09-1375-cr

To Be Argued By:
WILLIAM J. NARDINI

==========

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket Nos. 09-1375-cr (L)
09-1384-cr (XAP)

UNITED STATES OF AMERICA,
Appellee-Cross-Appellant,

-vs-

HASSAN ABU-JIHAAD, also known as PAUL HALL,
Defendant-Appellant-Cross Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT

==========

BRIEF FOR THE UNITED STATES OF AMERICA

==========

NORA R. DANNEHY
United States Attorney
District of Connecticut

ALEXIS COLLINS (E.D.N.Y.)
WILLIAM NARDINI (D. Conn.)
STEPHEN REYNOLDS (D. Conn.)
Assistant United States Attorneys

DAVID KRIS
Assistant Attorney General
National Security Division
U.S. Department of Justice

JOHN DE PUE
Senior Litigation Counsel
Counterterrorism Section

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

PURSUANT TO "BLUE BOOK" RULE 10.7, THE GOVERNMENT'S CITATION OF CASES DOES NOT INCLUDE "CERTIORARI DENIED" DISPOSITIONS THAT ARE MORE THAN TWO YEARS OLD.

STATUTES

RULES

OTHER AUTHORITIES

Statement of Jurisdiction

The district court (Kravitz, J.) had jurisdiction over this criminal prosecution. 18 U.S.C. § 3231. On April 3, 2009, judgment entered, and Abu-Jihaad noticed an appeal. JA34. This Court has jurisdiction to review the conviction. 28 U.S.C. § 1291.[1]

[1] The government is not pursuing its cross-appeal from the judgment of acquittal on Count One. No. 09-1384-cr (XAP).

Statement of Issues
Presented for Review

1. Did the district court properly deny Abu-Jihaad's motions for disclosure of FISA applications, orders and related materials, an adversary hearing, and suppression of FISA-derived evidence?

2. Did the district court abuse its discretion in admitting Abu-Jihaad's statements from recorded telephone conversations, excerpts from videos he ordered from Azzam Publications, and pages from the Azzam websites?

3. Was there sufficient evidence that Abu-Jihaad unlawfully disclosed national defense information to Azzam Publications?

4. Did the district court properly grant the government's motions for protective orders pursuant to Section 4 of CIPA and Rule16(d)?

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket Nos. 09-1375-cr (L)
09-1384-cr (XAP)

UNITED STATES OF AMERICA,
Appellee-Cross-Appellant,
-vs-

HASSAN ABU-JIHAAD, also known as PAUL R. HALL,
Defendant-Appellant-Cross Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT

BRIEF FOR THE UNITED STATES OF AMERICA

Preliminary Statement

In December 2003, British authorities found a diskette in a bedroom associated with Babar Ahmad, who ran Azzam Publications – an entity that maintained websites and published materials promoting jihad against the West. On the diskette was a file created in early 2001, which talked about the then-anticipated deployment of a U.S. naval battlegroup led by the *U.S.S. Constellation*. The

document listed classified information, including dates when ships were expected to be in Hawaii, Australia, and the Strait of Hormuz.

Investigators learned that in late 2000 and early 2001, Azzam was exchanging e-mails with the defendant, Hassan Abu-Jihaad, a sailor aboard the *U.S.S. Benfold* – a destroyer assigned to the *Constellation* battlegroup. As a signalman in the navigation division, Abu-Jihaad was among the limited circle of military personnel with access to the battlegroup's classified transit plan. Authorities recovered only a portion of Azzam's e-mail traffic, and found no message discussing the leak. But in recovered e-mails, Abu-Jihaad voiced strong support for jihadi attacks on U.S. forces, describing the bombing of the *U.S.S. Cole* as a "martyrdom operation." Other e-mails ordering jihadi materials showed that he closely followed the websites – including in late 2000, when Azzam asked readers to defend the Taliban against anticipated U.S. attacks, and when the *Benfold* was preparing for a Middle East deployment. Abu-Jihaad was the only member of the U.S. military that investigators were able to determine was communicating with Azzam in this period.

Some time after Abu-Jihaad left the Navy, his phone was wiretapped. Abu-Jihaad made thinly coded references to jihad during those calls. He talked about his ability to provide "hot meals," or current intelligence for attacking U.S. military bases. Most tellingly, he told one associate that he had not been "working . . . in the field of making meals . . . for . . . over . . . quatro years." Abu-Jihaad had been out of the Navy for four years.

After hearing the evidence, a jury found Abu-Jihaad guilty of leaking the information in the Battlegroup Document to Azzam. Abu-Jihaad now appeals his conviction for unauthorized disclosure of national security information, in violation of 18 U.S.C. § 793(d). He raises claims relating to the Foreign Intelligence Surveillance Act (FISA) and the Classified Information Procedures Act (CIPA). He also challenges the sufficiency of the evidence, as well as evidentiary rulings. As discussed below, his claims are meritless and his conviction should be affirmed.

Statement of the Case

On March 21, 2007, a grand jury returned a two-count indictment against Abu-Jihaad. JA4, 82-90. Count One charged that Abu-Jihaad provided material support to terrorists, in violation of 18 U.S.C. § 2339A. JA89-90. Count Two charged that Abu-Jihaad communicated national defense information to unauthorized persons, in violation of 18 U.S.C. § 793(d). *Id.*

On October 11, 2007, the government moved for a protective order under CIPA *in camera* and *ex parte*. SPA52-56; 2007 WL 2972623.

On January 31, 2008, the court (Kravitz, J.) granted in part and denied in part the government's motion in limine regarding the admissibility of certain statements by Abu-Jihaad. SPA85-96; 2008 WL 282368.

On February 4, 2008, the court granted the government's CIPA motion, holding that certain classified material submitted *ex parte* and *in camera* was not discoverable. SPA97-107.

On February 21, 2008, the court ruled on the admissibility of certain evidence, including jihadi videos Abu-Jihaad bought from Azzam, and written jihadi materials available on the websites. SPA108-20; 553 F.Supp.2d 121.

On February 22, 2008, the court ruled on the government's second CIPA motion, holding that the government had already provided impeachment material through discovery, and was not obligated to disclose materials in certain categories. SPA121-28; 2008 WL 596200.

On March 5, 2008, after five days of evidence, a jury found Abu-Jihaad guilty on both counts. JA93-96.

On March 4, 2009, the court granted Abu-Jihaad's motion for a judgment of acquittal on Count One, and denied the motion as to Count Two. SPA129-99; 600 F.Supp.2d 362.

On April 3, 2009, Abu-Jihaad was sentenced to the statutory maximum of 10 years in prison, followed by three years of supervised release. JA34. The same day, judgment entered, and Abu-Jihaad noticed his appeal. JA97-100.

Statement of Facts

Viewed in the light most favorable to the verdict, the evidence showed that Abu-Jihaad leaked classified information about the planned movements of a U.S. Navy battlegroup to Azzam Publications, which ran websites dedicated to jihad against the West.

A. Azzam Publications runs websites that promote violent jihad

From 1997 through 2002, London-based Azzam Publications ran websites promoting violent jihad against the West. JA248, 262, 367, 1522-1635. These included azzam.com and qoqaz.net. JA247. Azzam published video and audio recordings extolling exploits of the mujahideen (jihadi fighters) in Chechnya and Bosnia. JA248-50. Azzam glorified martyrdom in the name of jihad, with biographies "meant to show how individuals with no real connection to the jihad or to the mujahideen, including people living in western European countries and North America . . . could all of a sudden jump up and join the mujahideen and become a hero figure . . . . " JA285-90.

Azzam offered original material directly from mujahideen in hot spots around the globe. The website contained a "jihad photo library," with photos taken "by the foreign mujahideen in Chechnya," which were "exclusive to Azzam Publications." JA291, 1556. Viewers could download video clips of influential mujahideen leaders, JA297, or order longer videos by mail, JA299-

300, 1571-73. The website described the videos' content in the "Products" section. JA302-05, 1574-77, 1861.

In November 2000, the website warned readers of an imminent "Joint U.S.-Russian chemical attack on Afghanistan," targeting the Taliban. JA262, 1536-38. It reported that the U.S. assault was to retaliate for the bombing of the *U.S.S. Cole* in Yemen in October 2000, JA272, 1536 – an attack for which Al-Qaeda had publicly claimed credit, JA176. Azzam asked readers to help the Taliban by sending money or gas masks, or traveling to Afghanistan to provide battlefield medical services. JA279-80, 1536, 1548. The website linked to an article reporting that in 1998, the United States fired cruise missiles at Al-Qaeda's camps in retaliation for their bombing of U.S. embassies in East Africa. JA278-79, 1539-41. Azzam's direct appeal for assistance to the Taliban was unusually specific, even for its website, and solicited cash donations. JA281-82.

B. In 2003, British authorities find a computer file describing the movement of U.S. naval forces to the Persian Gulf in early 2001

On December 2, 2003, British authorities searched locations associated with Babar Ahmad, who was involved in Azzam Publications. JA156, 160-62, 1433-34. In one bedroom, they found a diskette and items relating to Ahmad and Azzam. JA186-97, 1436-94, 1845. Forensic analysis of the disk revealed several files, including "letter.doc," which the parties called the "Battlegroup Document."JA1428-30, 209-18. That file contained a

three-page unsigned document describing the anticipated deployment of U.S. naval forces to the Persian Gulf in early 2001. Interspersed were bracketed notations, suggesting that it was edited by someone other than the original author. The document predicted ship movements beginning on March 15, 2001, and therefore appeared to have been written before that date. The first page began:

> In the coming days the United States will be deploying a large naval/marine force to the Middle East.
>
> This will be a two group force: the Battle Group (BG) and the Amphibious Readiness Group (ARG) - these groups will be replacing the already deployed groups in the gulf.
>
> . . . .
>
> There is a possibility that the ships and submarines that are capable will carry out a strike against Afghanistan. Main targets: Usama and the Mujahideen, Taliban etc.
>
> . . . .
>
> Most of the ships that are part of the BG will deploy on March 15 2001 leaving their home ports out of California and Washington State. They will meet up with the other ships that are part of the BG which are stationed in Hawaii. Their first port stop is Hawaii on March 20, 2001, where some ships

> will load Tomahawk D missiles. The same missiles used on Afghanistan and Sudan. It has a warhead and 166 [mm?] fragment bomblets. Then the whole BG will head towards Australia. The main ship with high ranking officials will be at Sydney on April 6 2001, other ships - Melbourne, Perth, Bunbary etc. The BG will be going through the straits of Hormuz on the April 29 2001 at night . . . .

JA1428. Beneath was a diagram labeled "Formations Through St[r]aits," depicting the battlegroup in a two-column formation. Next came a ship-by-ship breakdown of the battlegroup, including the carrier *U.S.S. Constellation* and a destroyer named *U.S.S. Benfold*. JA1428-29.

The document also listed ships in the Amphibious Readiness Group: "These consist of three ships which are deploying out of homeport San Diego, March 14 2001." JA1429. The ARG itinerary was significantly less detailed: "The ARG port visit will be in South-East Asia before heading to the ME. Thailand (their favourite), Singapore, etc." JA1430. The document ended by assessing the forces' vulnerabilities:

> **Weakness:**
>
> They have nothing to stop a small craft with RPG etc, except their Seals' stinger missiles.
>
> **Deploy ops in Gulf 29 April - 04 October.**

29th APRIL is more likely the day through the Straits. For the whole of March is tax-free - a moral booster. Many sailors do not like the Gulf.

Please destroy message.

JA1430.

The diskette contained additional files relating to Azzam and its websites. One was entitled "For the guy in charge to read (01_08_01).zip." JA442-30, 1698, 1711-17. It listed passwords for Azzam's e-mail accounts, discussed how "our guy" edited material and "all the other guy has to do is put in html format and upload it," and talked about Azzam's inventory of books and videos. JA442-30-38. Another file instructed people to do certain things for Azzam, and to "request from Mr. T that the products backlog must be finished by Monday evening 10 p.m." JA442-39-40, 1720-21.

Forensic analysis of the file containing the Battlegroup Document strongly supported the inference that it was created and saved by a British citizen named Syed Talha Ahsan – the "Mr. T" who handled Azzam's products backlog – who then transmitted the disk to Babar Ahmad. The file's metadata matched files found on Ahsan's personal computer. JA442-25, 442-28, 442-44-48, 491, 1752-53, 1755-56, 1758-66. The file was opened and modified only twice: upon creation on April 2, 2001, and when last saved on April 12, 2001. JA442-23-24, 470-72. On that latter date, the graphic of the battlegroup's formation was created, and the document's "author" field

was manually changed from "S A Ahsan" to "Jon Greene." JA442-19-28, 1702, 1704, 1706. The Battlegroup Document was password protected, and the password was written on the cover of the floppy disk. JA442-17-19, 1701-02.

Agent Craig Bowling searched all electronic data accumulated during 6½ years of investigations, including computers seized from Ahsan and Ahmad, but found no traces of the information in the Battlegroup Document. JA442-53. Those computers contained no research relating to U.S. naval forces, the *Constellation* battlegroup, or an amphibious readiness group. *Id.* Nor did he find communications with "Jon Greene," or indeed anyone named Jon Greene who could have accessed the Navy information. JA483-84.

C. Abu-Jihaad exchanged e-mails with Azzam before and after the creation of the Battlegroup Document

Hassan Abu-Jihaad was a signalman on the destroyer *U.S.S. Benfold* during this period. He was born Paul Raphael Hall, but changed his name to "Hassan Abu-Jihaad" in 1997, a year before joining the Navy. JA378-79, 1773. Mujahideen typically choose as a nom de guerre an Arabic "kunya" beginning with "Abu" ("father of") JA285-86. "Jihad" means "holy struggle," and in the context of mujahideen "exclusively refers to individuals on a battlefield, fighting in the cause of Allah." JA262.

A search warrant on Azzam's Yahoo accounts yielded a number of e-mails that happened to have been retained. Agents found eleven e-mails between Azzam and Abu-Jihaad, demonstrating his support for jihad against the West. The messages spanned from August 21, 2000, through September 3, 2001. JA1495-1511. Some listed Abu-Jihaad's military e-mail addresses, JA1501-02, 1505-11, and others used his private e-mail address, JA1495-1500, 1503. Someone at Azzam saved Abu-Jihaad's military address in the address book for azzamproducts@yahoo.com. JA442-13-14, 442-51, 1512-14. No e-mails referenced the information in the Battlegroup Document, but they made clear that Abu-Jihaad and Azzam had additional correspondence that the government could not recover.

Some e-mails showed that Abu-Jihaad regularly visited the Azzam websites. In the earliest message recovered – August 21, 2000 – Abu-Jihaad followed up on previous correspondence with Azzam (apparently via physical mail), which was not recovered. JA391-95, 1495. He wrote to verify that Azzam received his order for "indocumentation on the bosnianwar . . . to be issued on SEP 4th" 2000. *Id.* This was a reference to the Azzam website, updated on August 13, 2000, inviting pre-orders of the video *Martyrs of Bosnia*. JA391-94, 1861. Azzam responded that they had received his order, but he had overpaid by $5. JA394-95, 1496-97. The original version of that e-mail was not recovered in the Yahoo account, having likely been deleted. JA398. But the text and abbreviated header information was embedded in Abu-Jihaad's reply. He suggested that Azzam add the $5 "to the

funds that you Brothers are spending the way of Allaah via videos, tapes and the great web sites Qoqaz & Azzam Pub.....etc." JA396, 1496-97. Abu-Jihaad and Azzam corresponded again in March and May 2001, discussing another order (again, the original of which the government did not recover) for videos from the website. JA406-09, 1498.

In his e-mails, Abu-Jihaad identified himself as a U.S. sailor aboard a warship deployed to the Persian Gulf. On May 15, 2001, Abu-Jihaad noted that he was in the "middle of this giant ucean," inquired about his order for *Chechnya from the Ashes*, and reported that his mother had received his order of *Russian Hell 2000*. JA1501. He listed his home address in California, as well as his hotmail address and his Navy e-mail address. *Id.* Three days later, Azzam sent an apologetic reply and promised to send the CD. JA1502. Abu-Jihaad again corresponded with Azzam in July 2001 about his video orders. JA1505-09. Writing from his Navy address, he explained that he had accidentally ordered a second copy of part 2 of *Russian Hell 2000* (which "will be a good gift for someone"), but apparently had not received *Russian Hell* part 1. He said he had previously given his military address (though it does not appear in other recovered e-mails), and asked whether that address was workable. JA1505-06. Azzam responded: "The address is OK as long as you think it is safe and you are confident that you will get our product." JA1507-08. Abu-Jihaad confirmed that Azzam should ship his order to his Navy address. JA1509.

Abu-Jihaad's e-mails left no doubt that he supported jihad against U.S. military forces. On July 19, 2001, Azzam sent an e-mail to Abu-Jihaad, thanking him for a previous message. Fortuitously, the text of Abu-Jihaad's earlier e-mail was embedded in Azzam's reply. JA433-37, 1503-04. He described himself as "a muslim station onboard a u.s. warship currently operating depolyed to the arabian gulf." *Id.* Abu-Jihaad praised the "psychological anxiety" among U.S. military forces "due to the martyrdom operation against the uss cole." *Id.* At a force-protection briefing, Navy officials warned that America faced "'an enemy with no borders, no government, no diplomats, nor a standing army that pledges allegiance to no state.'" *Id.* Abu-Jihaad praised these "Mujahideen" as "the true champions and soldiers of Allah." *Id.* During his three months in the Middle East, he saw "the effects of this psychological warfare taking a toll on junior and high ranking officers." *Id.* He signed as "Hassan," "a Brother serving a Kuffar [infidel] nation." JA1504. Abu-Jihaad wrote this while the *Benfold* was in the Persian Gulf. JA437-39, 1050, 1854-59. The incident praised by Abu-Jihaad as a "martyrdom operation" involved Al-Qaeda's suicide bombing of the *U.S.S. Cole* – a destroyer like the *Benfold* – off the coast of Yemen in October 2000. JA273-77, 440-41, 905.

Azzam praised Abu-Jihaad's support. "I trust that you are doing your best to make sure that the other brothers & sisters in uniform are reminded that their sole purpose of existence in this duniya [world] is purely to worship our Lord and Master, Allah . . . . Keep up with the Dawah [preaching Islam] and the psychlogical warefare. . . . From

just another slave of Allah at Azzam Publications." JA1503. The "reply-to" address for this e-mail was "qoqaz@azzam.com," to which readers were encouraged to send "e-mails of support, so that Azzam could demonstrate both its worldwide readership and the visceral effect that its materials were having on people." JA322-23, 442-3, 1638-55. *See* JA442-10-12, 1510-11 (September 2, 2001, e-mail from Abu-Jihaad, complimenting Azzam's coverage of Afghanistan, but opining that the Taliban were too lenient in declining to execute foreign aid workers who converted Muslims).

Abu-Jihaad's military e-mail address was saved in one of Azzam's electronic address books. JA442-13-14, 1512. Specifically, a user of azzamproducts@yahoo.com had saved "Abujihah@benfold.navy.mil." JA442-14. Yahoo turned over more than 23,000 e-mails to and from Azzam's accounts, but only a small portion of those addresses had been saved to Azzam's address books. JA442-14-15. Only a user of this Azzam account could have saved this address; it would not have been saved automatically. JA442-15.

Moreover, based on forensic analysis of the Yahoo information, Abu-Jihaad was the only member of the U.S. military in e-mail communication with Azzam during this period. JA380-84, 501-03. Agent Bowling searched for e-mail extensions such as .mil or .gov indicating use of a U.S. military or government account; for IP addresses associated with the Navy, or the military or government more generally; and for particular words unique to the Battlegroup Document itself, such as the ship names.

JA380-83. With one immaterial exception, Abu-Jihaad was the only correspondent with a .mil address in the pool of e-mails to and from Azzam. JA502-03.

D. Abu-Jihaad had access to the battlegroup's classified transit plans

In 2001, the U.S. Navy deployed a battlegroup led by the carrier *U.S.S. Constellation* to the Persian Gulf to enforce U.N.-mandated no-fly zones in Iraq, and to enforce the U.N. oil embargo against Iraq. JA521-23. The drafting of the group's transit plan from San Diego to the Middle East was a labor-intensive, months-long project, subject to frequent change. JA698. The *Constellation*'s 2001 transit plan was drafted by Quartermaster Chief Petty Officer Adam Conaway, who had spent nearly his entire career working in navigation. JA681-84, 697-99. Conaway and his supervisor would sit down and determine whether to use the northern route (via the Straits of Malacca) or southern route (via Australia), choose port calls, and determine the time needed to sail from San Diego to their area of operations. JA699-700, 707. He considered a range of variables, including the class of ships, their propulsion, and standard transit speeds. JA706. The plan often underwent several revisions before being finalized. JA700. As Conaway explained, "It's kind of a living document." JA714; *see* JA859-60.

The first iteration of the transit plan was circulated within the Navy on September 29, 2000, JA701, 1800, with successive revisions on October 3, 2000 (JA1804), December 20, 2000 (JA1809), February 10, 2001 (which

could not be located in Navy archives, JA710-12), and finally on February 24, 2001 (JA1814). Each revision had a general "milestones" section listing April 30, 2001, for the anticipated entry into the geographic region controlled by the U.S. Fifth Fleet. JA671. This was known as the "CHOP" point, referring to "change of operational control." JA551. The more detailed section of each transit plan, however, described precise dates, times, and locations for each milestone. This scheduled the CHOP for just before midnight on April 29. JA671-75, 707-08. Between the various revisions, Chief Conaway constantly adjusted the dates and locations for the battlegroup's Australian port calls. JA709-11. At the time of deployment from San Diego, there was no transit plan for the battlegroup's return from the Persian Gulf. JA826.

The final transit plan dated February 24, 2001, contained a port call that had not appeared in the September, October, or December 2000 revisions: a brief stop for the *Benfold* to load ammunition in Lualualei, Pearl Harbor, Hawaii on March 20, 2001. JA711-12, 733, 1814-18. This stop was first added in either the February 10 or 24 revision of the transit plan. JA711-13. The navigation division had to do significant last-minute work before deploying on March 15, adding charts for the Hawaii port call. JA866-67; *see* JA533, 686, 715, 808-09, 812-15, 863-64. The Hawaii stop was added because some of the *Benfold*'s training had cut into the crew's pre-deployment leave. JA867. As compensation, the Navy rewarded the *Benfold* crew with a liberty port call in Hawaii. *Id.* The *Benfold* was the only ship in the battlegroup to pull into

Pearl Harbor from San Diego for an ammunition onload. JA770, 868.

As a signalman, Abu-Jihaad was part of the limited circle of military personnel with a "secret" clearance and access to the *Benfold*'s transit plan. JA690, 818-19, 822-23, 850, 861, 1778. Signalmen on the *Benfold* were cross-training to learn quartermaster skills, since their rating was being phased out. JA791, 856. Abu-Jihaad participated in that cross-training. JA857. He regularly worked on the bridge (where the ship's charts and classified transit plans were stored in a chart room, JA801-02, 818-22), and the adjacent signal shack, JA803-07. Before deployment, signalmen worked alongside quartermasters for last-minute preparations of the charts. JA863-65; *see* JA819.

The transit plan was classified as "confidential." JA668, 672, 687, 1800-20. "Confidential" information is "information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe." JA692-93. A Navy manual indicates that "precise current or future operational deployment, locations of surface combatant ships," and "planned foreign port calls" are classified as "confidential" until after deployment or the host government has approved the visit. JA694-96, 1821-24. Diplomatic clearances sometimes are not approved until the day before a port call. JA739.

Advance knowledge of the battlegroup's route was not widely known, even aboard ship. The Navy did not

publicize in advance the dates of anticipated port calls or the dates for transiting the Strait of Hormuz. JA674. Petty Officer Josh Kelly testified that as deck seaman and later personnel specialist aboard the *Benfold*, he had no advance knowledge where the ship was going. JA921 ("No clue."). Before leaving San Diego in March, Kelly did not know which ports the ship would visit before reaching the Persian Gulf. JA926-28. He did not know whether the ship would take the northern or southern route. JA927.

If the disclosure had come from someone with broader access to classified information – for example, on the Navy's secure "SIPRnet" – the Battlegroup Document could have contained even more damaging national security information. JA716-18. Such access could have yielded more classified information about the battlegroup, as well as the Pacific Fleet's overall deployment plan. JA718, 810-11, 848, 861. Abu-Jihaad did not have SIPRnet access. JA809-10, 842.

E. Navy witnesses testify about the materiality of information in the Battlegroup Document to the national defense

Information about when particular ships would be in particular locations is relevant to the national defense. Retired Rear Admiral David C. Hart, Jr., who commanded the battlegroup, JA515, explained that ships can be particularly vulnerable while in port, JA539. They were "[a]bsolutely" more vulnerable during particular portions of their transits, JA539-40, such as the Strait of Hormuz,

a choke point where geography and vessel traffic narrow a ship's maneuverability, JA540-43, 908-09.

Although the Battlegroup Document contained some inaccuracies, Admiral Hart regarded it as a threat to the battlegroup's safety. Had he known about the Document, he would have "sought an opportunity to change the time and nature of our transit through the strait of Hormuz." JA550-51. Even though the Document predicted that April 29 was the most likely date for transiting the Strait of Hormuz, rather than the date for entering the Fifth Fleet area, he still would have been concerned because "we have just given away one of the key tactical elements that you like to have on your side, which is surprise." JA552. The most troubling aspect of the Document was "the time frame at which we would be operating in the Fifth Fleet area of responsibility and intent to try to transmit vulnerabilities, whether necessarily accurate or not, of the ships under my command." JA661. In asymmetrical warfare, it is critical for attackers to have advance information about a ship's future location. JA661-62; *see* JA910-11.

F. After his discharge, Abu-Jihaad talks about having been in the field of making "fresh meals" – that is, disclosing military intelligence

In late September 2006, the FBI in Rockford, Illinois, asked an informant – William Chrisman – to befriend a person named Derrick Shareef. JA977. Shareef came to live with Chrisman for three months, and introduced Chrisman to his friend Abu-Jihaad, who had left the Navy

and was then living in Phoenix, Arizona. JA979-80. Chrisman and Abu-Jihaad spoke by phone, webcam, and instant messaging. *Id.* The government had wiretapped Abu-Jihaad's telephone and recorded all phone conversations between the two, as well as conversations that Abu-Jihaad had with other people. JA981-82. The jury heard excerpts of four calls from late 2006.

Some calls showed that Abu-Jihaad was familiar with Azzam's websites. Abu-Jihaad referenced an article he had read about a "long time ago" in "the Pubs" (*cf.* JA1496 (Abu-Jihaad referring to "Azzam Pub" in e-mail)); and to "waaqiah" (an Azzam-run website, JA442-65). JA993-94, 3148.

Calls also showed that Abu-Jihaad was security-conscious and spoke in code. He referred to jihad as "J" or "7" (referring to the seventh heaven, for battlefield martyrs). JA990, 995, 3148. Abu-Jihaad cautioned that he didn't "like talking on the phone or, or internet . . . just for security purposes . . . ." JA996, 3150. He emphasized staying "tight" and not "introduc[ing] many people to . . . what you are." JA3151; *see* JA1006, 3158-59 (exhorting Shareef not to speak of associates, to "keep them secure" and use "kunyas" – not real names); JA3167 ("We can have all the conversations you want – me, you and my shredder . . . . no electronic components. You will be frisked at the door."). He warned that he doesn't "trust the phones. The phones are tapped. . . . About as tapped as the internet . . . ." JA998, 3153. He continued, "I'm also about . . . securing myself. I'm not gonna . . . hand myself to a Kafir [infidel]." JA3155. Abu-Jihaad wouldn't openly tell

a non-Muslim that he supported jihad: He wouldn't "sit there in front of the Kafir like, 'Yes I thought that was a good . . . M.O.' . . . . You don't tell the Kafir that." JA1000-01, 3155. (Abu-Jihaad elsewhere described the *Cole* bombing as a "martyrdom operation." JA433-37, 1503.)

Abu-Jihaad made coded references to supporting attacks on U.S. military bases. He spoke with Shareef, Chrisman, and a friend named Miguel Colon about "cold meals" and "fresh" or "hot meals." JA1002-05. Chrisman explained that during their conversations, Abu-Jihaad used the term "meal" to refer to "intelligence about military bases." JA1004. "Cold meals" meant "[o]utdated intelligence," whereas a "fresh meal" or a "hot meal" referred to current intelligence. JA1004-05. Abu-Jihaad told Shareef that he had talked about "L" (meaning "logistics"), but that "L" from Abu-Jihaad was "like a cold meal. 'Cuz it ain't fresh. . . . you should figure out, what a fresh meal is . . . if it ain't fresh, it's outdated. . . . ." JA1002-03, 3157.

In code, Abu-Jihaad also admitted having previously had access to military intelligence, and disclosing it. In one three-way conversation with Chrisman, Abu-Jihaad apologized for his lack of fresh military intelligence, but pointed Shareef to Colon, who recently left the military:

> And I said, and I'll say it again, with whatever I can give, that's beneficial, I'll give it to you. But . . . if it's cold turkey, I can't give it to you. . . . 'Cuz . . . if it's cold turkey – I'm talking about "L" you

> figure it out – . . . *I haven't been on that job,* so I don't – you know what I'm saying, I haven't been there . . . to see . . . what the fresh meal is.
>
> . . . .
>
> If I can't, if I can't give you the fresh meal – I ain't been there in "X" amount of years. . . .
>
> See what I'm saying? Now if . . . the Hispanic, if the Mexican, he just, was there a minute ago – he can give you a fresh meal. . . . So you put that together. . . . if it's in those terms, he can give you a fresh meal 'cuz, you know what I'm saying, he just finished his job, there, less than a month ago, or . . . two . . . . But I, I mean – in those terms and "L's," – I would be giving you a cold meal.

JA3161-62 (emphasis added). When Abu-Jihaad said he hadn't "been on that job," Chrisman understood him to mean that he had been out of the Navy for a while. JA1009. Later in that conversation, Abu-Jihaad again referred Shareef to his associate who could provide a "hot meal . . . ." JA3164. Chrisman understood the "Mexican," who "was there a minute ago," to be Miguel Colon, who left the Marine Corps in September 2006. JA1011-13, 1844.

Shortly afterward, Abu-Jihaad spoke with Colon. JA1017, 3171 ("I told 'em about a cold meal and a hot meal. And I ain't got nothing hot for you, homey."). Describing the earlier call, Abu-Jihaad said:

> I peep, I peep the game that he wants a hot meal. You know what I'm saying? . . . I don't know how to get him no hot meal. I told him I, *I ain't been working uh, in, in, in the field of making meals* and or, you know . . . . in a, *in a long time. I've been out of that for, uh, over uh, quatro years* you know.

JA1017-18, 3176 (emphasis added). Abu-Jihaad had been out of the Navy for four years.

Summary of Argument

1. The district court did not err by denying Abu-Jihaad's motions to suppress FISA-derived wiretap evidence, for an adversarial hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), and for disclosure of FISA applications, orders and related materials.

First, the district court correctly concluded that FISA as amended comports with the Fourth Amendment. This Court has twice ruled that FISA's requirements regarding probable cause, notice, particularity, duration and *ex parte* review by a neutral magistrate are constitutional. *United States v. Stewart*, 590 F.3d 93, 128-29 (2d Cir. 2009); *United States v. Duggan*, 743 F.2d 59, 73-78 (2d Cir. 1984). FISA's amended requirement that a high-ranking Executive official certify that a "significant purpose" of the collection is to obtain foreign-intelligence information is no less constitutional than the previous "primary purpose" standard. Since criminal prosecution can properly be used along with other techniques to disrupt

international terrorism and espionage by foreign powers, the government's interests in collecting foreign-intelligence information and law enforcement often overlap. The "primary purpose" standard imposed an artificial and unworkable separation between these two legitimate interests, hampering the effectuation of both. The "significant purpose" standard strikes a different but nonetheless reasonable balance between the government's need for foreign-intelligence information and privacy rights. Because it requires articulation of a significant foreign-intelligence purpose and precludes collection for the sole objective of criminal prosecution, it too comports with the Fourth Amendment.

Second, the district court properly held that the FISA collection was lawfully authorized. The classified record makes clear that there were ample facts to support a finding of probable cause to believe that the target was an agent of a foreign power at the time collection was authorized and that a significant purpose of the collection was to obtain foreign-intelligence information.

Third, the district court properly denied Abu-Jihaad's request for a *Franks* hearing because the classified record reveals no basis for finding that probable cause rested on any material misstatements.

Fourth, the district court did not abuse its discretion by reviewing the FISA applications, orders and related materials *in camera* and *ex parte* because disclosure was neither necessary to assess the legality of the collection nor required by due process. The classified record contains no

potential material misrepresentations, inaccuracies or irregularities that could trigger the need for disclosure and an adversary hearing. Moreover, since the district court was armed with knowledge of those facts that Abu-Jihaad believed were potentially misstated when it reviewed the FISA material, it was capable of determining the legality of the collection on its own. Furthermore, the classified record reveals that there was no exculpatory or impeachment information contained in the FISA material of which due process would require disclosure.

2. The district court did not abuse its broad discretion when it admitted Abu-Jihaad's statements from recorded telephone conversations, excerpts from videos that he ordered from Azzam Publications, or pages from Azzam websites. Abu-Jihaad's admissions were highly probative, demonstrating his familiarity with Azzam and his intense focus on secrecy. Abu-Jihaad's statements about his ability to provide support through his coded references to "hot meals" and "cold meals" were also highly probative of the conduct charged – namely, the provision of intelligence. Second, the clips of videos that Abu-Jihaad ordered from Azzam were directly relevant to his motives and intent. Any risk of unfair prejudice was low, because the clips were not overly graphic or gruesome. Third, the admission of materials available on the Azzam websites in 2000-2001 was highly probative of Abu-Jihaad's motives and intent, particularly given evidence that he frequently visited the sites during that period and even viewed them aboard the *U.S.S. Benfold*. Finally, for each category of challenged evidence, the court properly determined that its probative value was not substantially outweighed by unfair

prejudice, and it gave the jury careful limiting instructions regarding its permissible use.

3. There was sufficient evidence to conclude beyond a reasonable doubt that Abu-Jihaad leaked national defense information to Azzam. As a Navy signalman, Abu-Jihaad had access to the limited universe of classified information contained in the Battlegroup Document. The evidence pointed to an insider as the source of the Document, given its predictions of a Hawaii port call on March 20, 2001, that the *Constellation* would be in Sydney on April 6, and that April 29 would be the date for transiting the Strait of Hormuz. Although the classified transit plan called for the battlegroup to enter the Fifth Fleet operating area, rather than the Strait of Hormuz, on April 29, there was evidence that even sailors in the navigation division sometimes confused where these points were. Significantly, the Battlegroup Document did not make similar predictions of ship itineraries beyond what was in the transit plan to which Abu-Jihaad had access. Although the Battlegroup Document contained certain inaccuracies, those did not relate to classified information and reflected imperfect knowledge by someone conversant in military jargon – in other words, someone precisely like Abu-Jihaad. The jury was entitled to reject Abu-Jihaad's argument that the Battlegroup Document might have been compiled by an unknown researcher based on information publicly available on the internet. Nearly all the web pages introduced by the defense were posted on the internet *after* the leak had occurred, and none predicted March 20, April 6, or April 29 as dates in the *Constellation*'s westward transit.

E-mail traffic between Abu-Jihaad and Azzam showed that he had both a strong motive and opportunity to disclose the information in the Battlegroup Document. In e-mails between August 2000 and September 2001, he demonstrated his familiarity with the Azzam websites, bought jihadi videos, praised the recent bombing of the *U.S.S. Cole* as a "martyrdom operation," and disclosed his identity and military status. Although none of these e-mails made reference to the information in the Battlegroup Document, they make clear that the government was unable to recover the full array of communications between Abu-Jihaad and Azzam. Moreover, Abu-Jihaad was the only member of the U.S. military known to be in communication with Azzam during this period, and Abu-Jihaad's importance to Azzam is demonstrated by the fact that someone at Azzam took the unusual step of saving his e-mail address in their online address book.

Finally, during recorded conversations in 2006, Abu-Jihaad spoke in code about jihad, operational security, and his current ability to provide associates only with "cold meals" rather than "fresh meals" or "hot meals" – meaning that he could only provide them with outdated military intelligence. During one conversation, he explained to an associate: "I ain't been working . . . in the field of making meals . . . in a long time. I've been out of that for, uh, over uh, quatro years you know." Abu-Jihaad had left the Navy four years earlier. The jury could reasonably interpret this as an admission that Abu-Jihaad had indeed been "in the field of making meals" – that is, leaking military intelligence – while in the Navy.

4. The district court did not abuse its discretion by granting the government's motions for relief from discovery pursuant to CIPA and reviewing them *in camera* and *ex parte*.

Even though the court's rulings pre-dated this Court's decision in *United States v. Aref*, 533 F.3d 72 (2d Cir. 2008), the court applied essentially the same standard adopted in *Aref*. The court examined the information proposed to be withheld from discovery, and determined whether it was discoverable and privileged. The court ordered disclosure in an unclassified form of information that was helpful and material to the defense, and permitted nondisclosure of information that did not meet that standard.

The classified record establishes that all of the classified information at issue in the government's motions was appropriately withheld. The majority was irrelevant to the case and therefore not discoverable. The discoverable information was correctly found to be privileged based on the government's submissions. Except for certain impeachment information that was disclosed to the defense in an unclassified form, none of the privileged information was helpful and material to the defense, but instead was either inculpatory or cumulative of information the defense already possessed. The court therefore properly exercised its discretion in granting the government's CIPA motions.

The court's review of the government's CIPA motions *in camera* and *ex parte* was also well within its discretion

based on long-standing Circuit precedent. Because the discoverability of the information at issue was the very issue for decision, disclosing the government's motion to the defense would have defeated the purpose of CIPA Section 4 and the discovery rules.

Argument

I. The district court properly denied Abu-Jihaad's motions for disclosure of FISA applications, orders and related materials, an adversary hearing and suppression of FISA-derived evidence

A. Relevant facts

After serving notice of intent to use information collected pursuant to orders issued by the Foreign Intelligence Surveillance Court ("FISC") under the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. §§ 1801 *et seq.* ("FISA"), Doc. 34, 117, the government produced to Abu-Jihaad a large amount of declassified telephone recordings and e-mails obtained pursuant to FISA, Doc. 160 at 7. While the government moved in limine to admit a number of declassified calls, only four were admitted at trial. Doc. 138; JA1425-26.

Abu-Jihaad moved to suppress the FISA-derived evidence; for disclosure of the FISA applications, orders and other materials (hereinafter "FISA Material"); and for an adversary hearing. He argued that FISA was

unconstitutional, that the FISA collection targeting him was illegal, and that the FISA applications must have been based on material misstatements.

In opposition, the government submitted a classified memorandum of law (Doc. 157); certified copies of the FISA Material (*id.* Sealed Exs. 5-12); and a classified declaration by the FBI regarding compliance with minimization procedures (*id.* Sealed Ex. 3). The government publicly filed a redacted version of its memorandum (Doc. 160, 161) and proposed order (Doc. 162). The government also asked the court to review the relevant FISA Material *in camera* and *ex parte* pursuant to 50 U.S.C.§§ 1806(f) and 1825(g). Doc. 160 at 3. In support, the government filed an unclassified declaration by then-Attorney General Mukasey stating that national security would be harmed should the materials be disclosed or subject to adversary hearing (Doc. 158), and a classified declaration of the Assistant Director of the FBI's Counterterrorism Division confirming the classified nature of information in the FISA materials and describing specific harms that disclosure could cause (Doc. 157, Sealed Ex. 2.)

After reviewing the submissions, the court concluded that: (1) *in camera, ex parte* review of the classified submissions was appropriate; (2) FISA is not facially unconstitutional; (3) the FISA collection here did not violate the Fourth Amendment or FISA; and (4) the FISA applications contained no material misrepresentations that would warrant a hearing. SPA68-78.

B. Governing law and standard of review

The Fourth Amendment protects the right "to be secure in [one's] persons, houses, papers and effects against unreasonable searches and seizures." The touchstone of the Fourth Amendment is reasonableness. *Michigan v. Fisher*, 130 S.Ct. 546, 548 (2009); *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 167 (2d Cir. 2008). To determine whether a search is reasonable, courts "examine the 'totality of the circumstances' to balance 'on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *Id.* at 172 (quoting *Samson v. California*, 547 U.S. 843, 848 (2006)).

In *United States v. United States Dist. Ct. for the East. Dist. of Michigan*, 407 U.S. 297 (1972) ("*Keith*"), the Supreme Court held that the Fourth Amendment requires prior judicial approval to conduct electronic surveillance for domestic security purposes. The Court, however, expressed no opinion about "the issues which may be involved with respect to activities of foreign powers and their agents." *Id.* at 321-22. It recognized that, even in cases involving domestic security surveillance, the "focus of [such] surveillance may be less precise than that directed against more conventional types of crime":

> Given these potential distinctions between Title III criminal surveillances and those involving domestic security, Congress may wish to consider protective standards for the latter which differ from

> those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of the citizen rights deserving protection.

Id. at 322-23 (citing *Camara v. Municipal Court*, 387 U.S. 523, 534-35 (1967)). In enacting FISA, Congress sought to "clarif[y] and advance[] the development of the law" relating to foreign intelligence so as to eliminate the "uncertainty" noted in *Keith,* S. Rep. 95-701 at 9 (reprinted in 1978 U.S.C.C.A.N. at 3977), and to "remove any doubt as to the lawfulness of such surveillance," *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984) (quoting H.R. Rep. 1283, pt. I, 95th Cong., 2d Sess. 25 (1978)).

1. The FISA statute

FISA established a court of designated judges ("FISC judges") with jurisdiction over applications for electronic surveillance or physical searches relating to the gathering of potential foreign-intelligence information. 50 U.S.C. § 1803. The statute permits certain presidentially authorized officials, acting through the Attorney General, to seek an order approving surveillance or search targeting a foreign power or an agent of a foreign power for the purpose of obtaining foreign-intelligence information. *Id.*

§§ 1802(b), 1822(c). A "foreign power" includes "a group engaged in international terrorism or activities in preparation therefor." *Id.* §§ 1801(a)(4), 1821(1). An "agent of a foreign power" includes any person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power." *Id.* §§ 1801(b)(2)(C), 1821(1). In the context of U.S. person targets, foreign-intelligence information includes information necessary to (a) the national defense or security of the United States, or (b) its ability to protect against an actual or potential attack, sabotage, international terrorism and clandestine intelligence activities by foreign powers or their agents. *Id.* §§ 1801(e), 1821(1). International terrorism includes violent activities that are a violation of federal or state criminal law. *Id.* §§ 1801(c), 1821(1).

To secure an order authorizing electronic surveillance under FISA, the application must meet certain statutory requirements. *Id.* § 1804. These include stating (1) the identity, or a description, of the target of the surveillance, *id.* § 1804(a)(2); and (2) the facts and circumstances justifying the applicant's belief that (a) the target is a foreign power or an agent thereof and (b) each facility or location to be surveilled is being used or is about to be used by the target, *id.* § 1804(a)(3). The requirements for applications seeking authorization for a physical search largely replicate those for electronic surveillance, *id.* § 1823(a), except that the application must establish probable cause to believe that the property to be searched (a) contains foreign intelligence and (b) is, or is about to be, owned, used, possessed by, or in transit to or from a

foreign power or agent of a foreign power. *Id.* § 1823(a)(3)(B) and (C).

When the target of collection is a U.S. person, the government must minimize the acquisition and retention of nonpublicly available information and prohibit its dissemination, consistent with the need to obtain, produce and disseminate foreign-intelligence information. *Id.* §§ 1801(h), 1805(c)(2)(A), 1824(c)(2)(A), 1821(4). Minimization procedures must be set forth in the application. *Id.* §§ 1804(a)(4), 1823(a)(4).

Applications for FISA collection must be certified by a high-ranking Executive official. *Id.* §§ 1804(a)(6), 1823(a)(6). The official must certify that the information sought is deemed to be foreign-intelligence information of a type described in 50 U.S.C. § 1801(e), and that the information cannot be reasonably obtained by normal investigative techniques, and state the bases for such facts. *Id.* §§ 1804(a)(6)(A), (C), (D) and (E), 1823(a)(6)(A), (C), (D) and (E).

Before October 26, 2001, the Executive official was also required to certify that "the purpose" of the surveillance was to intercept foreign-intelligence information. *Id.* §§ 1804(a)(7)(B), 1823(a)(7)(B) (2000). Several courts presumed that the "primary objective" of the surveillance must be to intercept foreign-intelligence information. *See, e.g., United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991); *Duggan*, 743 F.2d at 77. *But see United States v. Sarkissian*, 841 F.2d 959, 964-5 (9th Cir.

1988) (declining to decide whether "primary purpose" test applies to FISA).

On October 26, 2001, Congress amended FISA to provide that "a significant purpose" of a FISA surveillance or search had to be the gathering of foreign-intelligence information. *See* Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001), *codified at* 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B), *recodified at id.* §§ 1804(a)(6)(B), 1823(a)(6)(B). Its reasons for doing so were twofold. First, Congress sought to reverse the assumption created by several judicial decisions that in conducting foreign-intelligence surveillance, government authorities were required to decide which purpose – law enforcement or foreign-intelligence gathering – was "primary." *In Re Sealed Case*, 310 F.3d 717, 732-33 (FISA Ct. Rev. 2002) (quoting 147 Cong. Rec. S10591 (Oct. 11, 2001)). Second, in the wake of the September 11, 2001, attacks, Congress wanted to eliminate barriers to promptly sharing FISA-derived information with law enforcement authorities in instances where the primary purpose of the FISA collection was deemed to be for foreign intelligence. *Id.* at 733. If the government has a significant foreign-intelligence and criminal purpose, then it may obtain an order pursuant to FISA to investigate foreign-intelligence crimes, but not wholly unrelated ordinary crimes. *Id.* at 735-36. An application that states "a realistic option of dealing with the agent other than through criminal prosecution" or "articulates a broader objective than criminal prosecution – such as stopping an ongoing conspiracy – and includes other potential non-prosecution responses" meets the statutory test. *Id.* at 735.

To authorize collection, a FISC judge must find, among other things, that the facts in the application provide probable cause to believe that the target is a foreign power or an agent of such a power; and that facilities to be subject to surveillance are being used, or are about to be used, by the target or that the property to be searched contains foreign intelligence and is, or is about to be, owned, used, possessed by, or in transit to or from the target. 50 U.S.C. §§ 1805(a), 1824(a). The FISC judge may consider the target's past, current, and future activities. *Id.* §§ 1805(b), 1824(b). The FISC judge must also determine that the certifications are not clearly erroneous if the targets are U.S. persons. *Id.* §§ 1805(a)(4), 1824(a)(4).

2. The use of information collected via FISA in criminal cases

Although a significant purpose of the collection must be to obtain foreign-intelligence information, "otherwise valid FISA [collection] is not tainted simply because the government can anticipate that the fruits of such [collection] may later be used . . . as evidence in a criminal trial." *Duggan*, 743 F.2d at 78. To the contrary, the statute contemplates the introduction of information collected pursuant to FISA ("FISA information") in criminal prosecutions. 50 U.S.C. §§ 1806(b), 1825(c). As both Congress and this Court have recognized, "in many cases the concerns of the government with respect to foreign intelligence will overlap those with respect to law enforcement." *Duggan*, 743 F.2d at 78; *see also United States v. Stewart*, 590 F.3d 93, 128 (2d Cir. 2009).

Once the government intends to use or disclose FISA information in a criminal proceeding against an aggrieved person, it must notify that person and the court. 50 U.S.C. §§ 1806(c), 1825(d). The person may move to suppress the FISA information on the ground that it was unlawfully acquired or the collection was unlawfully conducted. *Id.* §§ 1806(e), 1825(f). While the court should presume the validity of representations submitted in support of the FISA application, *see Duggan*, 743 F.2d at 77 n.6, it should apply the same standard to the FISC's determination of probable cause as when reviewing a criminal search warrant pursuant to Fed.R.Crim.P. 41 or a criminal wiretap pursuant to 18 U.S.C. §§ 2510-2520.

Duggan instructs that due process concerns regarding fraudulent representations in a FISA application are governed by *Franks v. Delaware*, 438 U.S. 154 (1978). To obtain a hearing, the defendant must make "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included in the application and that the allegedly false statement was 'necessary' to the FISA [j]udge's approval of the application." *Duggan*, 77 F.3d at 77 n.6.

Because FISA Material contains sensitive classified information, the statute does not normally allow an aggrieved person to obtain it if the Attorney General states that disclosure or an adversarial hearing would harm national security. *See* 50 U.S.C. §§ 1806(f), 1825(g). Rather, *in camera*, *ex parte* review by the court of the applicable FISA applications, orders and related materials "is to be the rule." *Duggan*, 743 F.2d at 78 (internal

quotation marks omitted); *see also Stewart*, 590 F.3d at 128. While the court retains discretion to disclose portions of such FISA materials, it may do so "only if [it] decides that such disclosure is 'necessary to make an accurate determination of the legality of the surveillance' or is otherwise required by due process." *Duggan*, 743 F.2d at 78 (quoting 50 U.S.C. § 1806(f), citing *id.* § 1806(g)); *see also Stewart*, 590 F.3d at 128; 50 U.S.C. § 1825(g)-(h).

3. Standard of review

This Court reviews de novo a district court's legal conclusions about the interpretation and constitutionality of a statute, and resolving a suppression motion. *See, e.g.*, *United States v. Stewart*, 551 F.3d 187, 190-91 (2d Cir. 2009); *United States v. Awadallah*, 349 F.3d 42, 51 (2d Cir. 2003). Factual findings are reviewed for clear error. *Stewart*, 551 F.3d at 190-91.

This Court reviews for abuse of discretion a district court's refusal to disclose the substance of FISA material, *Duggan*, 743 F.2d at 78, or hold a suppression hearing, *In re Terrorist Bombings*, 552 F.3d at 165. There is no abuse of discretion absent, at minimum, misrepresentation of the facts or significant questions regarding compliance with minimization procedures. *Id.*

C. Discussion

1. FISA as amended is constitutional

Relying primarily upon conclusions drawn by a district court in *Mayfield v. United States*, 504 F.Supp.2d 1023 (D. Or. 2007), *rev'd on other grounds*, 588 F.3d 1252 (9th Cir. 2009), Abu-Jihaad argues that FISA as amended in 2001 is unconstitutional. This Court rejected most of these attacks, however, in *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984), and again in *United States v. Stewart*, 590 F.3d 93, 128-29 (2d Cir. 2009). The constitutionality of the "significant purpose" standard is an issue of first impression in this Circuit. *Id*. at 128. Because it represents a reasonable balance of privacy rights and the government's need to collect foreign intelligence, the amendment does not vitiate the statute's constitutionality.

Significant Purpose Standard. Abu-Jihaad reasons that the "significant purpose" standard improperly permits executive officials to bypass Fourth Amendment probable cause requirements in gathering evidence for a criminal prosecution through the employment of statutory standards governing foreign-intelligence surveillance. *See Mayfield*, 504 F.Supp.2d at 1037; Def. Br. at 24-27. This argument, however, relies on a flawed dichotomy between foreign-intelligence and law-enforcement investigations of foreign-intelligence crimes, and disregards the common-sense fact that criminal prosecution is often quite properly "used as part of an integrated effort to counter the malign efforts of a foreign power in a foreign intelligence

investigation." *In re Sealed Case*, 310 F.3d at 735, 746; *also In re Terrorist Bombings*, 552 F.3d at 172.

It is important to note that the statutory language never required a showing that the primary purpose of the FISA collection was not the prosecution of foreign-intelligence crimes. *See In re Sealed Case*, 310 F.3d at 723, 725, 727. Although the original version of FISA required the government to certify that the purpose of FISA surveillance was to obtain foreign-intelligence information, one of the key purposes of FISA surveillance Congress contemplated when it originally enacted FISA was the collection of evidence to prosecute foreign-intelligence crimes:

> [T]he definition of foreign intelligence information includes evidence of crimes such as espionage, sabotage or terrorism. Indeed, it is virtually impossible to read the 1978 FISA to exclude from its purpose the prosecution of foreign intelligence crimes, most importantly because, as we have noted, the definition of an agent of a foreign power – if he or she is a U.S. person – is grounded on criminal conduct.

Id. at 723; *see also* 50 U.S.C. §§ 1801(b)(2)(C), (c), (e)(1)(B). Since it was designed to gather foreign-intelligence information, which may include evidence of crimes, the FISA statute, as originally found constitutional by *Duggan*, always permitted collection of material to

gather evidence to prosecute foreign-intelligence crimes such as terrorism or espionage.[2]

The statutory language requiring that "a purpose" be to collect foreign-intelligence information was originally interpreted to require that it be the "primary purpose," based on *United States v. Truong Dinh Hung*, 629 F.2d 908, 915-16 (4th Cir. 1980). *See In re Sealed Case*, 310 F.3d at 725. *Truong,* however, dealt with a very different circumstance – namely, the standard for the President to exercise his inherent authority to conduct *warrantless searches* for foreign-intelligence information, and not the constitutional threshold for conducting foreign-intelligence surveillance pursuant to a judicially authorized FISA order. Thus, the *Truong* standard (which Abu-Jihaad urges) was improperly superimposed by courts upon the statutory language of FISA. *In re Sealed Case*, 310 F.3d at 742-44.

Consistent with its constitutional latitude to tailor warrant requirements to the needs of foreign-intelligence and national security investigations, *see Keith*, 407 U.S. at

---

[2] Congress explicitly recognized that "intelligence and criminal law enforcement tend to merge" since FISA collection targeting U.S. persons "is part of an investigative process often designed to protect against the commission of serious crimes such as espionage . . . and terrorist acts committed by or on behalf of foreign powers." *See* S. Rep. 95-701, 95th Cong. 2d Sess., at 10-11, reprinted in 1978 U.S.C.C.A.N. 3973, 4032 (1978); H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., pt. 1 at 49 (1978).

322-23, Congress enacted the "significant purpose" standard in the wake of the September 11 attacks. The "substantial purpose" language was not intended to transform FISA into a mechanism for ferreting out domestic crime, but to make clear that law enforcement and foreign intelligence gathering are not mutually exclusive objectives. The Executive Branch would not have to choose which purpose was "primary" in regard to foreign-intelligence collection. *See In re Sealed Case*, 310 F.3d at 733 (citing legislative history), 735.

The fact that, at some point, the government determines that its obligation to interdict such conduct is best accomplished by prosecuting those involved – and to employ FISA-derived evidence for that purpose – does not transform FISC-authorized surveillance from a constitutionally permissible mechanism of detecting foreign threats to national security into an impermissible means of short-circuiting Fourth Amendment warrant requirements governing the investigation of domestic crime. As the FISA Court of Appeals explained in rejecting an identical claim:

> the false premise [undergirding the perceived need to adopt the latter standard] was the assertion that once the government moves to criminal prosecution, its 'foreign policy concerns' recede. . . . [T]hat is simply not true as it relates to counterintelligence. In that field, the government's primary purpose is to halt the espionage or terrorism efforts, and criminal prosecutions can be,

> and usually are, interrelated with other techniques used to frustrate a foreign power's efforts.

Id. at 743; *Truong*, 629 F.2d at 915 (acknowledging that "almost all foreign intelligence investigations are in part criminal investigations"). Because it requires articulation of a foreign-intelligence purpose to the collection and precludes collection for the sole objective of criminal prosecution, the statute still strikes a reasonable balance between privacy interests and the need to obtain foreign-intelligence information.

Duggan does not compel a different conclusion. In finding the original FISA statute constitutional, *Duggan* recognized that collection of foreign-intelligence information relating to counterintelligence and national security investigations is a valid government interest justifying procedures different from those required for warrants in criminal investigations. *Duggan*, 743 F.2d at 73. While *Duggan* mentioned that collection of foreign-intelligence information must be the "primary objective" of the surveillance, it never tied this standard to statutory language. *Id.* at 77; *also In re Sealed Case*, 310 F.3d at 726-27. Nor did the Court address the fact that the statute's definitions of foreign-intelligence information, international terrorism, and agent of a foreign power are all cast in terms of criminal conduct. *Id.* Conversely, later in the opinion, the Court recognized that Congress anticipated that "in many cases the concern of the government with respect to foreign intelligence will overlap those with respect to law enforcement." *Duggan*, 743 F.2d at 78. Consequently, the Court rejected the

notion that domestic law enforcement concerns preclude authorization of FISA collection as a constitutional matter. *Id.* Given these statements, it is not clear that *Duggan* adopted the "primary purpose" standard, much less believed that the standard was central to its finding that FISA was constitutional.

Moreover, this Court recently refused to adopt *Truong's* "primary purpose standard" in a case addressing warrantless foreign-intelligence collection outside the United States precisely because it failed to account for the government's legitimate interest in interdicting terrorism or espionage through criminal prosecution. *In re Terrorist Bombings*, 552 F.3d at 171-72. The Court found "the distinction between a 'primary purpose' and other purposes [to be] inapt." *Id.* Thus, this Court should not now engraft the same false dichotomy onto FISC-authorized collection and should instead find that the "significant purpose" standard is constitutional.

Probable Cause. Abu-Jihaad maintains that FISA is unconstitutional because it permits a surveillance order based on probable cause to believe that the target is a foreign power and that the facilities or places to be surveilled are being used or about to be used by a foreign power or an agent of a foreign power. Def. Br. 27-28. He asserts, that, under the Fourth Amendment, the government must demonstrate probable cause that a crime has been or is about to be committed. The *Keith* Court rejected this premise, however, recognizing that the contents of a warrant application could vary according to the governmental interest to be vindicated and the nature

of the rights at issue, and that different standards may be compatible with the Fourth Amendment if they relate to balancing the government's legitimate need for intelligence information with the rights of our citizens. *Keith*, 407 U.S. at 322-23. In *Duggan*, this Court "[a] fortiori . . . reject[ed]" this argument as well: "We conclude that [FISA's probable cause] requirements provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign-intelligence information, and that FISA does not violate the probable cause requirement of the Fourth Amendment."[3] *Duggan*, 743 F.2d at 73-74 & n.5. Thus, his claim should be rejected.

Notice and Ex Parte Review. Next, Abu-Jihaad maintains that FISA fails to pass muster under the Fourth Amendment because it only requires notice to an

---

[3] Moreover, as the Seventh Circuit recently observed in *United States v. Ning Wen*, FISA's definition is not constitutionally problematic because "the administrative search cases" make plain that the "probable cause of which the Fourth Amendment speaks is not necessarily probable cause to believe that any law is being violated." 477 F.3d 896, 898 (7th Cir. 2007). Such principles carry over to FISA. "Probable cause to believe that a foreign agent is communicating with his controllers outside our borders makes an interception reasonable." *Id.*; *see also United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (Kennedy, J.) ("We find that the probable cause showing required by FISA is reasonable."); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (adopting holdings of *Cavanagh* and *Duggan* about adequacy of FISA's probable cause requirements).

aggrieved person against whom the government intends to use FISA information and because it provides for *in camera*, *ex parte* review of the underlying FISA Material. Def. Br. 29-30. This claim has also been previously rejected by this Court.

At the outset, Abu-Jihaad's argument should be summarily rejected because he lacks standing. Since he received due notice of the collection, his challenge to the notice provision is directed at the rights of others, not his own. *See Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978).

In any event, this Court held that FISA's original procedures (which included the same notice provision) were generally constitutional and that *ex parte*, *in camera* inspections of FISA applications, orders and related materials pursuant to Section 1806(f) do not deprive a defendant of due process. *Duggan*, 743 F.2d at 73, 78. Even in ordinary non-FISA cases, this Court has upheld *ex parte* consideration of suppression motions: "[A]dversary proceedings and full disclosure are not necessarily required for resolution of every issue raised by an electronic surveillance. . . . To the contrary, such protections will not be required when the task is such that *in camera* procedures will adequately safeguard the defendant's Fourth Amendment rights." *United States v. Ajlouny*, 629 F.2d 830, 839 (2d Cir. 1980); *see also In re Terrorist Bombings*, 552 F.3d at 166-67.

Every other appellate court to address this issue has agreed. *See*, *e.g.*, *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005); *In re Sealed Case*, 310 F.3d at 741-

42; *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000); *United States v. Belfield*, 692 F. 2d 141, 149 (D.C. Cir. 1982). This unanimity is for good reason, because "notice that the surveillance has been conducted, even years after the event, may destroy a valuable intelligence advantage." *Belfield*, 692 F.2d at 145 n.8; *see also In re Terrorist Bombings*, 552 F.3d at 166-67. Consequently, FISA's notice and disclosure provisions are reasonable and do not violate the Fourth Amendment.

Particularity. Abu-Jihaad further claims that FISA improperly fails to require particularization in the surveillance application with respect to the offenses under investigation or the conversations to be intercepted. Def. Br. 30-31. Since this aspect of FISA has remained the same since *Duggan*, this argument too is wanting.

As with other distinctive features of FISA, its particularization components are tailored to intelligence surveillance rather than to ferreting out ongoing criminal activity. Even so, they compare favorably with the particularity requirements governing domestic law enforcement surveillance under Title III. For example, Title III requires probable cause to believe that communications concerning the specified crime will be obtained through the interception and that the targeted facility is being used in connection with the commission of a crime or are leased to or used by an individual – but not necessarily the target – committing the crime. 18 U.S.C. § 2518(3)(b), (d). In contrast, FISA requires probable cause to believe that the targeted facilities or property is being used or about to be used by an agent of a foreign

power, 50 U.S.C. § 1805(a)(2)(B), following a "detailed description" "of the nature of the information sought and the type of communications or activities to be subjected to the surveillance," and certification by a senior official that "the information sought [is] foreign intelligence information," *id.* §§ 1804(a)(4), 1804(a)(6)(a). *See also id.* §§ 1823(a)(2), 1823(a)(6)(A), 1824(a)(2)(B). In short, "FISA requires less of a nexus between the facility and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications." *In Re Sealed Case*, 310 F.3d at 740. As the district court observed, the requirements that the FISC judge examine the government's representations that the proposed target of surveillance is an agent of a foreign power and that the targeted premises are being used by the agent, more than adequately ensure particularization. SPA71; *see also Cavanagh*, 807 F.2d at 791.

Neutral and Detached Magistrate. Abu-Jihaad also maintains that, contrary to the Fourth Amendment, FISA fails to require that an interception order be issued by a "neutral and detached magistrate" because he is required to accept the certifications of the applicant unless they are "clearly erroneous." Def. Br. 31-32. This claim too is foreclosed by *Duggan*. *See Stewart*, 590 F.3d at 127-28.

Although it is true that judicial review of FISA applications is more circumscribed in some ways than that of search warrant applications, it is no rubber stamp. The certifications required by Section 1804 must be made by a high-ranking official, which provides an important check against reckless and arbitrary actions by law enforcement

officers. *See United States v. Bianco*, 998 F.2d 1112, 1124 (2d Cir. 1993) (requiring high-ranking official to authorize surveillance is "protection against arbitrary surveillance"). Moreover, whatever the boundaries of the "clearly erroneous" standard, the FISC judge retains substantial latitude to review the contents of FISA applications. Specific findings are required regarding probable cause and the sufficiency of the proposed minimization requirements. 50 U.S.C. §§ 1805(a)(2), (a)(3), 1824(a)(2), (a)(3). The FISC judge can demand additional information necessary to make such factual determinations, *see id.* §§ 1804(c), 1823(c), and to consider the target's past activities, as well as facts and circumstances relating to current or future activities of the target, *id.* §§ 1805(b), 1824(b). It can hardly be argued that the "FISA court provides anything other than neutral and responsible oversight of the government's activities in foreign intelligence surveillance." *Cavanagh*, 807 F.2d at 790.

Duration. Finally, Abu-Jihaad maintains that because FISA orders have a 90-day duration under Section 1805(d) (rather than the 30-day period authorized under Title III for domestic law enforcement surveillance without further judicial oversight), their duration is unconstitutionally long. Def. Br. 31-32. This difference, however, is based on "the nature of national security surveillance, which is often 'long range and involves the interrelationship of various types of information,'" and the longer surveillance period is balanced by continuing FISC oversight of minimization procedures. *In re Sealed Case*, 310 F.3d at 739 (quoting *Keith*, 407 U.S. at 322); *see In re Terrorist Bombings*, 552 F.3d at 175-76. Furthermore, "[g]iven the

targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities will involve multiple actors and complex plots." *In re Sealed Case*, 310 F.3d at 741. The extended duration will often be necessary simply to assess the types of information being communicated, and the sources and recipients of such information. Under such circumstances, the 90-day duration is reasonable. *See id.* at 746.[4]

2. The FISA collection was lawfully authorized

Abu-Jihaad claims that the court should have suppressed the FISA evidence because (a) there was no probable cause to believe he was an agent of a foreign power in 2006 based on his provision of intelligence to Azzam in 2001 or his conspiring to commit a domestic attack with Derrick Shareef; and (b) the FISA collection was for the sole purpose of gathering criminal evidence. Def. Br. 32-37. As Abu-Jihaad concedes, these arguments assume that the allegations in the FISA applications mirror those in the affidavit in support of the complaint in this case. Def. Br. 35 n.8.

---

[4] As for Abu-Jihaad's complaint concerning the absence of a return requirement, he does not explain why that is constitutionally mandated. In any event, FISA authorizes the issuing court to assess compliance with the order's minimization requirements "at or before the end of the period of time for which electronic surveillance is approved . . . ." 50 U.S.C. § 1805(d)(3).

As the classified record makes clear, however, these assertions are entirely unfounded. The FISA applications included ample probable cause to believe that the target of the collection was an agent of a foreign power and that a significant purpose of the collection was to obtain foreign-intelligence information. Indeed, the applications would have passed muster even if the "primary purpose" standard were required by FISA or the Constitution. The district court correctly upheld the legality of the collection.[5]

3. Abu-Jihaad was not entitled to a *Franks* hearing

Abu-Jihaad also asserts that the court wrongly denied a *Franks* hearing because the FISA applications misstated the accuracy and confidential nature of the information in the Battlegroup Document. Def. Br. 38-39. As the classified record makes clear, this argument is similarly misplaced. The FISA materials contained no misstatements regarding the Document, and the court correctly denied a hearing. SPA77-78.

---

[5] Even if the FISA collection were not lawfully authorized, the "good faith" exception to the exclusionary rule would apply. *United States v. Leon*, 468 U.S. 897 (1984). Under this exception, evidence is not suppressed if a reasonably well-trained officer would not know that the surveillance was illegal despite the FISC's order. *See United States v. Buck*, 813 F.2d 588, 592 (2d Cir. 1987). Moreover, admission of the four FISA-derived telephone calls would be harmless because the remaining evidence was sufficient for a reasonable jury to convict Abu-Jihaad.

4. The district court properly denied Abu-Jihaad's motion for disclosure of the FISA applications, orders and related materials

Finally, Abu-Jihaad argues that in light of his claims regarding lack of probable cause and the inaccuracy of the certifications, the court should have disclosed at least some portions of the FISA material. Def. Br. 59-62.

At noted above, the classified record makes clear that none of Abu-Jihaad's claims regarding misrepresentations and inaccuracies reflect the reality of the FISA applications. Even if Abu-Jihaad were right, however, the court still would not have been compelled to disclose any part of the FISA materials. Disclosure is only appropriate where necessary to accurately assess the legality of the collection or where due process requires. *See* 50 U.S.C. §§ 1806(f)-(g), 1825(g)-(h). Neither did *Duggan* mandate disclosure in such circumstances; it simply noted that disclosure *might* be required if the court's initial review revealed potential irregularities in the applications. *Duggan*, 743 F.2d at 78.

Here, disclosure was unnecessary. There were no material misrepresentations or potential irregularities. The court was made aware of those facts that Abu-Jihaad perceived as having been potentially misstated (Doc. 133 at 17-22, Exs. 1-7) and reviewed the materials keeping those facts in mind. SPA76. Thus, the court could assess the collection's legality without disclosing the FISA materials. Moreover, the FISA material contained no exculpatory or impeachment information of which due

process would require disclosure. Accordingly, the court did not abuse its discretion in denying disclosure.

II. The district court did not abuse its discretion in admitting Abu-Jihaad's recorded statements, excerpts from videos that he ordered from Azzam Publications, or pages from the Azzam websites

A. Relevant facts

Prior to trial, the government moved *in limine* to admit certain of Abu-Jihaad's recorded statements under Rules 801(d)(2)(A), 801(d)(2)(E), and/or 404(b). The court held a two-day evidentiary hearing on November 28 and 29, 2007, heard oral argument on January 4, 2008, and issued written rulings on January 9 and 31, 2008. The court denied the government's motion to admit certain statements in furtherance of an uncharged conspiracy. The court, however, granted the government's motion to admit other recorded statements by Abu-Jihaad under Rule 801(d)(2)(A) (admissions of a party opponent), finding that the probative value of those recordings outweighed any potential unfair prejudice. SPA85-96. The court reserved decision on whether it would admit additional statements under Rule 404(b), depending on how the evidence developed. *Id*. The jury ultimately heard ten excerpts from four calls recorded in late 2006, all admitted under Rule 801(d)(2)(A). JA3144-177. Those excerpts are described above in Section F of the Statement of Facts.

The court admitted short, pre-screened clips from three full-length videotapes that Abu-Jihaad ordered from

Azzam. The jury saw selected excerpts from *Martyrs of Bosnia*, after the court gave a careful limiting instruction. JA401-06, GE107a-107*i*. The video offered hagiographic descriptions of soldiers who died in jihad and included combat scenes, in which the videographer was just behind the fighters. JA402-04. Toward the end of the film, Ibn Khattab, leader of the foreign mujahideen in Bosnia, invited viewers to contact them through Azzam. JA294-96, 405-06. The jury watched brief clips from two additional videos that Abu-Jihaad ordered, *Russian Hell 2000*, GE108, and *Chechnya from the Ashes* (which included *Russian Hell 2000 Part II*), GE109a-109d. *Russian Hell 2000* included footage of mujahideen killing a Russian soldier in Chechnya. JA413-14. *Russian Hell 2000 Part II* included scenes with footage of a suicide truck bombing. JA424-25.

The court also admitted pages that were on the Azzam websites between August 2000 and March 2001 – when Abu-Jihaad's e-mails show that he was monitoring the sites. These pages included information about Azzam, JA1525-30, exhortations for readers to participate in jihad, JA1532-38, 1548-54, 1613-27, 1674-96, glorification of "martyrdom operations," JA1656-73, photos and videos depicting jihadi attacks in Chechnya, JA1556-70, advertisements for books, audiotapes, and videos promoting jihad, JA1571-83, 1630-35, Usama bin Laden's Declaration of War against the West, JA1587-1612, and "E-mails of Support" from readers, JA1638-55.

B. Governing law and standard of review

Rule 403 provides that "[a]lthough relevant, evidence may be excluded if its probative value is *substantially outweighed* by the danger of unfair prejudice, confusion of the issues, or misleading the jury . . . ." (Emphasis added). Unfair prejudice "speaks to the capacity of some concededly relevant evidence to lure the factfinder into declaring guilt on a ground different from proof specific to the offense charged," or "an undue tendency to suggest decision on an improper basis." *Old Chief v. United States*, 519 U.S. 172, 180 (1997) (internal quotation marks omitted).

"[W]hen reviewing a Rule 403 ruling," an appellate court "must review the evidence maximizing its probative value and minimizing its prejudicial effect." *United States v. Fabian*, 312 F.3d 550, 557 (2d Cir. 2002) (internal quotation marks omitted). This Court reviews the admission of evidence under Rule 403 only for abuse of discretion. *United States v. Bah*, 574 F.3d 106, 117 (2d Cir. 2009). Such rulings are reversed only if they are manifestly erroneous or wholly arbitrary and irrational. *See United States v. Yousef,* 327 F.3d 56, 156 (2d Cir. 2003); *United States v. Dhinsa*, 243 F.3d 635, 649 (2d Cir. 2001).

C. Discussion

1. The district court did not abuse its discretion by admitting Abu-Jihaad's own statements, showing his familiarity with Azzam, his interest in secrecy, and his coded references to intelligence about military facilities

The district court did not abuse its discretion when it admitted Abu-Jihaad's recorded statements. There is little that is more probative of a defendant's conduct, motives and intent.

To begin with, some of Abu-Jihaad's admissions demonstrated his familiarity with Azzam and its websites – the administrator of which possessed the Battlegroup Document. This evidence showed that Abu-Jihaad was aware of Azzam's support for jihad and that he authored the e-mail communications with Azzam. *See United States v. Cusack*, 229 F.3d 344, 348 (2d Cir. 2000) (per curiam) (evidence properly admitted to show defendant's knowledge).

Abu-Jihaad's interest in secrecy, his use of carefully coded references to jihad and his obsession with operational security were not only probative of consciousness of guilt, but also explained the absence of a forensic link between Abu-Jihaad and the Battlegroup Document itself. Indeed, a major focus of the defense was the absence of computer evidence linking Abu-Jihaad to the Battlegroup Document, and the absence of any e-mail

from Abu-Jihaad in which the intelligence was either transmitted or referenced. As the district court aptly noted, "Abu-Jihaad's rather intense focus on secrecy, use of code, and destruction of materials [wa]s surely relevant to issues that [were] contested in this case." SPA92.

Finally, Abu-Jihaad's statements about his ability to provide support through coded references to "hot meals" and "cold meals" related directly to the charges in this case – namely, leaking intelligence. A jury could have reasonably concluded that "meals" referred to intelligence that would be useful to strike U.S. military targets; that "making meals" referred to providing such intelligence; and that Abu-Jihaad's statement that he "ain't been working . . . in the field of making meals . . . in a long time. I've been out of that for uh, over uh, quatro years you know" was an admission that he previously did, in fact, provide such intelligence, and that such activity occurred over four years earlier – that is, while he was still in the military.

The high probative value of the defendant's statements was not substantially outweighed by any risk of unfair prejudice. This evidence related directly to the government's obligation to prove the requisite intent of the crimes charged – and a defendant's own statements are uniquely persuasive in that regard. Moreover, the defendant's statements were no more inflammatory than the serious charges in the case – (1) providing material support, knowing or intending that such support would be used in preparation for, or in carrying out a conspiracy to kill United States nationals; and (2) disclosing classified

information relating to the national defense with reason to believe that it could be used to injure the United States. *Cf. United States v. Livoti*, 196 F.3d 322, 326 (2d Cir. 1999) (upholding admission of evidence that "did not involve conduct more inflammatory than the charged crime"); *United States v. Kassir*, 2009 WL 976821 (S.D.N.Y. 2009) (same; high probative value of defendant's admissions that he killed people during jihad fighting was not substantially outweighed by the danger of unfair prejudice; evidence was uniquely persuasive regarding knowledge and intent; there was no less risky alternative proof that would have the same efficacy). Finally, when the evidence was admitted, the court carefully instructed the jury that: (1) Abu-Jihaad was not "charged with anything based on the conversations that you've just heard from 2006"; (2) "the events that form the basis of the charges in this case that you are deliberating on against Mr. Abu-Jihaad occurred in the year 2001 not 2006"; and (3) "you are not to speculate at any point about the nature of the investigation involving Mr. Shareef that Mr. Chrisman was involved with and whether or if any charges resulted from that investigation." JA1019-20.

Abu-Jihaad argues that the 2006 recordings had little probative value to a leak in 2001. Def. Br. 41. Yet the lapse of time, and the fact that they did not expressly mention the battlegroup information, relate only to the weight of the evidence, not its admissibility. As the court correctly held, "it is properly for the jury to determine whether the passage of time diminishes the strength of the inference[s] the government seeks to draw from the

evidence." SPA92 (citing *United States v. Schultz*, 333 F.3d 393, 414 (2d Cir. 2003)).

Abu-Jihaad also argues that his statements, about his ability to provide support, were effectively evidence of subsequent other acts improperly admitted under Rule 404(b). Def. Br. 42-44. This argument is misplaced. Abu-Jihaad's statements were admitted as *party admissions* under Rule 801(d)(2)(A), not *bad acts* under Rule 404(b). *See, e.g., United States v. Bibo-Rodriguez*, 922 F.2d 1398, 1400-02 (9th Cir. 1991); *see also United States v. Manafzadeh*, 592 F.2d 81, 89 (2d Cir. 1979) (finding defendant's subsequent statement that criminal conduct "had been done several times [before] and nothing ha[d] happened" was admission under Rule 801(d)(2)(A), not act subject to Rule 404(b)); *cf. United States v. Hammoud*, 381 F.3d 316, 340 n.11, 341 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005) (upholding admission of jihadi-related videotapes from defendant's apartment; "Rule 404(b) is simply not relevant here. To the extent the 'bad act' is the playing of the videotapes during Thursday night prayer meetings, it was intrinsic to the charged crime of providing material support to Hizballah"; excerpts were probative of defendant's intent and knowledge regarding Hizballah's aims).

2. The district court did not abuse its discretion by admitting carefully screened clips of Azzam videos that Abu-Jihaad ordered and Azzam webpages, subject to careful limiting instructions

The district court did not abuse its discretion by admitting the video clips or Azzam webpages.

First, the clips and webpages were directly relevant to the case and highly probative of Abu-Jihaad's motives and intent. Abu-Jihaad's e-mails with Azzam confirmed that he frequented their website both before and after his March 15, 2001, departure from San Diego. JA1496-97, 1505-06, 1509. Azzam posted detailed descriptions of the videos' content on its website, and a fellow sailor testified that Abu-Jihaad had shown him online clips aboard the *Benfold.* JA831-32, 1495, 1498, 1501, 1574-80, 1630-35. Abu-Jihaad ordered each video from Azzam in e-mails shown to the jury. The government's expert testified that the videos were popular among jihadists and were used by Azzam as a recruitment tool. JA302-05, 311. The videos and webpages glorified martyrdom and the killing of non-believers. Accordingly, the jury could reasonably rely on the content of the videos and webpages to determine Abu-Jihaad's motives and intent, including: (1) his knowledge of Azzam's support for terrorist groups – and hence their ability to forward intelligence to people who could attack the battlegroup; and (2) his intent to support jihad. *See United States v. Salameh,* 152 F.3d 88, 111 (2d Cir. 1998).

Second, the government had to answer the question why Abu-Jihaad would send information to terrorists who might blow up his own ship, or why Abu-Jihaad referred to the *Cole* bombing as a "martyrdom operation." JA1503-04. The videos and webpages answered these questions, because they glorified martyrdom, JA 1576-77, 1656-73 – indeed, they explained that martyrs never actually die but instead dwell in paradise, with a detailed explanation of the rewards a martyr could expect upon his death, GE107b, 107e.

In contrast to the highly probative nature of these materials, the risk of unfair prejudice was low. Despite Abu-Jihaad's claims, the video clips that the jury watched were not overly graphic. As the district court observed, many of the clips that depicted combat were "not particularly violent" and were less inflammatory than "nightly news dispatches from Baghdad" depicting the ongoing war in Iraq. SPA117. The risk of unfair prejudice did not "substantially outweigh" the probative value of the videos.

Additionally, the court conscientiously performed the requisite assessment of the videos under Rule 403. SPA118-20. The videos were admitted only after the court "watched each video in its entirety and also specifically reviewed those portions" that the government proposed to play. SPA116. The court carefully sought to prevent the jury from being exposed to inflammatory material that could cause them to judge the case on an improper basis. SPA118 (directing the government to shorten and excise

certain clips to avoid showing unnecessarily graphic images).

To minimize the risk of any unfair prejudice, the court also repeatedly gave cautionary instructions. It advised the jury of the proper use of the videos and webpages and warned them against passion, prejudice or bias. *See, e.g.*, JA257-61, 401, 415-16, 425-26, 1219-20. This instruction, submitted by the defense, Doc. 224, 234 at JA25-26, directed the jury to consider these materials only for the limited purpose of determining Abu-Jihaad's intent and knowledge and not as evidence that he in fact provided the battlegroup information. Juries are presumed to follow their instructions, *see, e.g., Britt v. Garcia*, 457 F.3d 264, 272 (2d Cir. 2006).

The government did not emphasize the video evidence during closing argument or otherwise. The government played each clip only once and referenced them only a few times during closing. JA1235, 1237, 1245, 1253-54, 1294-95. When the government did mention the videos, it followed the court's limiting instruction by citing them as evidence only of Azzam's participation in terrorist activity, Abu-Jihaad's knowledge of Azzam's capability to use the battlegroup information to further terrorist activity, or of his motive and intent in providing the information to Azzam. *Id.*

Finally, admission of these materials was entirely consistent with rulings in other terrorism-related cases. Courts have routinely admitted evidence of videos or other terrorism-related materials belonging to the defendant to

prove his knowledge, intent and motive. *See, e.g., Hammoud*, 381 F.3d at 342 (affirming admission of tapes belonging to defendant that depicted Hizballah military operations and rallies because probative of his knowledge of Hizballah's unlawful activities and his motive in raising funds for Hizballah); *see also United States v. Abdi*, 498 F.Supp.2d 1048, 1071-72 (S.D. Ohio 2007) (admitting images from al Qaeda websites found on defendant's computer and dissertation exhorting reader to prepare for jihad against infidels as probative of intent and motive in case alleging material support of terrorism).[6]

III. There was sufficient evidence that Abu-Jihaad disclosed national defense information to Azzam

A. Relevant facts

Judge Kravitz denied Abu-Jihaad's motion for acquittal on Count Two. He found sufficient evidence to conclude beyond a reasonable doubt that Abu-Jihaad leaked "closely held national defense information" – namely, (1) "that

---

[6] *United States v. Al Moayad*, 545 F.3d 139 (2d Cir. 2008), does not assist Abu-Jihaad. In *Al Moayad*, the district court improperly admitted highly emotional victim testimony describing a Hamas suicide bombing in Israel. The only evidence linking the defendants to the bombing was the fact that a Hamas representative had predicted the attack during a speech at a wedding the defendants attended. *Id.* at 147, 175. The evidence here, however, established a direct connection between Abu-Jihaad and the videos since he ordered them from Azzam and viewed Azzam videos online.

vessels would stop in Hawaii on March 20, 2001 to load ammunition"; (2) that the battlegroup would deploy from San Diego on March 15 and the *Constellation* would be in Sydney, Australia on April 6, 2001"; and (3) "that the battlegroup would transit the Strait of Hormuz at night on April 29, 2001." SPA164-65. While acknowledging that there was "evidence pointing in both directions," the court concluded that "when all of the reasonable inferences are accumulated in the light most favorable to the Government and the evidence is viewed in its totality," a rational jury could have found Abu-Jihaad guilty beyond a reasonable doubt. SPA172.

The court carefully surveyed the evidence. First, Abu-Jihaad's motive was clear, based on his frequent visits to the Azzam websites and his e-mail praising the *Cole* bombing as a "martyrdom operation." SPA172. Second, as a signalman, Abu-Jihaad had special access to the information in the Battlegroup Document, and the leak evidently came from someone with access *only* to the transit plan. SPA172-73. Third, Abu-Jihaad was in frequent contact with Azzam, and not all of their communications were recovered. SPA173. Abu-Jihaad was the only person with a military address that Azzam saved in its address books, and indeed the only military person (with one immaterial exception) communicating with Azzam during this period. *Id.* Fourth, the jury heard Abu-Jihaad's recorded conversations. When Abu-Jihaad said he had been out of the "field of making meals" for "over . . . quatro years," the jury could reasonably infer "that four years earlier he had been in the business of 'making meals' – that is, disclosing intelligence." SPA174.

Fifth, the inclusion of dates for port calls pointed to an inside source – particularly dates like the ammunition load in Hawaii on March 20, the *Constellation*'s decision to take the southern route across the Pacific, its Sydney port call on April 6, and the projected date for transiting the Strait of Hormuz. SPA174-75. The court noted that the document incorrectly described April 29 as the date for entering the Strait of Hormuz rather than the Fifth Fleet's area, and expressed doubt about whether Abu-Jihaad would have confused the two. SPA176. Nevertheless, the court found it "significant that every iteration of the Transit Plan showed the end of the battlegroup's passage as nighttime on April 29, precisely as noted in the Battlegroup Document," and that the date was linked to a tax benefit for sailors. *Id.* Finally, the Battlegroup Document ended: "**Please destroy message**." *Id.* Only an insider would include such a warning. The court reviewed the defense's remaining arguments, and concluded that they did not undermine the sufficiency of the evidence.

B. Governing law and standard of review

This Court has described the "heavy burden" that a defendant faces when challenging the sufficiency of the evidence:

> In considering such a challenge, we must credit every inference that could have been drawn in the government's favor, and affirm the conviction so long as, from the inferences reasonably drawn, the jury might fairly have concluded guilt beyond a reasonable doubt[.] We defer to the jury's

> determination of the weight of the evidence and the credibility of the witnesses, and to the jury's choice of the competing inferences that can be drawn from the evidence. Pieces of evidence must be viewed not in isolation but in conjunction, and the conviction must be upheld if any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt[.]

United States v. Reifler, 446 F.3d 65, 94-95 (2d Cir. 2006) (internal citations and quotation marks omitted).

A reviewing court applies this sufficiency test "to the totality of the government's case and not to each element, as each fact may gain color from others." *United States v. Guadagna*, 183 F.3d 122, 130 (2d Cir. 1999). The government need not disprove every reasonable hypothesis consistent with the defendant's innocence. *United States v. Glenn*, 312 F.3d 58, 63 (2d Cir. 2002); *United States v. Strauss*, 999 F.2d 692, 696 (2d Cir. 1993). A guilty verdict may be based solely on circumstantial evidence and reasonable inferences from that evidence. *Id.* "Circumstantial evidence in this respect is intrinsically no different from testimonial evidence. . . . In both, the jury must use its experience with people and events in weighing the probabilities. If the jury is convinced beyond a reasonable doubt, we can require no more." *Holland v. United States*, 348 U.S. 121, 140 (1954). "Circumstances altogether inconclusive, if separately considered, may, by their number and joint operation, especially when corroborated by moral coincidences, be sufficient to constitute conclusive proof." *United States v.*

Bieganowski, 313 F.3d 264, 278 (5th Cir. 2002) (citing *Coggeshall v. United States (the Slavers, Reindeer)*, 69 U.S. (2 Wall.) 383, 401 (1864)).

"The ultimate question is not whether we believe the evidence adduced at trial established defendant's guilt beyond a reasonable doubt, but whether any rational trier of fact could so find." *United States v. Payton*, 159 F.3d 49, 56 (2d Cir. 1998). In this regard, a court must be careful not to usurp the jury's role. *United States v. Autuori*, 212 F.3d 105, 114 (2d Cir. 2000). Caution is especially warranted because "jurors are entitled, and routinely encouraged, to rely on their common sense and experience in drawing inferences." *United States v. Huezo*, 546 F.3d 174, 182 (2d Cir. 2008).

This Court reviews de novo the district court's assessment of the sufficiency of the evidence. *United States v. Abdulle*, 564 F.3d 119, 125 (2d Cir. 2009).

C. Discussion

1. Abu-Jihaad had access to the limited universe of classified information contained in the Battlegroup Document – namely, the *Constellation* battlegroup's transit plan from San Diego to the Middle East

The evidence pointed to a Navy insider – Abu-Jihaad – as the source of the classified information in the Battlegroup Document. Most blatantly, the Document ended with a warning: "**Please destroy message.**"JA1430.

The jury could reasonably infer that such a warning indicated an insider who feared detection. Indeed, the Document contained closely held information about the dates when ships in the *Constellation* battlegroup would be in particular places on its westward transit – information to which Abu-Jihaad had access through the classified transit plan on the *Benfold.* Specifically, it reported that ammunition would be loaded in Hawaii on March 20, 2001; that the *Constellation* would be in Sydney on April 6, 2001; and that the battlegroup would be transiting the Strait of Hormuz on April 29, 2001.

The Navy personnel most intimately involved in planning the battlegroup's movements did not anticipate a stop in Hawaii until one month before departure. JA711-12, 733, 1814-18. The Hawaii stop appeared on no draft plans until February 10 or 24, 2001. JA1800-13. That port call was added only for the *Benfold*, because missile practice kept it at sea longer than anticipated before deployment. JA866-67. It is implausible that an outsider simply made a lucky guess that there would be a Hawaii port call on March 20 – especially considering that the standard sailing time between San Diego and Hawaii was six days, JA734, not the five days contained in the transit plan and accurately predicted in the Battlegroup Document, JA769-70.

Even if an outsider were lucky enough to guess a Hawaii stop on March 20, it would require greater luck to also guess that the *Constellation* would be in Sydney on April 6. JA1428. Ships could take either of two routes between San Diego and the Persian Gulf – either via

Southeast Asia or Australia. Although Admiral Hart testified that it wasn't a secret that the *Constellation* would be following the Australian route to the Persian Gulf, JA636, there was no evidence that such information was publicly available, much less that the precise dates of port calls were known to anyone outside the military. Indeed, the route and dates in the transit plans were all classified as "confidential." Because there are two routes west, the general public could not "predict prior to deployment the dates and times of . . . port calls and the strait of Hormuz transit . . . ." JA665. Another officer testified that he had often been deployed to the Persian Gulf, but his route was different every time. JA868. The *Constellation* and other ships had variously taken either route in past deployments. JA576-77, 1163-65, 1936; 1966. Moreover, two naval groups were leaving San Diego in March 2001, and it would have required inside knowledge to know which group would head north, and which would head south. Indeed, Petty Officer Kelly testified that before leaving San Diego in March, he did not know which port calls the *Benfold* would make before the Persian Gulf, or even whether the ship would take the northern or southern route. JA926-28.

Another indicator that the disclosure came from inside the military was the Battlegroup Document's focus on April 29, 2001, for transiting the Strait of Hormuz. In every iteration of the transit plan, just before midnight on April 29 was the time and date fixed for the battlegroup to enter the Fifth Fleet area. JA671-75, 707-08. People sometimes confused the Fifth Fleet CHOP line with the Strait of Hormuz, which marked the entry into the Persian

Gulf. JA551, 665. Even in the navigation division, one officer had observed confusion as to precisely where the Fifth Fleet CHOP line was. JA829. Those two points were separated by only about two days' sailing, JA603, which might not necessarily seem significant to sailors who had spent weeks transiting the Pacific Ocean to what they knew to be their ultimate destination: the Persian Gulf. The ease of such confusion was illustrated for the jury when two extraordinarily knowledgeable witnesses – a two-star admiral and a career navigator – offered dramatically different descriptions of where the CHOP line lay. *Compare* JA582-87, 3051-52 (Hart) *with* JA735-37, 3054 (Conaway). The transit plan simply identified the CHOP point by latitude and longitude, without any descriptors of where that point lay vis-à-vis the Persian Gulf. JA1818. If a person were disclosing information directly from the transit plan rather than a map, such confusion would have been easy – particularly for an inexperienced enlisted sailor like Abu-Jihaad, who was still being cross-trained about navigation. JA856-57. In any event, the Battlegroup Document accurately predicted that the April 29 date would be driven by the Navy's desire to boost morale by crossing into a tax-free zone before month's end. If an outsider were simply guessing, there is no reason for choosing *two* days before month's end. In short, the Battlegroup Document's focus on April 29 strongly indicates that it was based on the transit plan.

Significantly, the Battlegroup Document did *not* predict dates and milestones beyond the *Constellation*'s westbound transit. It did not predict dates for port calls in the Persian Gulf, or for the return home. Nor did the

Document predict port dates for the amphibious readiness group – which was leaving San Diego at the same time. Likewise, the Document did not predict dates or port calls for the "already deployed groups in the gulf," even though they would have been exiting the Persian Gulf around the same time. JA1094. In short, the fact that the Battlegroup Document predicted only the westward movements of the *Constellation* battlegroup strongly suggests that its source had access only to that group's transit plan.

As a signalman with "secret" clearance and access to the *Benfold*'s chart room, Abu-Jihaad had precisely that limited access to classified information – namely, to the *Constellation* group's westward transit plan, but not to the *Boxer*'s schedule, or the eastward tracks of returning ships. Abu-Jihaad was cross-training with quartermasters, and was involved in preparing the *Benfold*'s transit plan before the 2001 deployment. JA791, 856-57. Unlike the *Benfold*'s officers, Abu-Jihaad had no access to other classified information on the Navy's secure SIPRnet, such as the Pacific Fleet's deployment plan. JA717-18, 809-11, 842, 848, 861, 894. In short, Abu-Jihaad's access to classified information about ship movements was remarkably co-extensive with the Battlegroup Document's predictions.

Abu-Jihaad points to inaccuracies in the Battlegroup Document, in an effort to argue that he could not have been its source. For example, the Battlegroup Document contained a graphic depicting two parallel columns of ships as the "Formation Through St[r]aits," JA1428, even though the battlegroup actually used a single-column

formation unaccompanied by the submarines, JA639-41. The label "Formation Through St[r]aits," however, appeared only over the left-hand column; Admiral Hart testified that if the left column (with the heading) were placed over the right, the depicted formation would be more reasonable for transiting the Strait (minus the submarines). JA673-74. As another Navy witness testified, the formation actually used during a given transit would be chosen "immediately prior to the transit itself," after the ships left Australia. JA872.

Other inaccuracies did not relate to classified information, and reflected imperfect knowledge by someone conversant in military jargon. For example, Admiral Hart's title was COMCRUDESGRU1, not COMCRUDESRON1 as listed in the Battlegroup Document. JA548. He did not recall saying that the battlegroup would be sitting off the Pakistani coast with launch pads, but he often spoke to sailors before deployment, and it was not uncommon to participate in exercises with Pakistani forces. JA548-49. The Battlegroup Document correctly noted that SEALS were on the *Constellation,* even though they were not on other ships and had no Stinger missiles. JA654-56, 779-80, 783. To the extent there are errors in non-classified information in the Battlegroup Document, that would be expected from an enlisted sailor like Abu-Jihaad with brief tenure in the Navy, who would not be fully conversant in details like arms carried by SEALs. Indeed, Abu-Jihaad's e-mails reveal a less-than-meticulous person. Imperfections in the Battlegroup Document are exactly what would be expected from him.

The Battlegroup Document also correctly noted that the group's deployment to the Middle East would trigger tax benefits for sailors, though it misstated the month involved. For any month during which personnel serve one day within the Fifth Fleet operating area, that month is tax-free. JA619-21. Accordingly, by "chopping" into the Fifth Fleet area on April 30, the sailors enjoyed all of April tax-free. JA621-22. The Battlegroup Document erroneously stated that with an April 29 transit, March (rather than April) would be tax-free. JA1430. Yet the reference to March is so obviously mistaken that it does not suggest that an outsider was the Document's author.

2. Abu-Jihaad was the only member of the U.S. military known to be in contact with Azzam during this period, and his e-mails strongly sympathize with Azzam's advocacy of jihad against U.S. military forces

Abu-Jihaad was the only member of the U.S. military known to be communicating with Azzam in late 2000 and early 2001, when the battlegroup's deployment was being planned. JA502-03. Agents recovered eleven messages between Abu-Jihaad and Azzam between August 21, 2000, and September 3, 2001. JA383-84, 1495-1511. This was not their entire universe of contacts; the e-mails referred to other communications that the government did not recover. JA392-93, 410-11, 450-51, 462-63, 484-85, 1495, 1505-06.

Those monitoring Azzam's e-mail viewed Abu-Jihaad as important enough to save his e-mail address in an online address book. Agent Bowling recovered more than 23,000 e-mail messages to and from Azzam's accounts, but only a small portion of the addresses – including Abu-Jihaad's – were saved in Azzam's address books. JA442-13-15, 442-51, 1512. Only the account user for azzamproducts@yahoo.com could save an e-mail address, JA442-15, and Ahsan – the apparent creator of the file containing the Battlegroup Document – managed Azzam's products backlog, JA442-41, 442-48-51, 491, 1721.

Abu-Jihaad's e-mails with Azzam – remarkable for a U.S. sailor – clearly demonstrated his motive for leaking classified information. In late 2000 and early 2001, Azzam begged its readers to help the Taliban against anticipated U.S. attacks. JA270-82, 1536-41, 1548-54. The website spoke about missile strikes, JA278-79, 1536 – the very sort of attack that the battlegroup could mount. Azzam's website extolled the virtues of martyrdom, particularly when fighting infidels like Americans. JA285-90, 1656-73, 1682-96. Abu-Jihaad sympathized with these views in his e-mails, which showed that he ordered products marketed as martyrdom videos, and regularly visited Azzam's site and followed their reports on the Taliban. JA291-305, 391-95, 442-10-12, 1495, 1510-11, 1556, 1571-77, 1861.

Most disturbingly, Abu-Jihaad praised the bombing of the *U.S.S. Cole* as a "martyrdom operation." JA434-42-1, 1503. In an e-mail apparently designed to be posted on Azzam's "E-mails of Support" page, JA323-24, 1638-55,

Abu-Jihaad derided the United States as a "Kuffar [infidel] nation," and gave thanks to Allah because the "Mujahideen" were "american enemies," JA1504. Writing from the Persian Gulf, Abu-Jihaad was pleased that "you can truly see the effects of this psychological warfare taking a toll on junior and high ranking officers . . . ." JA1050, 1504, 1855.

Faced with this powerful evidence, Abu-Jihaad argues that he did not hide his sympathies for Azzam, using ship computers to view radical websites and videos in front of shipmates, using his real name when corresponding with Azzam, and arranging to receive martyrdom videos at his military address. Def. Br. 51. He argues that these are not the actions of a person who leaked classified material to Azzam. *Id.* This argument is undermined by his *Cole* e-mail, however, praising that bombing as a "martyrdom operation." One would hardly expect a U.S. sailor to write such a testimonial, designed to be posted on an "E-mails of Support" webpage, if he expected word to get back to the U.S. military. Notably, he did *not* list his full identity in the text of that e-mail. The jury could therefore infer that Abu-Jihaad distinguished between actions with which he was willing to associate publicly (such as watching or ordering videos) and those he was not (such as praising the *Cole* bombing, or, by extension, disclosing classified information).

3. The jury could reasonably interpret Abu-Jihaad's recorded statements as admissions that, while in the Navy, he leaked intelligence about U.S. military targets

In wiretapped calls with Derrick Shareef, William Chrisman, and Miguel Colon in late 2006, Abu-Jihaad repeatedly spoke in code about his current ability to provide them only with "cold meals" – outdated military intelligence. JA1004. He explained that Shareef could obtain "fresh" or "hot meals" – current military intelligence, JA1004-05 – from Colon ("the Mexican") who was in the military just a "minute ago." JA3161. (Colon was discharged from the Marines two months before. JA1011-13, 1844.) Abu-Jihaad essentially admitted having disclosed military intelligence in the past, explaining to Colon: "*I ain't been working . . . in the field of making meals . . . in a long time. I've been out of that for, uh, over uh, quatro years you know.*" JA1017-18, 3176 (emphasis added). Abu-Jihaad was discharged from the Navy four years earlier, in 2002. JA379, 1769. The jury could reasonably interpret Abu-Jihaad's statement that he had not been "working . . . in the field of making meals" for over four years as an admission that he provided such intelligence while he was in the military. SPA93.[7]

---

[7] Abu-Jihaad argues that the "guilty interpretation" of these words is no more compelling than the "innocent interpretation advocated by the defense," and that Chrisman "correctly understood the defendant to be saying only that he (continued...)

The inculpatory nature of Abu-Jihaad's admission was reinforced by his insistence upon using code words during these conversations. He repeatedly indicated to Shareef his unwillingness to speak openly about these and related matters. *E.g.,* JA3161 ("I'm talking about 'L' you figure it out"); *id.* ("Now if . . . the Hispanic, if the Mexican, he just, was there a minute ago – he can give you a fresh meal . . . . So you put that together."); JA3162 ("I can elaborate on that more if you want me to . . . to your face – not on the phone."); JA3164 ("I'm throwing it out – cold and, cold and hot meals, you know what I'm saying?"). *See* JA996, 3150; 998, 3153; 1006, 3157-59; 1014-15, 3167.

4. The jury was entitled to reject the defense theory that the Battlegroup Document was compiled from public-source information

On appeal, Abu-Jihaad renews his argument that publicly available information on the internet provided a "reasonable alternative explanation" for the Battlegroup Document, and that perhaps someone other than Abu-

---

[7] (...continued)
had been out of the Navy for many years and that he was therefore in no position to provide any current information." Def. Br. 56-57. This fails for two reasons. First, it is the jury's province to choose among competing inferences, and this Court will not second-guess such factual determinations. *See Reifler*, 446 F.3d at 94-95. Second, the portion of Chrisman's testimony referenced by Abu-Jihaad relates to an earlier call with Shareef (JA 1009, 3161), not to the call cited above, where Abu-Jihaad told Colon that he had not been "working . . . in the field of making meals" for over four years (JA1017-18, 3176).

Jihaad – whether Ahmad and Ahsan, or someone else "somewhere in the world" – might have been the author. Def. Br. 58. The jury was entitled to reject this speculative claim.

The evidence strongly pointed away from Ahmad or Ahsan as the source of the intelligence. The Battlegroup Document spoke about events to occur in "the coming days," beginning in mid-March 2001 – suggesting that the source material predated the computer file's creation (apparently by Ahsan) in April 2001. The file contains bracketed notations, sometimes including question marks, indicating that the original source material was edited by someone less familiar with military jargon. It appears that Ahsan then provided the Battlegroup Document to Ahmad, since it appears on a diskette found in a bedroom associated with Ahmad, which contained other files relating to the administration of Azzam. JA186-97, 1436-94, 1845. Agent Bowling testified that forensic examination of computers seized from both Ahmad and Ahsan uncovered no traces of research relating to the Battlegroup Document. JA442-53. The jury could reasonably conclude that neither Ahmad nor Ahsan was the source of the Battlegroup Document.

The jury reasonably concluded that the Battlegroup Document came from a source inside the Navy (namely, Abu-Jihaad) – not an unknown internet researcher "somewhere in the world." The defense introduced webpages from 2001, in an effort to show that the *Benfold*'s schedule would have been available in advance for someone researching on the internet. But with one

exception, these pages post-dated the battlegroup's deployment. For example, one of battlegroup ships – the *Thach* – posted a schedule on its website. JA2956-62. This website was retrieved in April 2001, however, and there was no evidence that it was posted before the *Thach* left San Diego on March 15; it did not appear to have a link for the March schedule at all; the schedule described each day simply as "Deployed," "Port Visit," or "Inport San Diego"; and port names were never added to the website, even after they were visited in March and April 2001. JA1166-67. Likewise, the *Boxer* posted webpages about its port visits only after they were completed. JA1168-71, 1183-84, 1864-70. Moreover, although the defense found articles talking about the battlegroup's Australian port calls, they were written in April 2001 – after the battlegroup left San Diego, and hence after the Battlegroup Document was written. JA1171-72. The only thing the defense was able to locate predating March 15 that discussed the *Constellation*'s deployment was an entry on the MIT alumni website dating to February 11, 2001. JA1132, 1875, 2968. In a class note, a recent graduate said he would be deploying for six months as a pilot aboard the *Constellation* from San Diego on March 15, 2001, and that he expected port calls in Sydney, Perth, Bahrain, and Dubai. JA1133. The jury could reasonably dismiss this isolated item as a source for the Battlegroup Document, given that it made no mention of Hawaii or the dates for anticipated port calls (as appear in the Document), and predicted port calls in Bahrain and Dubai (which did not appear in the Document).

Finally, publicly available information about the *Constellation* battlegroup would not have enabled a researcher to compile its anticipated route before its departure. As explained above in Part III.C.1, the jury could have found unreasonable, based on the trial evidence, that an outside researcher would have predicted the March 20 stop in Hawaii; stated that the *Constellation* would be in Sydney on April 6; or thought that April 29 would be the date for transiting the Strait of Hormuz.

IV. The district court did not err by granting the government's motions for protective orders pursuant to Section 4 of the Classified Information Procedures Act and Federal Rule of Criminal Procedure 16(d)

A. Relevant facts

On August 31 and December 22, 2007, the government filed with the Court Security Officer two classified motions for the district court's *in camera* and *ex parte* review.[8] Doc. 88, 165. Both motions sought protective orders over classified material pursuant to Section 4 of the Classified Information Procedures Act, 18 U.S.C. App. III ("CIPA") and Fed.R.Crim.P. 16(d)(1). Redacted versions of both motions and proposed orders were filed on the public docket. Doc. 89, 90, 165.

---

[8] The government refers to the motion filed on August 31, 2007, as the "First CIPA Motion" and the motion filed on December 22, 2007, as the "Second CIPA Motion."

These motions are available in the classified record. In general, both motions requested authorization to withhold from discovery certain classified material that the government did not intend to use during the case and was either not relevant or not helpful and material to the defense. Doc. 165 at 1; Doc. 89 at 2. The Second CIPA Motion also sought permission to provide unclassified substitutions for certain classified impeachment information that could not be disclosed in original form without jeopardizing national security interests. Doc. 165 at 1. Because these filings and the court's rulings predated this Court's decision in *United States v. Aref*, 533 F.3d 72 (2d Cir. 2008), the government's submissions conformed with the prevailing practice at the time. Namely, in support of each motion, the government submitted a classified declaration by a government official with original classification authority over the classified material in question, Doc. 165 at 2; Doc. 89 at 2, rather than a claim of privilege by "the head of the department which has control over the matter," *Aref*, 553 F.3d at 80. Each declaration established that the information at issue was properly classified pursuant to law and stated the harm that could arise from unauthorized disclosure of the information. SPA100, 122.

As the court directed, the government submitted a supplemental classified memorandum regarding each CIPA motion for *ex parte* review, with redacted versions filed publicly. Doc. 179, 218; SPA97, 122. The court held two *ex parte* meetings with the government regarding the Second CIPA motion, which were noticed on the public

docket and recorded to permit appellate review. SPA83, 121-22; Doc. 202.

Abu-Jihaad challenged the court's *ex parte* review of the government's motion and any protective order withholding discovery. Doc. 95, 98. The court rejected his argument, holding that *ex parte* review was necessary because the issue to be resolved was whether the material was subject to discovery at all. SPA54-55.

In February 2008, the court granted both of the government's CIPA motions and entered protective orders over the classified material at issue. SPA106-07, 128. With respect to the Second CIPA Motion, the court ordered the government to provide additional details regarding the discoverable impeachment information. SPA125. In ruling that the government's final substitutions provided Abu-Jihaad with all of the impeachment information to which he was entitled, the court noted that the defense had in fact used the information at a pretrial proceeding and therefore suffered *no* disadvantage from not having received the information in original form. *Id.*

B. Governing law and standard of review

1. Section 4 of CIPA

CIPA's procedures for handling classified information in criminal cases are designed "to protect and restrict the discovery of classified information in a way that does not impair the defendant's right to a fair trial." *Aref*, 533 F.2d

at 78 (alterations and internal quotation marks omitted). Section 4 of CIPA permits a court to

> authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove.

18 U.S.C. App. III § 4. This clarifies the court's power under Rule 16(d)(1) to issue protective orders denying or restricting discovery for good cause, including to protect national security information. *Aref*, 533 F.3d at 78.

Both CIPA Section 4 and Rule 16(d)(1) expressly authorize *ex parte* submissions. This Court has also authorized *ex parte* hearings to resolve classified motions seeking relief under these provisions. *Aref*, 533 F.3d at 81.

While the source of protection of classified information is grounded in the common-law state secrets privilege, the substantive standard that courts should apply in determining the propriety of relief from discovery of classified information is derived from the government-informant privilege established in *Roviaro v. United States*, 353 U.S. 53 (1957). *Aref*, 533 F.3d at 78-80. Applying that standard, the court first decides whether the classified information is discoverable. If so, then it must determine whether the state secrets privilege applies

because there is "a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged" and the privilege is lodged by the "head of the department which has control over the matter, after actual personal consideration by that officer." *Id.* at 80; *see also Stewart*, 590 F.3d at 131. If the information is discoverable but privileged, the court must determine whether it is helpful or material to the defense, in that it is useful to counter the government's case or bolster a defense. *Id.*; *Aref*, 533 F.3d at 80. If it is not discoverable or not helpful or material to the defense, then it need not be disclosed.

To be helpful, the information need not rise to the level of exculpatory material covered by *Brady v. Maryland*, 373 U.S. 83 (1963). *Stewart*, 590 F.3d at 131; *Aref*, 533 F.3d at 80. But information that is duplicative or cumulative to information already possessed by the defense need not be disclosed. *See*, *e.g.*, *United States v. Smith*, 780 F.2d 1102, 1108, 1110 (4th Cir. 1985).

When allowing the government to substitute a summary of classified information in discovery in lieu of original material, the court should assess whether the substitution would materially disadvantage the defense. *See United States v. Moussaoui*, 382 F.3d 453, 477 (4th Cir. 2004) (dealing with analogous provision in CIPA Section 6(c)(1)). "Precise, concrete equivalence" is not required. *See* H.R. Conf. Rep. No. 96-1436 at 12-13 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4307, 4310-11. Nor must the summary include irrelevant, unhelpful or nondiscoverable information; it must convey only the

arguably discoverable classified information. *See United States v. Rezaq*, 134 F.3d 1121, 1142 (D.C. Cir. 1998).

2. Standard of review

Both a district court's decision to issue a protective order under CIPA Section 4 and Rule 16(d)(1) and its determination of whether information is "helpful" or "material to the defense" is reviewed for abuse of discretion. *Stewart*, 590 F.3d at131; *Aref*, 533 F.3d at 80. When assessing the materiality of withheld information, this Court considers "not only the logical relationship between the information and the issues in the case, but also the importance of the information in light of the evidence as a whole." *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 93, 125 (2d Cir. 2008). A decision to permit substitutions of unclassified summaries for classified information is reviewed for abuse of discretion. *See*, *e.g.*, *United States v. Dumeisi*, 424 F.3d 566, 578 (7th Cir. 2005); *Rezaq*, 134 F.3d at 1142; *see also United States v. Rosen*, 557 F.3d 192, 199 (4th Cir. 2009).

C. Discussion

Abu-Jihaad challenges the *ex parte* consideration of the government's CIPA motions and asks this Court to carefully review the classified record. Def. Br. 62-63. When this Court does so, it will find that the court acted well within its discretion in reviewing the government's submissions *ex parte* and granting its motions.

1. The district court properly considered the government's motions *ex parte* and *in camera.*

The district court in this case did not unthinkingly accept the government's request for *ex parte* review, but instead thoughtfully considered whether such review was appropriate given the circumstances. SPA54-55. Its ruling that such review was appropriate to determine the underlying discoverability of the information at issue was within its discretion.

This Court has repeatedly held that *in camera*, *ex parte* hearings and review of motions to withhold information – whether classified or non-classified – is proper when determining whether that information is subject to disclosure. *See*, *e.g.*, *Stewart*, 590 F.3d at 132; *Aref*, 533 F.3d at 81; *United States v. Wolfson*, 55 F.3d 58, 60 (2d Cir. 1995) (affirming *ex parte* review of potential *Brady* information). The reason is very clear: To subject the question of whether particular information is discoverable to "an adversary hearing with defense knowledge" would defeat the very purpose of the discovery rules. *See Stewart*, 590 F.3d at 132 (quoting *Aref*, 533 F.3d at 81). With motions under CIPA Section 4, *ex parte* review can be critical because the purpose of that provision is to protect classified information from unnecessary disclosure. *See United States v. Apperson*, 441 F.3d 1162, 1193 n.8 (10th Cir. 2006); *United States v. O'Hara*, 301 F.3d 563, 568 (7th Cir. 2002). Nothing distinguishes this case from the many others in which courts have affirmed *in camera*, *ex parte* review of a motion under CIPA Section 4.

2. The district court did not abuse its discretion in granting the First or Second CIPA Motions

Even though its rulings pre-dated *Aref* by several months, the district court applied essentially the same standard outlined in that case. It properly ruled that the information sought to be withheld was either not discoverable or, if discoverable, was not helpful or material to the defense, and that the summary of discoverable impeachment information produced to the defense provided the same ability to make a defense as would disclosure of the original classified information.

First, as the classified record shows, much of the information at issue in the CIPA motions was not discoverable under Rule 16 or otherwise because it was irrelevant to the case. This information therefore was properly withheld under the first step of the *Aref* inquiry.

Second, based on the government's submissions, the court determined that the remaining information that was discoverable was indeed privileged. SPA100, 122. Even though the identity of the government officials claiming privilege differed from that subsequently required by *Aref*, the declarations asserted specific facts explaining the basis for the classification and the harm to national security that could arise should the classified information be revealed. They provided an adequate foundation for the court to determine the existence of "a reasonable danger that compulsion of the evidence will expose . . . matters which,

in the interest of national security, should not be divulged."[9] *Aref*, 533 F.3d at 80.

Having determined that this material was privileged, the court scrutinized the government's submission and properly determined that the information to be withheld was neither helpful nor material to the defense. SPA105-106, 125-28. As the classified record makes clear, this information was unhelpful and immaterial for a variety of reasons, particularly in light of the court's evidentiary rulings. To the extent the classified material contained discoverable impeachment information, the underlying information was fully disclosed in another form and the defense used it during the case.[10] SPA125.

---

[9] The government acknowledges the new requirement set forth in *Aref* but, as in that case, there is little benefit in remanding this case solely to have the appropriate department head assert the state secrets privilege. *See Stewart*, 590 F.3d at 132; *Aref*, 533 F.3d at 80.

[10] In assessing the materiality of the information to be withheld, the district court acted with extraordinary care to fully consider Abu-Jihaad's likely defenses. The court delayed ruling on the government's motions for several months until it held a hearing regarding contested evidence and learned more about those defenses. SPA97. Far from blindly accepting the government's submissions, the court requested additional briefing regarding the connections between the material to be withheld and other unclassified evidence that would be presented at trial. (*See*, *e.g.*, Doc. 179 at 1.) The court also ordered additional disclosure of details regarding impeachment

(continued...)

Even if the protective orders were improvidently issued, however, the defense was not prejudiced by lack of access to the withheld information. As the court noted, the vast majority of the classified information was either patently irrelevant to the case, inculpatory, or mirrored unclassified information that Abu-Jihaad already possessed. SPA105-06, 125-28. Indeed, the court noted that the defense had already demonstrably made use of some of this information in pre-trial proceedings and therefore could use it at trial. SPA105-06, 125-27. The court did not abuse its discretion in precluding discovery of classified information that at best was cumulative and at worst useless to the defense.

---

[10] (...continued)
information. SPA125. Abu-Jihaad's right to present a meaningful defense was amply protected.

CONCLUSION

The judgment of the district court should be affirmed.

Dated: February 10, 2010

Respectfully submitted,

NORA R. DANNEHY
United States Attorney
District of Connecticut

ALEXIS COLLINS (E.D.N.Y.)
WILLIAM NARDINI (D. Conn.)
STEPHEN REYNOLDS (D. Conn.)
Assistant United States Attorneys

DAVID KRIS
Assistant Attorney General
National Security Division
U.S. Department of Justice

JOHN DE PUE
Senior Litigation Counsel
Counterterrorism Section

CERTIFICATION PER FED. R. APP. P. 32(A)(7)(C)

This is to certify that the foregoing brief complies with the 21,000-word limitation authorized by order of this Court dated February 2, 2010. The brief is calculated by the word processing program to contain approximately 20,994 words, exclusive of the Table of Contents, Table of Authorities, this Certification, and the Addendum.

WILLIAM J. NARDINI
ASSISTANT U.S. ATTORNEY

ADDENDUM

18 U.S.C. § 793(d). Transmitting Defense Information

Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it;

. . .

Shall be fined under this title or imprisoned not more than ten years, or both.

18 U.S.C. Appendix 3 - Classified Information Procedures Act (CIPA)

§ 1. Definitions

(a) "Classified information", as used in this Act, means any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).

(b) "National security", as used in this Act, means the national defense and foreign relations of the United States.

§ 2. Pretrial conference

At any time after the filing of the indictment or information, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution. Following such motion, or on its own motion, the court shall promptly hold a pretrial conference to establish the timing of requests for discovery, the provision of notice required by section 5 of this Act, and the initiation of the procedure established by section 6 of this Act. In addition, at the pretrial conference the court may consider any matters which relate to classified information or which may promote a fair and expeditious trial. No admission made by the defendant or by any attorney for the defendant at such a conference may be used against the defendant

unless the admission is in writing and is signed by the defendant and by the attorney for the defendant.

§ 3. Protective orders

Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court of the United States.

§ 4. Discovery of classified information by defendants

The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

§ 5. Notice of defendant's intention to disclose classified information

(a) Notice by Defendant

If a defendant reasonably expects to disclose or to cause the disclosure of classified information in any manner in connection with any trial or pretrial proceeding involving the criminal prosecution of such defendant, the defendant shall, within the time specified by the court or, where no time is specified, within thirty days prior to trial, notify the attorney for the United States and the court in writing. Such notice shall include a brief description of the classified information. Whenever a defendant learns of additional classified information he reasonably expects to disclose at any such proceeding, he shall notify the attorney for the United States and the court in writing as soon as possible thereafter and shall include brief description of the classified information. No defendant shall disclose any information known or believed to be classified in connection with a trial or pretrial proceeding until notice has been given under this subsection and until the United States has been afforded a reasonable opportunity to seek a determination pursuant to the procedure set forth in section 6 of this Act, and until the time for the United States to appeal such determination under section 7 has expired or any appeal under section 7 by the United States is decided.

(b) Failure to Comply

If the defendant fails to comply with the requirements of subsection (a) the court may preclude disclosure of any classified information not made the subject of notification

and may prohibit the examination by the defendant of any witness with respect to any such information.

§ 6. Procedure for cases involving classified information

(a) Motion for Hearing

Within the time specified by the court for the filing of a motion under this section, the United States may request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding. Upon such a request, the court shall conduct such a hearing. Any hearing held pursuant to this subsection (or any portion of such hearing specified in the request of the Attorney General) shall be held in camera if the Attorney General certifies to the court in such petition that a public proceeding may result in the disclosure of classified information.. As to each item of classified information, the court shall set forth in writing the basis for its determination. Where the United States' motion under this subsection is filed prior to the trial or pretrial proceeding, the court shall rule prior to the commencement of the relevant proceeding.

(b) Notice

(1) Before any hearing is conducted pursuant to a request by the United States under subsection (a), the United States shall provide the defendant with notice of the classified information that is at issue. Such notice shall identify the specific classified information at issue whenever that information previously has been made

available to the defendant by the United States. When the United States has not previously made the information available to the defendant in connection with the case, the information may be described by generic category, in such form as the court may approve, rather than by identification of the specific information of concern to the United States.

(2) Whenever the United States request a hearing under subsection (a), the court, upon request of the defendant, may order the United States to provide the defendant, prior to trial, such details as to the portion of the indictment or information at issue in the hearing as are needed to give the defendant fair notice to prepare for the hearing.

(c) Alternative procedure for disclosure of classified information

(1) Upon any determination by the court authorizing the disclosure of specific classified information under the procedures established by this section, the United States may move that, in lieu of the disclosure of such specific classified information, the court order--,

(A) the substitute for such classified information of a statement admitting relevant facts that the specific classified information would tend to prove; or

(B) the substitution for such classified information of a summary of the specific classified information.

The court shall grant such a motion of the United States if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information. The court shall hold a hearing on any motion

under this section. Any such hearing shall be held in camera at the request of the Attorney General.

(2) The United States may, in connection with a motion under paragraph (1), submit to the court an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis for the classification of such information. If so requested by the United States, the court shall examine such affidavit in camera and ex parte.

(d) Sealing of records of in camera hearings

If at the close of an in camera hearing under this Act (or any portion of a hearing under this Act that is held in camera) the court determines that the classified information at issue may not be disclosed or elicited at the trial or pretrial proceeding, the record of such in camera hearing shall be sealed and preserved by the court for use in the event of an appeal. The defendant may seek reconsideration of the court's determination prior to or during trial.

(e) Prohibition on disclosure of classified information by defendant, relief for defendant when United States opposes disclosure

(1) Whenever the court denies a motion by the United States that it issue an order under subsection (c) and the United States files with the court an affidavit of the Attorney General objecting to disclosure of the classified information at issue, the court shall order that the defendant not disclose or cause the disclosure of such information.

(2) Whenever a defendant is prevented by an order under paragraph (1) from disclosing or causing the disclosure of classified information, the court shall dismiss the indictment or information; except that, when the court determines that the interests of justice would not be served by dismissal of the indictment or information, the court shall order such other action, in lieu of dismissing the indictment or information, as the court determines is appropriate. Such action may include, but need not be limited to--,

(A) dismissing specified counts of the indictment or information;

(B) finding against the United States on any issue as to which the excluded classified information relates; or

(C) striking or precluding all or part of the testimony of a witness.

An order under this paragraph shall not take effect until the court has afforded the United States an opportunity to appeal such order under section 7, and thereafter to withdraw its objection to the disclosure of the classified information at issue.

(f) Reciprocity

Whenever the court determines pursuant to subsection (a) that classified information may be disclosed in connection with a trial or pretrial proceeding, the court shall, unless the interests of fairness do not so require, order the United States to provide the defendant with the information it expects to use to rebut the classified information. The court may place the United States under a continuing duty to disclose such rebuttal information. If

the United States fails to comply with its obligation under this subsection, the court may exclude any evidence not made the subject of a required disclosure and may prohibit the examination by the United States of any witness with respect to such information

50 U.S.C. § 1801. Definitions

As used in this subchapter:

(a) "Foreign power" means--

(1) a foreign government or any component thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

(b) "Agent of a foreign power" means--

(1) any person other than a United States person, who-

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore;

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

(2) any person who--

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence

activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) "International terrorism" means activities that--

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended--

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) "Sabotage" means activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States.

(e) "Foreign intelligence information" means--

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) "Electronic surveillance" means--

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code.

(h) "Minimization procedures", with respect to electronic surveillance, means--

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of

nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless

the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

(j) "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

(o) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

(p) "Weapon of mass destruction" means--

(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;

(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;

(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in section 178 of Title 18) that is designed, intended, or has the capability to cause death, illness, or serious bodily injury to a significant number of persons; or

(4) any weapon that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.

50 U.S.C. § 1803. Designation of judges

(a) Court to hear applications and grant orders; record of denial; transmittal to court of review

(1) The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection (except when sitting en banc under paragraph (2)) shall hear the same application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this chapter, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b) of this section.

(2)(A) The court established under this subsection may, on its own initiative, or upon the request of the Government in any proceeding or a party under section 1861(f) of this title or paragraph (4) or (5) of section 1881a(h) of this title, hold a hearing or rehearing, en banc, when ordered by a majority of the judges that constitute such court upon a determination that--

(i) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or

(ii) the proceeding involves a question of exceptional importance.

(B) Any authority granted by this chapter to a judge of the court established under this subsection may be exercised by the court en banc. When exercising such authority, the court en banc shall comply with any requirements of this chapter on the exercise of such authority.

(C) For purposes of this paragraph, the court en banc shall consist of all judges who constitute the court established under this subsection.

(b) Court of review; record, transmittal to Supreme Court

The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which

shall have jurisdiction to review such decision.

(c) Expeditious conduct of proceedings; security measures for maintenance of records

Proceedings under this chapter shall be conducted as expeditiously as possible. The record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.

(d) Tenure

Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) of this section shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) of this section shall be designated for terms of three, five, and seven years.

(e)(1) Three judges designated under subsection (a) of this section who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) of this section as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have jurisdiction to review petitions filed pursuant to

section 1861(f)(1) or 1881a(h)(4) of this title.

(2) Not later than 60 days after March 9, 2006, the court established under subsection (a) of this section shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section 1861(f)(1) or 1881a(h)(4) of this title by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge.

(f)(1) A judge of the court established under subsection (a), the court established under subsection (b) or a judge of that court, or the Supreme Court of the United States or a justice of that court, may, in accordance with the rules of their respective courts, enter a stay of an order or an order modifying an order of the court established under subsection (a) or the court established under subsection (b) entered under any title of this chapter, while the court established under subsection (a) conducts a rehearing, while an appeal is pending to the court established under subsection (b), or while a petition of certiorari is pending in the Supreme Court of the United States, or during the pendency of any review by that court.

(2) The authority described in paragraph (1) shall apply to an order entered under any provision of this chapter.

(g)(1) The courts established pursuant to subsections (a) and (b) of this section may establish such rules and

procedures, and take such actions, as are reasonably necessary to administer their responsibilities under this chapter.

(2) The rules and procedures established under paragraph (1), and any modifications of such rules and procedures, shall be recorded, and shall be transmitted to the following:

(A) All of the judges on the court established pursuant to subsection (a) of this section.

(B) All of the judges on the court of review established pursuant to subsection (b) of this section.

(C) The Chief Justice of the United States.

(D) The Committee on the Judiciary of the Senate.

(E) The Select Committee on Intelligence of the Senate.

(F) The Committee on the Judiciary of the House of Representatives.

(G) The Permanent Select Committee on Intelligence of the House of Representatives.

(3) The transmissions required by paragraph (2) shall be submitted in unclassified form, but may include a classified annex.

(i) Nothing in this chapter shall be construed to reduce or contravene the inherent authority of the court established under subsection (a) to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court

50 U.S.C. § 1804. Applications for court orders

(a) Submission by Federal officer; approval of Attorney General; contents

Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include--

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the specific target of the electronic surveillance;

(3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that--

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is

about to be used, by a foreign power or an agent of a foreign power;

(4) a statement of the proposed minimization procedures;

(5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official--

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories

described in section 1801(e) of this title; and

(E) including a statement of the basis for the certification that--

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

(7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(8) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application; and

(9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.

(10) Redesignated (9)

(11) Repealed. Pub.L. 110-261, Title I, § 104(1)(A), July 10, 2008, 122 Stat. 2460

(b) Additional affidavits or certifications

The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(c) Additional information

The judge may require the applicant to furnish such other information as may be necessary to make the determinations required bysection 1805 of this title.

(d) Personal review by Attorney General

(1)(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) of this section an application under that subsection for a target described in section 1801(b)(2) of this title.

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.

(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

(2)(A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) of this section for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.

(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any,

of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) of this section for purposes of making the application under this section.

(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

(e) Redesignated (d)

50 U.S.C. § 1805. Issuance of order

(a) Necessary findings

Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that--

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that--

> **(A)** the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
>
> **(B)** each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and

(4) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

(5) Redesignated (4)

(b) Determination of probable cause

In determining whether or not probable cause exists for purposes of an order under subsection (a)(2) of this section, a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c) Specifications and directions of orders

(1) Specifications

An order approving an electronic surveillance under this section shall specify--

(A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 1804(a)(3) of this title;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and

(E) the period of time during which the electronic surveillance is approved.

(F) Repealed. Pub.L. 110-261, Title I, § 105(a)(3)(C), July 10, 2008, 122 Stat. 2461

(2) Directions

An order approving an electronic surveillance under this section shall direct--

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier,

landlord, custodian, or other specified person, or in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(3) Special directions for certain orders

An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the

applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of--

(A) the nature and location of each new facility or place at which the electronic surveillance is directed;

(B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;

(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and

(D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.

(d) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated

(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, for the period specified in the application or for one year, whichever is less, and (B) an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this subchapter may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that (A) an extension of an order under this chapter for a surveillance targeted against a foreign power, as defined in paragraph (5), (6), or (7) of section 1801(a) of this title, or against a foreign power as defined in section 1801(a)(4) of this title that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed 1 year.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e)(1) Notwithstanding any other provision of this subchapter, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General--

(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;

(B) reasonably determines that the factual basis for the issuance of an order under this subchapter to approve such electronic surveillance exists;

(C) informs, either personally or through a designee, a judge having jurisdiction under section 1803 of this title at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

(D) makes an application in accordance with this subchapter to a judge having jurisdiction under section 1803 of this title as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.

(2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title.

(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury,

department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(f) Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel

Notwithstanding any other provision of this subchapter, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to--

(1) test the capability of electronic equipment, if--

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and:

(D) *Provided*, That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if--

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the

existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of Title 18, or section 605 of Title 47, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if--

(A) it is not reasonable to--

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this subchapter; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are

destroyed as soon as reasonably possible.

(g) Retention of certifications, applications and orders

Certifications made by the Attorney General pursuant to section 1802(a) of this title and applications made and orders granted under this subchapter shall be retained for a period of at least ten years from the date of the certification or application.

(h) Release from liability

No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this chapter for electronic surveillance or physical search.

(i) In any case in which the Government makes an application to a judge under this subchapter to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 1842(d)(2) of this title.

50 U.S.C. § 1806. Use of information

(a) Compliance with minimization procedures; privileged communications; lawful purposes

Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Notification by United States

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress

Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that--

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress

evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other

United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of--

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Consultation with Federal law enforcement officer

(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1804(a)(7)(B) of this title or the entry of an order under section 1805 of this title.

50 U.S.C. § 1825. Use of information

(a) Compliance with minimization procedures; lawful purposes

Information acquired from a physical search conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No information acquired from a physical search pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Notice of search and identification of property seized, altered, or reproduced

Where a physical search authorized and conducted pursuant to section 1824 of this title involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search conducted pursuant to this chapter and shall identify any property of such person seized, altered, or reproduced during such search.

(c) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(d) Notification by United States

Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from a physical search pursuant to the authority of this subchapter, the United States shall, prior to the trial, hearing, or the other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(e) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof against an aggrieved person any information obtained or derived from a physical search pursuant to the authority of this subchapter, the State or political subdivision thereof

shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(f) Motion to suppress

(1) Any person against whom evidence obtained or derived from a physical search to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such search on the grounds that--

(A) the information was unlawfully acquired; or

(B) the physical search was not made in conformity with an order of authorization or approval.

(2) Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(g) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (d) or (e) of this section, or whenever a motion is made pursuant to subsection (f) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to a physical search authorized by this subchapter or to discover, obtain, or suppress evidence or information obtained or derived from a physical search authorized by this subchapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination

of the legality of the physical search.

(h) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (g) of this section determines that the physical search was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the physical search was lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(i) Finality of orders

Orders granting motions or requests under subsection (h) of this section, decisions under this section that a physical search was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to the physical search shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

(j) Notification of emergency execution of physical search; contents; postponement, suspension, or elimination

(1) If an emergency execution of a physical search is authorized under section 1824(d) of this title and a subsequent order approving the search is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to the search as the judge may determine in his discretion it is in the interests of justice to serve, notice of--

(A) the fact of the application;

(B) the period of the search; and

(C) the fact that during the period information was or was not obtained.

(2) On an ex parte showing of good cause to the judge, the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed 90 days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Consultation with Federal law enforcement officers

(1) Federal officers who conduct physical searches to acquire foreign intelligence information under this subchapter may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1823(a)(6) of this title or the entry of an order under section 1824 of this title.

Federal Rules of Evidence

Rule 401. Definition of "Relevant Evidence."

"Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

Rule 402. Relevant Evidence Generally Admissible; Irrelevant Evidence Inadmissible.

All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible.

Rule 403. Exclusion of Relevant Evidence on Grounds of Prejudice, Confusion, or Waste of Time.

Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.

Rule 404. Character Evidence Not Admissible To Prove Conduct; Exceptions; Other Crimes.

(a) Character evidence generally. – Evidence of a person's character or a trait of character is not admissible

for the purpose of proving action in conformity therewith on a particular occasion, except:

(1) Character of accused. – In a criminal case, evidence of a pertinent trait of character offered by an accused, or by the prosecution to rebut the same, or if evidence of a trait of character of the alleged victim of the crime is offered by an accused and admitted under Rule 404(a)(2), evidence of the same trait of character of the accused offered by the prosecution;

(2) Character of alleged victim. – In a criminal case, and subject to the limitations imposed by Rule 412, evidence of a pertinent trait of character of the alleged victim of the crime offered by an accused, or by the prosecution to rebut the same, or evidence of a character trait of peacefulness of the alleged victim offered by the prosecution in a homicide case to rebut evidence that the alleged victim was the first aggressor;

(3) Character of witness. – Evidence of the character of a witness, as provided in Rules 607, 608, and 609.

(b) Other Crimes, Wrongs, or Acts. – Evidence of other crimes, wrongs, or acts is not admissible to prove the character of a person in order to show action in conformity therewith. It may, however, be admissible for other purposes, such as proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident, provided that upon request by the accused, the prosecution in a criminal case shall provide reasonable notice in advance of trial, or during trial if the

court excuses pretrial notice on good cause shown, of the general nature of any such evidence it intends to introduce at trial.

Rule 801. Definitions

The following apply under this article:

(a) Statement. A "statement" is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion.

(b) Declarant. A "declarant" is a person who makes a statement.

(c) Hearsay. "Hearsay" is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.

(d) Statements which are not hearsay. A statement is not hearsay if –

(2) Admission by party-opponent. The statement is offered against a party and is (A) the party's own statement, in either an individual or representative capacity or (B) a statement of which the party has manifested an adoption or belief in its truth, or (C) a statement by a person authorized by the party to make the statement concerning the subject, or (D) a statement by the party's agent or servant concerning a matter within the scope of the agency

or employment, made during the existence of the relationship, or (E) a statement by a coconspirator of a party during the course and in furtherance of the conspiracy. The contents of the statement shall be considered but are not alone sufficient to establish the declarant's authority under subdivision (C), the agency or employment relationship and the scope thereof under subdivision (D), or the existence of the conspiracy and the participation therein of the declarant and the party against whom the statement is offered under subdivision (E).

ANTI-VIRUS CERTIFICATION

Case Name: U.S. v. Abu-Jihaad

Docket Number: 09-1375-cr

I, Louis Bracco, hereby certify that the Appellee's Brief submitted in PDF form as an e-mail attachment to **criminalcases@ca2.uscourts.gov** in the above referenced case, was scanned using CA Software Anti-Virus Release 8.3.02 (with updated virus definition file as of 2/9/2010) and found to be VIRUS FREE.

Louis Bracco
Record Press, Inc.

Dated: February 9, 2010

CERTIFICATE OF SERVICE

09-1375-cr USA v. Abu-Jihaad

I hereby certify that two copies of this Brief for the United States of America were sent by Regular First Class Mail to:

Dan E. LaBelle, Esq.
Halloran & Sage LLP
315 Post Road West
Westport, CT 06880

Attorneys for Defendant-Appellant-
Cross-Appellee

I also certify that the original and five copies were also shipped via Hand delivery to:

Clerk of Court
United States Court of Appeals, Second Circuit
United States Courthouse
500 Pearl Street, 3rd floor
New York, New York 10007
(212) 857-8576

on this 9th day of February 2010.

Notary Public:

_____

Sworn to me this

February 9, 2010

RAMIRO A. HONEYWELL
Notary Public, State of New York
No. 01HO6118731
Qualified in Kings County
Commission Expires November 15, 2012

_____

SAMANTHA COLLINS
Record Press, Inc.
229 West 36th Street, 8th Floor
New York, New York 10018
(212) 619-4949