western Tools to Battle the Skype Rebellion*, WALL ST. J., June 1, 2011, http://online.wsj.com/article/SB10001424052702304520804576345970862420038.html 8

Surveillance of Skype Messages Found in China, John Markoff, https://www.nytimes.com/2008/10/02/technology/internet/02skype.html (October 1, 2008) 5

The Architecture of Control: Internet Surveillance in China, James A. Lewis, Center for Strategic and International Studies http://csis.org/files/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf (7/06) 5

"The Connection Has Been Reset," James Fallows, March, 2008, http://www.theatlantic.com/magazine/archive/2008/03/-ldquo-the-connection-has-been-reset-rdquo/6650/ 5

Timothy Karr, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," HUFFINGTON POST, January 28, 2011, http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html 7

Trevor Timm, "Spy Tech Companies & Their Authoritarian Customers, Part 1: Fin FinFisher and Amesys" (February 16, 2012), https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys 3

I. INTRODUCTION

Plaintiffs' are well-known democracy activists in China who have been persecuted by the Chinese authorities for their speech and other activities in violation of international human rights law. Their First Amended Complaint ("FAC") alleges specific facts that, if proven, would demonstrate that Defendants, both individual officers of the company and the American corporation Cisco Systems, Inc. (collectively "Cisco") knowingly customized, marketed, sold and provided continued support and service for technologies it provides to the government of China that facilitate those human rights abuses. Specifically, Plaintiffs allege that Cisco's activities enabled Chinese officials to violate Plaintiffs' human rights under the laws of nations by tracking, monitoring, breaching the anonymity of Plaintiffs in their speech and other democracy-building activities.

Plaintiffs support these allegations with evidence of their personal injuries, actual links between their personal injuries and the surveillance technologies provided by defendants and, most importantly, a presentation by the American company, Cisco Corporation, Inc. (rather than a Chinese subsidiary) that demonstrates Cisco's knowledge, promotion and intent that their products would be used for the abuse of political dissidents. In response, Cisco's Motion to Dismiss Plaintiffs' First Amended Complaint ("MTD") generally argues that Plaintiffs' Complaint fails to state a claim for which relief can be granted and that its allegations of Cisco's technology customization are factually inaccurate. However, Plaintiffs' Complaint satisfies *Twombly*'s pleading requirements, leaving only disputes of fact, which cannot be decided at this juncture.

Amicus the Electronic Frontier Foundation ("EFF") here addresses two of the key points relied upon by Defendants in their MTD: 1) whether the FAC sufficiently alleges a U.S. nexus, if such a showing is required after *Kiobel*, 2) whether the FAC sufficiently alleges that Cisco affirmatively acted with the purpose of assisting the Chinese government in using its products to violate human rights. Although the parties also disagree about the legal standards applicable to

both of these issues, Amicus files this brief to point out that, even under Defendants' articulation of the standards, which we do not endorse, this Complaint should survive the motion to dismiss.[1]

EFF is sensitive to the issues arising from holding technology companies liable for violations of international law under the Alien Tort Statute ("ATS") based solely on the misuse of their technologies by others. However, that is not what the Complaint alleges. Rather Plaintiffs offer four sets of factual allegations specific to this case that, if proven, would demonstrate much more direct involvement by Cisco in facilitating the human rights abuses suffered by Plaintiffs. Taken together, these state a claim for human right abuses sufficient to survive to discovery. Specifically, Plaintiffs' Complaint describes:

1) Marketing: The Complaint offers detailed allegations regarding the marketing, sale and support of the products for the facilitation of human rights violations by China against political dissidents. Most dramatically, Exhibit A to the Complaint is a marketing presentation by Cisco to the Chinese government that asserts that the technologies can help the Chinese government to "combat 'Falun Gong' evil religion and other hostilities."

2) Customization: The Complaint alleges that Cisco customized its technologies for the purpose of facilitating human rights violations by China against dissidents,

3) Specific Knowledge: The Complaint highlights China's well-documented practice of engaging in gross human rights violations against democracy activists, including Plaintiffs, and Cisco's specific knowledge of China's use of the technologies for those purposes, including the knowledge demonstrated in Exhibit A.

4) Ongoing Support: The Complaint offers detailed factual allegations confirming Defendants' ongoing relationship with the Chinese government and ongoing support of the customized products.

---

[1] Defendants' MTD includes additional legal arguments. Amicus addresses only these two key issues.

II. INTEREST OF AMICUS

EFF is a 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 23,000 dues-paying members all over the United States and internationally, including in 400 Maryland. EFF also has over 210,000 newsletter subscribers, and a social media reach of well over 1.5 million followers across different social networks.

EFF has also been a leader in raising concerns about the use of Western surveillance technologies to facilitate human rights abuses in repressive regimes. EFF has tracked the misuse of these technologies in a series of publications,[2] has testified about them before the European Parliament,[3] has assisted members of Congress in consideration and development of potential legislation addressing this issue and has written a white paper suggesting voluntary tests that companies should adopt to prevent assisting in human rights violations, drawing on the standards for behavior by companies under the Foreign Corrupt Practices Act and Export Administration Act.[4]

---

[2] *See, e.g.* "Mass Surveillance Technologies," https://www.eff.org/issues/mass-surveillance-technologies; Jillian York, "Blue Coat: Concern for Criminal Penalties, Not Human Rights," (October 29, 2011) https://www.eff.org/deeplinks/2011/10/blue-coat-acknowledges-syrian-government-use-its-products; Trevor Timm, "Spy Tech Companies & Their Authoritarian Customers, Part 1: Fin FinFisher and Amesys" (February 16, 2012), https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-i-finfisher-and-amesys; Trevor Timm, "Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA," (February 21, 2012) https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa.

[3] Trevor Timm, "Time to Act on Companies Selling Mass Spy Gear to Authoritarian Regimes," (February 7, 2102) https://www.eff.org/deeplinks/2012/02/time-act-companies-selling-mass-spy-gear-authoritarian-regimes.

[4] Cindy Cohn & Jillian C. York, "'Know Your Customer' Standards for Sales of Surveillance Equipment" (Oct. 24, 2011), https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment.

III. STATEMENT OF FACTS

Plaintiffs have articulated the basic facts in their Complaint and Opposition. Amicus here discusses the facts pertinent to its arguments.

A. China's Abuses of Democracy Activists, Including Plaintiffs, is Widely Known and Was Known to Cisco.

Plaintiffs are well-known human rights and democracy activists, whose activities include Internet publication of reports of human rights abuses in China.[5] The Complaint sufficiently alleges that China's abuse of them was known to Cisco. FAC ¶¶ 73-75.

Indeed, China's human rights abuses are notorius and publicly documented. For example, the 2012 U.S. State Department report on China confirms the targeting of activists like Plaintiffs for human rights abuses: "Repression and coercion, particularly against organizations and individuals involved in rights advocacy and public interest issues, were routine .... Authorities resorted to extralegal measures such as enforced disappearance, 'soft detention,' and strict house arrest, including house arrest of family members, to prevent the public voicing of independent opinions."[6] The State Department Report 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 22.

The State Department Report even specifically describes the Chinese government's imprisonment of Plaintiff, Liu Xianbin for promoting democracy through publications on websites:

---

[5] *See, e.g.,* Du Daobin, http://pen.org.au/about-us/honorary-members/bio/du-daobin/ (this article also mentions abuses against Plaintiff Zhou Yuanzhi); Liu Xianbin, http://www.bbc.co.uk/news/world-asia-pacific-12859050.

[6] U.S. State Dep't, Bureau of Democracy, Human Rights and Labor, Country Reports on Human Rights Practices for 2012, China (2012) at 1 [hereinafter State Department Report], http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper. While this report is not cited by the parties, Federal Rule of Civil Procedure 201(b) allows the Court to take notice of facts that are not subject to reasonable dispute because they "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned."

> In 2010 activist Liu Xianbin, signatory of Charter '08 (a manifesto calling for human rights and democracy), was indicted for subversion for an article he wrote following his 2009 release from a previous prison term. In March 2011 he was sentenced to 10 years in prison for inciting "subversion of state power." Formally detained in 2010, Liu was charged for articles he wrote and posted on overseas Web sites, as well as for involvement with a Beijing seminar regarding three Fujian persons imprisoned for Internet postings. Liu was reportedly denied access to his lawyers during his detention.

Id. at 20. Discovery can further reveal and confirm Cisco's knowledge of these human rights abuses.

B. Cisco's Technology is Used to Assist in the Repression of Chinese Democracy Activists.

The Complaint also alleges that Cisco's technology assists China in its repression of democracy activists by facilitating surveillance and tracking of activists, as well as the collection of evidence of their activism. *See, e.g.,* FAC ¶¶ 3, 16, 19, 23, 46-71, 75,78-9, 83-108, 175-177. Cisco's involvement centers around its development, sale and ongoing support of China's Golden Shield Project, often referred to in the West as the Great Firewall of China. According to the complaint as well as published articles on the topic the system contains a series of extensive techniques to monitor and track the Internet usage of people in China.[7] The government is often able to not only track what sites an individual visits, but also pinpoint who that individual is, what messages that person posts, and even the content of her communications, including unmasking anonymous speakers or those using a pseudonym or otherwise taking steps to avoid detection by the Chinese government.

The complaint alleges that the system sold by Cisco, and subsequent training by Cisco, allows Chinese officials to "access private internet communications, identify anonymous web log

---

[7] *See, e.g.*, The Architecture of Control: Internet Surveillance in China, James A. Lewis, Center for Strategic and International Studies http://csis.org/files/media/csis/pubs/0706_cn_surveillance_and_information_technology.pdf (7/06); "The Connection Has Been Reset," James Fallows, March, 2008, http://www.theatlantic.com/magazine/archive/2008/03/-ldquo-the-connection-has-been-reset-rdquo/6650/; Surveillance of Skype Messages Found in China, John Markoff, https://www.nytimes.com/2008/10/02/technology/internet/02skype.html (October 1, 2008); China Boosts Internet Surveillance, Tania Branigan, (July 26, 2011) http://www.guardian.co.uk/world/2011/jul/26/china-boosts-internet-surveillance.

authors, prevent the broadcast and dissemination of peaceful speech, and otherwise aid and abet in the violation of Plaintiffs' fundamental human rights." FAC ¶. 2. Specifically, Plaintiffs allege that they were individually tracked and monitored using Cisco's systems. FAC ¶¶ 117, 122, 134, 135, 140, 146, 154, 155, 156, 159. For instance, "On October 28, 2003, because of Du's activities online – which were monitored, tracked, and surveilled with Cisco technology – CCP authorities criminally detained and arrested Du and raided his house." FAC ¶ 117. Furthermore, Plaintiffs allege in their Opposition to Defendants' MTD, that "Du published articles under pseudonyms, detected with Cisco technology, and these articles were the basis for the harms that Du suffered" and "Zhou was detained, severely tortured and otherwise subjected to gross violations of his basic human rights, on the basis of [his] anonymous articles." Opposition at 5.

Plaintiffs have sufficiently alleged in their Complaint that through the use of Cisco's customized surveillance technology the Chinese government surveilled and tracked them as part of violating their human rights.

C. The Broader Context: Authoritarian Governments Around the World Rely on the Technology Developed and Sold by U.S. and European Companies to Facilitate Gross Human Rights Abuses.

The allegations against Cisco here sadly fit into a pattern EFF has tracked around the world: Western technology companies providing the technologies used in human rights abuses and, as alleged here, being actively involved in developing and selling the technologies for those purposes. EFF has documented a growing industry of U.S. and European technology companies that sell state-of-the-art electronic surveillance equipment to governments known for violating human rights including Tunisia, Egypt, and Syria.[8] This surveillance technology has been linked to harassment, arrests, and even torture of journalists, human rights advocates, and democratic activists in various counties with repressive regimes. Specifically, this technology can enable

[8] Jennifer Valentin-Devries, Julia Angwin and Steve Stecklow, *Document Trove Exposes Surveillance Methods,* http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html; Wired for Repression, Bloomberg, http://topics.bloomberg.com/wired-for-repression/.

governments to track and listen in on cell phone calls,[9] use voice recognition to scan mobile networks, read emails and text messages, censor web pages, track movements.[10] 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 activist tortured in Bahrain."[11]

The Silicon Valley-based subsidiary of The Boeing Company, Narus[12] was revealed to have sold such sophisticated surveillance equipment to Egypt.[13] News reports suggest that Narus provided Egypt Telecom with "Deep Packet Inspection equipment, a tracking and content-filtering technology that allows network managers to inspect, track and target content from users of the Internet and mobile phones, as it passes through routers on the information superhighway."[14] Although Narus' involvement in Egypt caught the attention of the press, it is also noteworthy that 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.[15]

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.[16] Munich-based Trovicor GmbH and Sundby, Denmark-based ETI A/S both supplied the Tunisian government with high-technology products critical to

---

[9] http://www.bloomberg.com/data-visualization/wired-for-repression/.

[10] 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")

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

[12] http://www.narus.com.

[13] Timothy Karr, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," HUFFINGTON POST, January 28, 2011, http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html.

[14] *Id.*

[15] *Id.*

[16] Tunisia Big Brother, *supra*.

the government's repressive goals.[17]

Western companies have also played a significant role in enabling Hosni Mubarak, former Egyptian president, and his regime's suppression of Internet and phone communication. Gamma International, a UK-based corporation was identified by activists who found company records indicating that it provided Mubarak with a five-month trial of its sophisticated spying technology that can wiretap encrypted Skype phone calls and instant messages.[18]

Evidence published by activist collective, Telecomix,[19] along with more detailed reports from Global Voices Advocacy[20] and Mother Jones[21] shows that the Syrian regime restricted speech and online activities also using Western surveillance and censorship technology. Even despite a U.S. embargo and export laws prohibiting sales to Syria, the technology of Blue Coat, a Sunnyvale, California company, was provided to the regime through a third-party distributor.[22] For its violations, the third- party distributor known as Computerlinks settled with the U.S. Commerce Department's Bureau of Industry and Security for a $2.8 million fine.[23]

These examples are not an exhaustive list. Yet they demonstrate why issues like the claims against Defendants here need to be taken seriously and require careful consideration by the courts. American law, including the Alien Tort Statute and ordinary tort law, is available to help ensure that Americans, including American companies, are not actively involved in developing and

---

[17] *Id.*

[18] Steve Stecklow, Paul Sonne, & Matt Bradley, *Mideast Uses Western Tools to Battle the Skype Rebellion*, WALL ST. J., June 1, 2011, http://online.wsj.com/article/SB10001424052702304520804576345970862420038.html.

[19] http://telecomix.org/.

[20] 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/.

[21] 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.

[22] *Bluecoat's Role in Syrian Censorship and Nationwide Monitoring System #OpSyria*, REFLECTS.INFO, http://reflets.info/bluecoats-role-in-syrian-censorship-and-nationwide-monitoring-system/.

[23] Settlement Agreement, *available at* https://www.eff.org/sites/default/files/e2315.pdf.

selling high technology products that facilitate gross human rights violations by repressive regimes.

Nor would the Court be alone in recognizing the problems. The House panel that oversees international human rights, which is chaired by Congressman Chris Smith of New Jersey, passed the Global Online Freedom Act ("GOFA") in March of 2012 which would prohibit the export of hardware or software that can be used for surveillance, tracking, blocking, and similar activities to governments in "Internet-restricting" countries.[24] GOFA was drafted "[i]n response to numerous reports of U.S. technology being used to filter political and religious speech, as well as track down or conduct surveillance of activists through the Internet or mobile devices." *Id.*[25]

The European Parliament has also recognized the seriousness of technology companies selling surveillance equipment to repressive governments that use the technology to surveil democracy activists. It has passed a resolution barring overseas sales of systems including those that monitor phone calls and text messages, or provide targeted surveillance, if those systems are used to violate democratic principles, human rights or freedom of speech.[26]

IV. DISCUSSION

A. Legal Standard for a Motion to Dismiss

The sufficiency of a complaint can be determined by a two-pronged test: 1) a complaint must contain factual allegations in addition to legal conclusions, and 2) "[t]o survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Robertson v. Sea Pines Real Estate Cos.*, 679 F.3d 278, 288 (4th Cir. 2012) (quoting *Bell Atlantic Corp. v. Twombly*, 127 S.Ct. 1955, 1974 (2007)). "The

---

[24] Press Release, Congressman Chris Smith, Smith Bill Promoting Online Freedom Is Passed by Key House Subcommittee (Mar. 27, 2012) http://chrissmith.house.gov/news/documentsingle.aspx?DocumentID=287401.

[25] http://chrissmith.house.gov/news/documentsingle.aspx?DocumentID=287401. The barriers to export under consideration in GOFA would complement existing potential liability under the ATS or other law.

[26] Vernon Silver, *EU Curbs Export of Surveillance Systems*, BLOOMBERG, Sept. 27, 2011, http://www.bloomberg.com/news/2011-09-27/eu-curbs-export-of-surveillance-systems.html.

purpose of a Rule 12(b)(6) motion is to test the sufficiency of a complaint; 'importantly, [a Rule 12(b)(6) motion] does not resolve contests surrounding the facts, the merits of a claim, or the applicability of defenses.'" *Edwards v. City of Goldsboro*, 178 F.3d 231, 243 (4th Cir. 1999) (citing *Republican Party v. Martin*, 980 F.2d 943, 952 (4th Cir. 1992)). Therefore dismissal under Rule 12(b)(6) "should only be granted if, after accepting all well-pleaded allegations in the plaintiff's complaint as true and drawing all reasonable factual inferences from those facts in the plaintiff's favor, it appears certain that the plaintiff cannot prove any set of facts in support of his claim entitling him to relief." *Id.* at 244.

As noted above, the parties disagree about the appropriate standards that must be met for both extraterritoriality and whether the Complaint sufficiently alleges acts by defendants that would create liability. Amicus believes that Plaintiffs make important points about the standard to be applied in both instances. However, even assuming the defendants are correct about the tests to be applied, the Complaint easily meets the 12(b)(6) standard and should therefore be permitted to continue to discovery.

B. The Complaint Sufficiently Alleges a U.S. Nexus.

The defense argues that first question for the Court in the aftermath of the Supreme Court's *Kiobel* decision is whether the Complaint sufficiently pleads a U.S. nexus. Plaintiffs bring suit, in part, under the Alien Tort Statute ("ATS"), which provides that "[t]he district courts shall have original jurisdiction of any civil action by an alien for a tort, only, committed in violation of the law of nations or a treaty of the United States." 28 U.S.C. § 1350. The ATS is a jurisdictional statute that does not regulate conduct or afford relief, but rather "allows federal courts to recognize certain causes of action based on sufficiently definite norms of international law. *Kiobel v. Royal Dutch Petroleum Co.*, 133 S.Ct. 1659, 1664 (2013) (*see Sosa v. Alvarez-Machain*, 542 U.S. 692 (2004)). Although *Sosa* generally constrained the ATS as a jurisdictional statute, 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 to

rebut the presumption against extraterritoriality which otherwise would apply. Under the facts of *Kiobel* the necessary nexus did not exists 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 served to "help explain their business to potential investors." *Kiobel* at 1677.

Even apart from the legitimate questions raised by Plaintiffs about whether the "nexus" burden applies in this case,[27] 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 states 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 notes 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). Justice Alito comments 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).

Thus, although the Supreme Court found no extraterritorial application of the ATS based on the specific facts before it, the Court made clear that extraterritorial application may indeed apply to cases in which there is a sufficient connection between the tort committed and the U.S.

---

[27] *See, e.g., Sexual Minorities Uganda v. Lively,* No. 3:12-cv-30051-MAP (D. Mass. filed Mar. 14, 2012) (memorandum order denying defendants' motion to dismiss) rejecting extraterritorial restriction when "defendant and his or her conduct are based in this country." p. 5.

Because the Court only recently decided *Kiobel* in April of 2013, few courts have had the opportunity to analyze *Kiobel*'s "touch and concern" test. However, in *Mwani v. Bin Laden*, No. 99-125-JMF, 2013 WL 2325166 (D.D.C. May 29, 2013) the court found that a bombing of the United States embassy in Nairobi, Kenya "'touched and concerned' the United States with 'sufficient force' to displace the presumption against extraterritorial application of the ATS." *Id.* at *4. The court in *Mwani* stated that an attack on the United States Embassy in Nairobi 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" *Id.* (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. Mwani* demonstrates that a plaintiff can indeed rebut the presumption against extraterritoriality and that overt acts taking place in the U.S. in furtherance of a conspiracy are a factor for consideration in that inquiry.

Plaintiffs here have made sufficient allegations to withstand a motion to dismiss on the issue of U.S. nexus, even assuming they have that burden.[28] Along with their complaint, Plaintiffs submitted Exhibit A, presentation in English by Defendant Cisco Systems, Inc., – the U.S. Corporation – that suggests Cisco marketed and sold customized technology to the Chinese government that specifically enabled government officials to violate Plaintiffs' rights under international law.[29] A senior director of corporate communications at Cisco acknowledged that at least one of Cisco's engineers was involved in creating the presentation, but discovery can develop these facts and reveal the extent of U.S. involvement.[30] The complaint further alleges that Cisco's

---

[28] Plaintiffs have also claimed that extraterritoriality does not apply. Opposition at 13. Amicus addresses only whether a U.S. nexus has been sufficiently pled, assuming it is required.

[29] While Cisco has several Chinese subsidiaries, the Complaint alleges that the relevant acts were done by the American corporation and this allegation is supported by Exhibit A. The presentation is identified on every page as being the product of the American company, Cisco Systems, Inc.

[30] 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/ (last visited Aug. 14, 2013).

routers were customized by Cisco Systems, Inc. – again the U.S. corporation – for the purpose of persecuting and subjecting Plaintiffs to torture and inhumane treatment on the basis of their Internet activity.

Plaintiffs also explain in their complaint that Cisco is an American company headquartered in San Jose, California. Compl. ¶ 11. In fact, Cisco has over 36,000 U.S. employees (out of a total of over 75,000) according to its 2012 10-K report to the Securities and Exchange Commission.[31] 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.[32]

The specific factual allegations of U.S. overt acts at this juncture should be sufficient to overcome a motion to dismiss. They demonstrate that the actual degree of Cisco's U.S. involvement and whether it satisfies *Kiobel*'s "touch and concern" test (if it indeed applies) is a question of fact which must be decided after Plaintiffs have been given the opportunity to conduct discovery.

C. The Complaint Sufficient Alleges Actions by Cisco that Could Create ATS Liability

Turning to the merits, and again accepting arguendo Defendants' formulation of the relevant standards against which to assess Cisco's liability for its role in the violation of Plaintiffs' rights under the laws of nations, Plaintiffs' factual allegations are easily "enough to raise a right to relief above the speculative level ... on the assumption that all the allegations in the complaint are true (even if doubtful in fact)." *Twombly*, 127 S.Ct. at 1965. This is particularly true if, as it must, the court draw all plausible inference in the Plaintiffs' favor and presumes that general allegations

---

[31] Cisco Systems, Inc., *United States Securities and Exchange Commission, Form 10-K,* http://investor.cisco.com/sec.cfm?NavSection=SEC&DocType=Annual&Year=2012 (last visited Aug. 14, 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).

[32] *Id.*

embrace those specific facts that are necessary to support the claim," *Lujan v. Nat'l Wildlife Fed.*, 497 U.S. 871, 889 (1990).

1. ATS Liability Standards Alleged by the Defense Are Met by Plaintiffs Factual Allegations.

According to the defendants' formulation, ATS liability for aiding and abetting is available when the defendant provides: 1) 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 for that crime." *Aziz v. Alcolac, Inc.*, 658 F.3d 388, 396 (4th Cir. 2011).

In the alternative, a corporation may be liable if it has conspired to commit a human right violation. The district court of Maryland has already confirmed that "numerous U.S. and international bodies have recognized causes of action under ATS ... based on theories of conspiracy ..." *Lizarbe v. Rondon,* 642 F. Supp. 2d 473, 490 (D. Md. 2009). Defendants assert (and plaintiffs disagree) that the proper test was articulated by *Presbyterian Church of Sudan v. Talisman Energy, Inc.*, 582 F.3d 244 (2009): "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." *Id.* at 260 (citations omitted).

2. The Liability Standards Alleged by the Defense Are Sufficiently Alleged and Factually Supported by Evidence Available to the Court at this Juncture.

Plaintiffs' Complaint presents a variety of factual allegations that, taken together, state a claim for relief even under defendants' formulation. The Complaint alleges that Cisco engaged in the following conduct: 1) sales and marketing of the products toward the commission human rights violations, 2) technical customization of the products to better assist with human rights violations, 3) knowledge that the purchaser was using the products for gross human rights violations, 4) ongoing technical and other forms of support for the product.

These allegations are neither implausible nor conclusory. To the contrary, Plaintiffs' factual allegations are supported by specific evidence from the public record, in particular Cisco's

own statements and conduct. Cisco disagrees with Plaintiffs' interpretation of those statements and conduct, but that factual dispute is properly a matter for summary judgment or trial. Taking those allegations as true, and drawing all inferences in Plaintiffs favor, a jury could conclude that Cisco acted purposefully to either facilitate the commission of human rights abuses and/or participated in a common design to violate human rights under laws of nations sufficient under either aiding and abetting or conspiracy theories. That is all that is required at this stage.

(a) Marketing and Sale of the Product for Uses that Violate Human Rights.

Exhibit A to the Complaint contains not just allegations, but shocking evidence of a shared purpose and common design to facilitate human rights violations by the Chinese government against political dissidents. On page 57 of the presentation, in describing the benefits of with the Golden Shield Project to the Chinese government, the presentation notes that one of the goals is to "Combat Falun Gong evil religion and other hostilities." This can be reasonably construed as a reference to the use of the Golden Shield to facilitate human rights abuses, since Cisco knew that the Chinese government has committed and continues to commit gross human rights violations against the members of the Falun Gong religion along with democracy advocates like Plaintiffs, its surveillance tools can identify and track them. This statement alone presents facts sufficient to survive a motion to dismiss about whether Defendants had a sufficient "purpose" or "common design" to facilitate these activities by providing and supporting the Golden Shield technology necessary to do so.[33]

---

[33] Cisco appears to have confirmed its knowledge of the Chinese government's goal to violate human rights and at a minimum, created a question of fact about Cisco's purpose to meet that goal in a press release issued after Exhibit A became public in which its 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*, https://www.networkworld.com/community/node/27957 (last visited Aug. 14, 2013).

(b) Technical Customization of the Tools for the Purpose of Facilitating Human Rights Violations by China Against Dissidents.

The Complaint also alleges specific and articulable facts that support the conclusion that the "Golden Shield" sold to the Chinese government is not merely a general-purpose tool, but rather a product customized specifically to assist the Chinese government's persecution of certain dissident individuals and groups. FAC ¶¶ 30, 60-63, 71, 83, 87, 188, 200, 212, 224. Importantly, Exhibit A supports that conclusion by articulating the Chinese government's goal of "combatting" these elements as part of promotion of the Golden Shield. In response, Cisco simply denies that it engaged in any customization. Specifically, the Opposition states that in testimony before Congress, Cisco's Chairman and CEO Chandler made "clear that the security and filtering features of Cisco products are generic and not customized for particular users." Opposition at 7-8. When a factual allegation has been sufficiently made and is met with a factual denial, the case presents a classic question of disputed fact worthy of discovery and cannot be decided on a motion to dismiss.

(c) China's Well-Documented Practice of Engaging in Gross Human Rights Violations, Using Surveillance Technologies like Those Provided by Defendant.

The Complaint also sufficiently alleges first, that the Chinese government had a well-documented practice of gross human rights violations against democracy activists like Plaintiffs, and indeed against Plaintiffs themselves. This practice is also documented by the U.S. State Department, as noted above.

Cisco's knowledge of these practices is seen in the presentation itself, which directly references the use of the Golden Shield against political dissidents, referred to as the "other hostilities" along with a religious minority, the Falun Gong, which has also suffered a well-documented campaign of gross human rights abuses by the Chinese government. This is sufficient to survive a motion to dismiss.

(d) The Ongoing Relationship with China and Ongoing Support of the Customized Tools.

The Complaint alleges ongoing technical and customer support by Defendants, which

distinguishes this situation from one in which a vendor merely sells a product that is later used to commit human rights abuses. As described further below, EFF does not support ATS liability for vendors who merely sell technologies that are misused later. The Complaint plausibly alleges something different: an ongoing and intertwined relationship between Defendants and the Chinese government, involving support, customization and development of the technologies to facilitate human rights abuses.

3. 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. Liability under the ATS for technology vendors under either aiding and abetting or conspiracy theories must be carefully cabined. 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 to the Chinese government. Unlike commercial sales to the public, international law attaches to actions taken by state actors or taken under color of law, with only minimal exceptions. *See, e.g.*, *Kadic v. Karadzic*, 70 F.3d 232, 245 (2nd Cir. 1995). Thus, the sale of technologies to private actors for private use generally cannot serve as the basis for vendor liability under international law. This limitation also means that the chances that a company would unwittingly provide technologies for use in international human rights abuses are slim – government contracting is generally a sophisticated and eyes-open process whether the purchaser is the U.S. or the Chinese government.

Second, liability under the ATS only reaches specific, universal, and obligatory violations of international law.[34] *Sosa*, 542 U.S. at 732 (*quoting In re Estate of Marcos, Human Rights Litigation,* 25 F.3d 1467, 1475 (9th Cir. 1994)); *see also Kiobel*, at 1665. Thus, liability under the

[34] 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.

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, crimes against humanity, arbitrary arrest and detention and cruel, inhuman or degrading treatment. Liability under the ATS simply does not reach not garden-variety offenses or crimes.

Third, in this specific case the four factors noted above plainly differentiate this situation from one in which a company sells a dual-purpose product that is subsequently misused. Most important 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 Chinese government 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. Indeed, routers can be used for both lawful surveillance pursuant to a warrant or other legal process, and unlawful surveillance in violation of international law. Yet the facts alleged in the Complaint and supported by Exhibit A indicate that Defendants did far more than merely sell off-the-shelf routers to the Chinese government. Instead, they allege that Defendants knowingly customized their router-based technologies for use by the Chinese government in tracking, unmasking, surveilling and locating the disfavored speech of dissidents such as Plaintiffs. If Defendants specifically design and implement special features in their regular routers or other technologies to facilitate the Chinese government's commission of international human rights violations, liability is appropriate. Here, the allegations of these facts at a minimum support the denial of the motion to dismiss and the opening of discovery to determine where and what kind of customization was provided.

V. CONCLUSION

Based upon the foregoing, Plaintiffs have sufficiently alleged facts with state a claim against Defendants. The Motion to Dismiss should be denied.

Respectfully submitted,

/s/ Jan I. Berlage
Jan I. Berlage #23937
GOHN, HANKEY & STICHEL, LLP
201 North Charles Street
Baltimore, MD 21201
Phone: (410) 752-9300
Facsimile: (410) 752-2519
JBerlage@ghsllp.com

Cindy Cohn (*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
cindy@eff.org

Counsel for Amicus Curiae
Electronic Frontier Foundation

Dated: August 15, 2013

Motions

8:11-cv-01538-PJM Daobin et al v. CISCO Systems, Inc. et al

U.S. District Court

District of Maryland

Notice of Electronic Filing

The following transaction was entered by Berlage, Jan on 8/15/2013 at 4:33 PM EDT and filed on 8/15/2013

Case Name: Daobin et al v. CISCO Systems, Inc. et al
Case Number: 8:11-cv-01538-PJM
Filer: Electronic Frontier Foundation
Document Number: 52

Docket Text:
MOTION for Leave to File *Brief Amicus Curiae* by Electronic Frontier Foundation Responses due by 9/3/2013 (Attachments: # (1) Schedule 1)(Berlage, Jan)

8:11-cv-01538-PJM Notice has been electronically mailed to:

Daniel Sage Ward dan@wardlawdc.com, kerry@wardlawdc.com

Faith E Gay faithgay@quinnemanuel.com

Isaac Nesser isaacnesser@quinnemanuel.com

Jan Ingham Berlage jberlage@ghsllp.com

Kathleen M Sullivan kathleensullivan@quinnemanuel.com

Lincoln Owens Bisbee lbisbee@morganlewis.com

Taimur Rabbani trabbani@wardlawdc.com

8:11-cv-01538-PJM Notice will not be electronically delivered to:

The following document(s) are associated with this transaction:

Document description: Main Document
Original filename:n/a
Electronic document Stamp:
[STAMP dcecfStamp_ID=1046883720 [Date=8/15/2013] [FileNumber=4621933-0
] [613d6a365b3fbe0e76129d30b699833f9a9f1e9e25eddbb8dcc878d17812a95844b
07c579334c34d1dc68c8ac877dbcef386393c459e32a933276e6cf5b3ae7a]]
Document description: Schedule 1
Original filename:n/a
Electronic document Stamp:
[STAMP dcecfStamp_ID=1046883720 [Date=8/15/2013] [FileNumber=4621933-1
] [05e29418759ef440fcd78c3baed62dae8dc91ab8dac9290a17b807c40660f0c35a7
9c68dfdb137d48012e00324fcce204963786632a33f0e7575aa16ce89a604]]