MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY

UNITED STATES OF AMERICA v. KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN 'ATTASH, RAMZI BIN AL SHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI	AE284(WBA) **Defense Motion** to Compel the Production of Information Related to the Monitoring and/or Collection of Attorney-Client Privileged Information 26 March 2014

1. Timeliness:

This filing is timely pursuant to Military Commissions Trial Judiciary Rule of Court 3.7(b) and Rule for Military Commissions (RMC) 905.

2. Relief Sought:

Pursuant to R.M.C. 701 and 10 U.S.C. § 949j, the Commission should order the United States Government to produce the following documents, records, recorded communications, papers, photographs, and/or tangible objects concerning Intelligence Community (IC) monitoring of defense communications:

a. All information pertaining to the IC's monitoring or collection of information regarding Defense team telephone numbers (metadata or actual content), including, but not limited to, the following numbers:

[redacted]

Filed with TJ
26 March 2014

b. **All information pertaining to the IC's monitoring or collection of information regarding Defense team email accounts (metadata or actual content), including, but not limited to, the following email addresses: cheryl.bormann [redacted] ctb@cherylbormannlawoffices.com, james.hatcher [redacted] tjs@ocslawgroup.com, [redacted] Anthony.everett [redacted] terry.obrien [redacted] sean.safdi [redacted] Michael.schwartz [redacted] tim.semmerling [redacted] todd.swensen [redacted].**

c. **All information pertaining to investigations and/or reports in the possession of the IC where Defense team members are mentioned by name, phone number, email address, or any other means of identification. This includes both investigations or reports where a Defense team member was the focus of the investigation or report, and investigations or reports where a Defense team member was not the focus of the investigation, but is mentioned in connection with another individual, to include any investigations or reports of foreign nationals.**

d. **All information pertaining to investigations and/or reports in the possession of the IC where a Defense team member's information, to include name, phone number, email address, Skype address, or any other means of identification, is collected under 50 U.S.C. 1861 (also known as "Section 215"). This information includes investigations or reports where Defense team data is collected and stored as metadata.**

e. **All information pertaining to documents drafted by or for the Foreign Intelligence Surveillance Court (FISC), FISC orders, and FISC decisions where a Defense team member's information, to include name, phone number, email address, Skype address, or any other means of identification, is discussed as being collected, queried, reviewed, or received by the IC under 50 U.S.C. 1861.**

f. **All information pertaining to the IC's policies and procedures for monitoring, gathering, collecting, recording, storing, and querying information derived from communications between or among attorneys, members of legal teams, witnesses, and clients, including, but not limited to, anything that can reasonably be referred to as attorney work product.**

g. All communications between or among members of OCP and the IC pertaining to any of the areas mentioned in this discovery request in paragraphs 2(a)-(g).

h. All information pertaining to NSA's storage and usage of archived encryption keys associated with any member of the Defense team. This request includes NSA's standard operating procedure for storing, decrypting, and/or reviewing emails containing privileged information. It also includes any information NSA reviewed or derived from Defense team encryption keys.[1]

i. All information pertaining to the IC's involvement, whether past or present, in the construction, design, monitoring and/or operation of the following at Guantanamo Naval Base, Guantanamo, Cuba:

(1) The Expeditionary Legal Center (ELC) including, but not limited to, courtrooms, client meeting rooms, attorney offices, buildings AV 29 and/or AV-34, and the telephonic and network communication lines.

(2) All living spaces provided for Defense teams including, but not limited to, the tents, Cuzco Trailers, Bachelor Officers' Quarters, and townhomes in East Caravella.

(3) Camp 7.

(4) Echo II, including, but not limited to, all meeting rooms, the surveillance room, all audio and video transmittal and recording equipment regardless of whether the equipment is currently connected, and the repairs and/or upgrades to any equipment before or after hurricane damage in October 2012.

(5) All government owned vehicles provided to the Defense team while staying at Guantanamo Bay.

3. Overview:

Defense counsel represent a capital defendant who, from 2003 until 2006, was a victim of torture under the Central Intelligence Agency's Rendition, Detention, and

[1] This request is based on the testimony of Mr. Brent Glover who stated, when asked about the encryption keys of Defense team members, "the encryption key is archived…under the NSA control program. It is in a store…the store is controlled by NSA and the DoD." (Trial Tr. 5802:17-5803:12.)

Interrogation Program. Over the course of pre-trial litigation in this case, it has become apparent that the United States has chosen to prosecute Mr. bin 'Attash under the Military Commissions Act, as opposed to a legitimate and regularly-constituted system of justice, in an effort to keep secret the horrific, unlawful treatment Mr. bin 'Attash received at the hands of the CIA.

Despite efforts to obtain discoverable information material to the preparation of a defense, properly-cleared defense counsel have been denied access to any evidence related to the CIA's torture of Mr. bin 'Attash between 2003 and 2006. Despite counsel's efforts to investigate the CIA's RDI Program, limitations on resources and travel have ensured that details of Mr. bin 'Attash's torture remain hidden from defense counsel.

Recent media reports demonstrate the CIA's efforts to prevent the release of information that would reveal its criminal conduct. Defense counsel question whether those efforts include secret surveillance of counsel carrying out their DoD-appointed duties of defending Mr. bin 'Attash's life at a capital trial. Apart from being illegal, such surveillance violates the attorney-client privilege and denies Mr. bin 'Attash constitutional and statutory rights.

On 6 November 2013, Mr. bin 'Attash requested the U.S. Government provide the aforementioned discovery concerning the monitoring of telephone conversations and email accounts of members of Mr. bin 'Attash's defense team. Attachment B. On 26 November 2013, the Prosecution responded to Mr. bin 'Attash's 6 November discovery request and declined to provide the requested items. Attachment C. The Prosecution responded that "[w]hatever the contours of any electronic surveillance that the United States may or may not be conducting, *no member of the prosecution team at the Office of*

the Chief Prosecutor has come upon, reviewed, seen, heard, or in any way learned of any communications (metadata or content) of any of Mr. Mohammad's [sic] *defense counsel*." (emphasis added). *Id.* at ¶ 4. Additionally, the Prosecution added that "none of the prosecutors or law enforcement agents assigned to this matter have come across, reviewed, seen, or otherwise learned of any such communications (metadata or content). *Id.*

Whether or not the Prosecution is aware of or has been provided the results of IC monitoring activities, the Prosecution's response fails to account for Trial Counsel's duty to investigate the existence of and locate such documentation within the records of other Government agencies. Tellingly, at no point does the Prosecution's discovery response indicate that such records do not exist, and the Prosecution also does not dispute the materiality of such records. Instead, the Prosecution simply relies upon conclusory statements that it has not itself engaged in inappropriate monitoring of the attorney-client relationship. However, IC monitoring of and interference with the attorney-client relationship has a chilling impact that exists independent of the knowledge or complicity of the Prosecution.

Numerous reports from American and European news organizations detail the IC's use of surveillance and the IC's ability and willingness to monitor the communications of U.S. citizens.[2] These reports have caused the U.S. Government to confirm, through white papers, declassified FISC opinions, and declassified documents,

---

[2] *See* Robert O'Harrow Jr., Ellen Nakashima, and Barton Gellman, *U.S., Company Officials: Internet Surveillance Does Not Indiscriminately Mine Data*, Washington Post, June 8, 2013; Siobhan Gorman and Jennifer Valentino-Devries, *Government is Tracking Verizon Customers' Records*, Wall Street J., June 6, 2013; Kathleen Hennessey, *Obama Administration Defends Collecting Verizon Phone Data*, L.A. Times, June 6, 2013; Nicole Perlroth, Jeff Larson, and Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. Times, Sep. 5, 2013.

the existence of invasive surveillance programs within the IC.[3] Given the nature of this case, and the fact that the Defense utilizes communication through several of the companies referenced in both news articles and declassified documents, the Defense has a good faith basis to believe that its communications have been the subject of monitoring by the IC – potentially piercing sacrosanct privileges and exposing crucial attorney-client communications and attorney work product to Government review.

4. Burden of Proof:

The defense bears the burden of proof as to the facts as the moving party on this motion. The standard of proof is a preponderance of the evidence. R.M.C. 905(c).

5. Facts:

a. On 28 January 2013, during an unclassified session of the Commission, the audio and video feeds were cut by a then-unknown entity when counsel for Mr. Mohammad stated on the record the unclassified title of the unclassified pleading AE080, Joint Defense Motion to Preserve Evidence of Any Existing Detention Facility. Tr. at 1445. After the Prosecution provided conflicting information as to the source of the disruption, the Commission was finally able to ascertain that the disruption was caused by the clandestine monitoring and interference of an Original Classification Authority (OCA). Tr. at 1485. The 28 January 2013 stoppage was the third such incident, none of which involved the actual disclosure of classified information. *See* AE133 (WBA Sup).

[3] *See* Administration White Paper: *Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act*, Aug. 9, 2013; Letter from Peter J. Kadzik, Principal Deputy Assistant Att'y Gen., Dep't of Justice, to Rep. F. James Sensenbrenner Jr. (July 16, 2013); Letter from Ronald Weich to Sens. Dianne Feinstein and Saxby Chambliss, Feb. 2, 2011; Office of the Dir. of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosures of Classified Information* (June 6, 2013); Mark Landler and David Sanger, *Obama May Ban Spying on Heads of Allied States*, N.Y. Times, Oct. 29, 2013.

b. On 31 January 2013, Mr. bin 'Attash and his co-accused filed a joint motion to remove the sustained barrier to attorney-client communication and to prohibit the U.S. Government from monitoring and recording attorney-client communication in any location at Guantanamo Bay, Cuba. AE133.

c. During the February 2013 hearings, counsel for Mr. bin 'Attash informed the Commission that listening devices disguised as smoke detectors were discovered in the huts at "Echo II" where attorneys meet with the accused. *See* AE133V (KSM).

d. In March 2013, the Prosecution was provided with at least one internal, privileged defense email pertaining to *Ibrahim Ahmed Mahmoud al Qosi v. United States*. *See* AE154. The defense has repeatedly emphasized breaches of security and confidentiality that ultimately led the Chief Defense Counsel to order that "counsel not…use the electronic systems that are the backbone of the Office infrastructure for privileged and case-confidential material." *See* AE155M, AE155J Attachment A.

e. One principle purpose of holding detainees at Guantanamo Bay is intelligence-gathering. Former JTF-GTMO Commander BG Jay W. Hood noted in an article authored for the 31 December 2004 issue of GTMO's base newspaper, *The Wire*, "[S]ince the creation of JTF-GTMO, we have achieved many noteworthy accomplishments, including. . .[c]onstruction of state-of-the-art detention and *intelligence-gathering* facilities" (emphasis added).

f. Recent open-source media accounts demonstrate the expansive nature of previously undisclosed clandestine intelligence gathering and bulk data collection efforts operated by the IC, particularly the National Security Administration. *See* Attachment B.

g. On 6 November 2013, Mr. bin 'Attash submitted a discovery request to the U.S. Government requesting the production of "[a]ll information pertaining to the IC's monitoring or collection of information regarding Defense team telephone numbers . . . and email accounts." Attachment B.

h. On 26 November 2013, the Prosecution responded by not disavowing the existence of, but by refusing to produce the requested discovery.

6. Law and Argument:

This Commission should compel the Government to produce the requested discovery. The requested discovery is material to the preparation of the Defense. Counsel for Mr. bin 'Attash have a duty to protect attorney-client privileged information. *See, e.g.* ABA Model Rule 1.6(c). Communications to and from members of the Defense team must remain privileged and confidential. Any monitoring of these communications by the U.S. Government constitutes a violation of domestic law and presents a grave ethical dilemma for counsel. Accordingly, the Defense requests all information pertaining to the IC's monitoring or collection of information regarding Defense team telephone numbers and email accounts in order to provide Mr. bin 'Attash with full and effective assistance of counsel. The Defense believes that such information exists based on an analysis of 50 U.S.C. § 1861 and recent disclosures by the U.S. Government on this topic.

a. Applicable Standard for Discovery

In any criminal trial, the defendant has a fundamental due process right to present a complete defense. *See e.g. United States v. Webb,* 66 M.J. 89, 92 (C.A.A.F. 2008) ("[t]he due process clause of the Fifth Amendment guarantees that criminal defendants be

afforded a meaningful opportunity to present a complete defense"), *citing California v. Trombetta,* 467 U.S. 479, 485 (1984). Inseparable from the right to present a complete defense is the right to obtain evidence to present such defense. In the Military Commissions Act of 2009, Congress specifically and consciously recognized the importance of discovery and production when it directed that "[t]he opportunity to obtain witnesses and evidence shall be comparable to the opportunity available to a criminal defendant in a court of the United States under article III of the Constitution." 10 U.S.C. § 949j.

Although often confused, pretrial discovery is distinct from the production of witnesses and evidence for use at trial. When it comes to the examination of documents in discovery, rather than the production of documents for use at trial, both article III and military courts have consistently applied a "materiality" rather than relevance or admissibility standard. *See* R.M.C. 701(c)(1); R.C.M. 701(a)(2)(A); Fed. R. Crim. P. 16(a)(1)(E) (universally permitting the examination of documents "material" to the preparation of the defense); *Lockett v. Ohio,* 438 U.S. 586, 604 (1978) (capital defendant entitled to obtain evidence that is "*material* either to guilt or to punishment") (emphasis added); *United States v. Yunis*, 867 F.2d 617, 625 (D.C. Cir. 1989) ("material to the preparation of the defense" includes information that is "helpful to the defense of an accused."). The standard is broad, liberal, and "is not focused solely upon evidence known to be admissible at trial." *See, e.g. United States v. Roberts,* 59 M.J. 323, 325 (C.A.A.F. 2004).

Discovery of "material" information generally applies to information within the possession, custody, or control of the Government. While the Prosecution's response

seems to suggest that the Prosecution does not have a duty to search for and locate the requested information because "none of the prosecutors or law enforcement agents assigned to this matter have come across, reviewed, seen, or otherwise learned of any such communications (metadata or content)," the Prosecution's duty with respect to this discovery request goes far beyond a passive analysis of its own records. It is well established that "[d]iscovery is not limited to matters within the scope of trial counsel's personal knowledge." *United States v. Jackson,* 59 M.J. 330, 334 (C.A.A.F. 2004). Instead, particularly with respect to potentially exculpatory or impeaching evidence, the prosecutor "has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police." *Kyles v. Whitley,* 514 U.S. 419, 437 (1995). Accordingly, "[t]rial counsel must exercise due diligence in discovering…reports not only in his possession but also in the possession, control, or custody of other 'military authorities.'" *United States v. Simmons,* 38 M.J. 376 (C.M.A. 1993). "To the extent that relevant files are known to be under the control of another governmental entity, the prosecution must make that fact known to the defense and engage in 'good faith efforts' to obtain the material." *United States v. Williams,* 50 M.J. 436, 441 (C.A.A.F. 1999). While the Prosecution's duty to search the investigative files of other governmental entities may be limited to entities aligned with the prosecution (of which the IC would be included in the instant case), this duty is expanded and constructive knowledge of the existence of such documents can be imputed where "the defense has made a specific request for the information." *United States v. Veksler,* 62 F.3d 544, 550 (3d Cir. 1995).

Mr. bin 'Attash requested the information in the instant request from the *U.S. Government*, not from the Prosecution. The Prosecution clearly missed this detail in the requested by responding that no member of the prosecution in this matter saw or reviewed any communications of Mr. Mohammad's [sic] defense team. Demonstrating the lack of attention that the Prosecution chose to give to this discovery request, the response even fails to note that the request originated with Mr. bin 'Attash, instead referencing Mr. bin 'Attash's co-accused Mr. Mohammad.

b. Materiality of Requested Information

The information requested by Mr. bin 'Attash is material to the presentation of his case in that Mr. bin 'Attash's defense team has a duty to protect attorney-client privileged information associated with his case. Mr. bin 'Attash has a statutory and constitutional right to counsel before this capital Military Commission. *See, e.g.* 10 U.S.C. § 948k, 10 U.S.C. § 949c, *Strickland v. Washington,* 466 U.S. 668 (1984). The right to counsel is the right to the effective assistance of counsel. *See e.g. McMann v. Richardson,* 397 U.S. 759 (1970); *Reece v. Georgia,* 350 U.S. 85 (1955); *Glasser v.United States,* 315 U.S. 60 (1942). The right to effective assistance of counsel includes "the right of private consultation with [counsel]." *Coplon v. United States,* 191 F.2d 749, 757 (D.C. Cir. 1951). The surreptitious interception and monitoring of private attorney-client communications interferes with the right to effective assistance of counsel. *See, e.g. Weatherford v. Bursey,* 429 U.S. 545, 554 n.4 ("[o]ne threat to the effective assistance of counsel posed by government interception of attorney-client communications lies in the inhibition of free exchanges between defendant and counsel because of the fear of being overhead."); *Caldwell v. United States,* 205 F.2d 879, 881 (D.C. Cir. 1953) ("interception

of supposedly private telephone consultations between accused and counsel, before and during trial, denies the accused his constitutional right to effective assistance of counsel, under the Fifth and Sixth Amendments.") (citing *Coplon,* 191 F.2d 749).

The attorney-client privilege is truly the backbone of the legal profession. It encourages the client to be open and honest with his or her attorneys without fear that others will be able to pry into those conversations, and possibly use those conversations to gain a distinct advantage in the case. Without the privilege, clients would be unwilling to share critical information with their attorneys as this information could be used against them. If a client knows that his conversations, or the conversations between his defense team, are being monitored, the client will be less likely to share valuable information to his attorneys thereby inhibiting their ability to provide effective assistance. Counsel for Mr. bin 'Attash have an ethical duty to ensure that attorney-client communications remain private and privileged. *See e.g.* ABA Model Rule 1.6(a) ("A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent…"); R.M.C. 502(d)(7), Discussion (addressing the duties of defense counsel and noting that "[d]efense counsel must guard the interests of the accused zealously within the bounds of the law . . . represent the accused with undivided fidelity and *may not disclose the accused's secrets or confidences except as the accused may authorize*…" (emphasis added)). Far from simply forbidding the knowing communication of client confidences, the ABA Model Rules and Rules for Military Commissions place an ethical obligation on counsel to *proactively* prevent breaches by taking reasonable measures to prevent intentional or unintentional revelations, including unauthorized access. *See* ABA Model Rule 1.6(c) ("[a] lawyer shall make reasonable

efforts to prevent the inadvertent or unauthorized disclosure of, *or unauthorized access to*, information relating to the representation of a client.") (emphasis added). The Rules indicate that counsel has an obligation not only to respond to past breaches or secure known threats, as the Government seems to contemplate in its various suggestions that no past breaches have occurred, but also to act proactively to prevent even the inadvertent disclosure of confidential information.

Counsel's ethical duty to prevent unauthorized access to client confidences extends to email and other electronic communications. Comment 19 to ABA Model Rule 1.6 states that "[w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require the lawyer to use special security measures if the method of communication affords a reasonable expectation of privacy." Similarly, the Army Rules of Professional Conduct for Lawyers states that "[c]ontrol or access by others to automated data processing systems or equipment utilized by the lawyer also must be considered. Control or access by personnel who are not subject to the Rules, or supervised by those subject to these Rules, may lead to a violation of the confidentiality required by this Rule." Army Regulation 27-26 at 8.

Here, the assurance that Mr. bin 'Attash's communications with his attorneys are privileged is crucial to the legitimacy of this Commission. The U.S. Government wants to kill Mr. bin 'Attash. Mr. bin 'Attash must rely completely on the U.S. Government for a fair trial. From his three year detention with the CIA, to being held for eleven years without trial, to having his privileged communication with his lawyers monitored or

confiscated as "contraband", Mr. bin 'Attash's experience with this system has shown a complete disregard for the attorney-client relationship. If anything in this process must be respected, it is the attorney-client privilege, the oldest of the privileges for confidential communications known to the common law. 8 J. Wigmore, Evidence §2290 (McNaughton rev. 1961).

In this case, in addition to providing information to inform arguments concerning potential violations of the attorney-client privilege, the requested information may also inform existing arguments before the Commission concerning "unlawful influence." In AE031, Mr. bin 'Attash and his co-accused moved to dismiss the charges in the instant case due to unlawful influence. As Mr. bin 'Attash noted in AE031, the Military Commissions Act of 2009 *broadens* the traditional military definition of unlawful influence, extending the scope of the prohibition to "any person" – not only those persons subject to the UMCJ – and prohibiting attempts to coerce or influence the "exercise of professional judgment by trial counsel or defense counsel" – not only the action of the Commission itself. *See* 10 U.S.C. § 949b(a)(2)(C). Unlawful influence has long been referred to as the "mortal enemy of military justice." *United States v. Thomas,* 22 M.J. 388, 393 (C.M.A. 1986). In addition to actual unlawful influence, the mere "appearance of unlawful command influence is as devastating to the military justice system as the actual manipulation of any given trial." *United States v. Allen,* 33 M.J. 209, 212 (C.M.A. 1991). The appearance of unlawful influence, also known as implied unlawful influence, is "judged objectively, through the eyes of the community." *United States v. Stoneman,* 57 M.J. 35, 42 (C.A.A.F. 2002).

Here, action by the NSA and other Government agencies to surreptitiously monitor the communications of defense counsel may be indicative of either actual or implied unlawful influence. The chilling effect of such actions on the attorney-client relationship, if substantiated, would doubtlessly influence the professional judgment of defense counsel in the manner that he or she interacts with the client. Even if the effort was not specifically aimed at altering the outcome of the instant case, efforts of the U.S. Government to intercept and monitor attorney-client communications would at a minimum give the appearance of unlawful influence, as judged objectively through the eyes of the community.

In the face of the clear materiality of the requested discovery, the Prosecution declines to provide "any additional discovery beyond what was provided in connection with AE133 and AE155," claiming that all "defense claims of monitoring have been previously litigated in AE133 and AE155." The Prosecution's argument is off-point; the discovery request related to AE133 was specific to the monitoring of attorney-client privileged communication in Courtroom II, at the Echo II attorney-client meeting huts, and the ELC holding cells, and the discovery requested in AE155 was specific to the U.S. Government's access to OCDC's network drive and government email accounts. Here, the Defense request was broader and specifically requested information from the intelligence community with regard to defense team official *and* personal phone numbers and official *and* personal emails. While those arguments put forth in AE133 and AE155 should inform the Commission's determination as to the present request by demonstrating the pervasiveness of Government-sanctioned monitoring, this request is distinct from those matters covered in AE133 and AE155.

Recent reports from American and European news organizations detailing the IC's use of surveillance to monitor the communications of U.S. citizens are particularly troubling in the context of the present case. Given the nature of this case, the fact that elements of the U.S. Government view Mr. bin 'Attash and his co-accused as intelligence assets (whether or not this view is shared by the Prosecution), and the fact that the Defense utilizes communication through several of the companies referenced in both news articles and declassified documents, the Defense has a good-faith basis that Defense communications have been and continue to be the subject of IC monitoring. For the foregoing reasons, Mr. bin 'Attash requests that the Commission compel the production of the discovery requested in Attachment B.

7. Oral Argument:

The defense requests oral argument.

8. Witnesses:

A. None at this time. Mr. bin 'Attash reserves the right to add to this witness list.

9. Certificate of Conference:

The Prosecution opposes this motion.

10. Attachments:

A. Certificate of Service

B. Defense Request for Discovery dtd 6 November 2013

C. Prosecution Response to 6 November 2103 Request for Discovery

//s//
CHERYL T. BORMANN
Learned Counsel

//s//
JAMES E. HATCHER, LCDR, JAGC, USNR
Defense Counsel

//s//
MICHAEL A. SCHWARTZ, Capt, USAF
Defense Counsel

//s//
TODD M. SWENSEN, Capt, USAF
Defense Counsel

CERTIFICATE OF SERVICE

I certify that on 26 March 2014, I electronically filed the foregoing Defense Motion to Compel the Production of Information Related to the Monitoring and/or Collection of Attorney-Client Privileged Information with the Trial Judiciary by e-mail.

//s//
CHERYL T. BORMANN
Learned Counsel

DEPARTMENT OF DEFENSE
OFFICE OF THE CHIEF DEFENSE COUNSEL
1620 DEFENSE PENTAGON
WASHINGTON, DC 20301-1620

6 November 2013

MEMORANDUM FOR TRIAL COUNSEL, *UNITED STATES v. MOHAMMAD, et al.*

FROM: Cheryl Bormann, Learned Counsel for Walid bin 'Attash

SUBJECT: Request for Discovery dtd 5 November 2013

Pursuant to RMC 701 and 10 U.S.C. § 949j, Mr. bin 'Attash requests that the Government provide the following information in discovery. Failure to provide the requested information will deny Mr. bin 'Attash of his rights to the due process of law, to the effective assistance of counsel, a fair, speedy, and public trial, and to be free from cruel and unusual punishment, guaranteed by the Fifth, Sixth, and Eight Amendments to the United States Constitution and/or other provisions of U.S. and international law.

1. For purposes of this discovery request, references to the Intelligence Community (IC) include all U.S. government agencies engaged in the practice of conducting intelligence activities as described in Executive Order 12333, including, but not limited to, the CIA, NSA, FBI, DIA, the National Reconnaissance Office, and the offices within DOD specializing in the collecting of intelligence. Also for purposes of this discovery request, references to Mr. bin 'Attash's defense team include all individuals assisting in the defense of Walid bin 'Attash, including, but not limited to, Cheryl Bormann, Michael Schwartz, Ali al Arashi, [redacted] James Hatcher, [redacted] Todd Swensen, Tim Jon Semmerling, [redacted] Tim Orr, Terry O'Brien, [redacted] and Sean Safdi.

2. Please produce the following documents, records, recorded communications, papers, photographs and/or tangible objects. If any of the requested documents, records, or communications will be withheld, please identify the parties involved and the reasons for withholding.

a. All information pertaining to the IC's monitoring or collection of information regarding Defense team telephone numbers (metadata or actual content), including, but not limited to, the following numbers: [redacted]

b. All information pertaining to the IC's monitoring or collection of information regarding Defense team email accounts (metadata or actual content), including, but not limited to, the following email addresses: cheryl.bormann[redacted], [redacted]

DR-132-WBA

[redacted] ctb@cherylbormannlawoffices.com, james hatcher [redacted]
tjs@ocslawgroup.com, Anthony.t.everett
[redacted]
Anthony.everett
Kenneth.henkel terry.obrien
sean.safdi Michael.schwartz tim.semmerling
todd.swensen
[redacted]

c. All information pertaining to investigations and/or reports in the possession of the IC where Defense team members are mentioned by name, phone number, email address, or any other means of identification. This includes both investigations or reports where a Defense team member was the focus of the investigation or report, and investigations or reports where a Defense team member was not the focus of the investigation, but is mentioned in connection with another individual, to include any investigations or reports of foreign nationals.

d. All information pertaining to investigations and/or reports in the possession of the IC where a Defense team member's information, to include name, phone number, email address, Skype address, or any other means of identification, is collected under 50 U.S.C. 1861 (also known as "Section 215"). This information includes investigations or reports where Defense team data is collected and stored as metadata.

e. All information pertaining to documents drafted by or for the Foreign Intelligence Surveillance Court (FISC), FISC orders, and FISC decisions where a Defense team member's information, to include name, phone number, email address, Skype address, or any other means of identification, is discussed as being collected, queried, reviewed, or received by the IC under 50 U.S.C. 1861.

f. All information pertaining to the IC's policies and procedures for monitoring, gathering, collecting, recording, storing, and querying information derived from communications between or among attorneys, members of legal teams, witnesses, and clients, including, but not limited to, anything that can reasonably be referred to as attorney work product.

g. All communications between or among members of OCP and the IC pertaining to any of the areas mentioned in this discovery request in paragraphs 2(a)-(g).

h. All information pertaining to NSA's storage and usage of archived encryption keys associated with any member of the Defense team. This request includes NSA's standard operating procedure for storing, decrypting, and/or reviewing emails containing privileged information. It also includes any information NSA reviewed or derived from Defense team

encryption keys.[1]

i. All information pertaining to the IC's involvement, whether past or present, in the construction, design, monitoring and/or operation of the following at Guantanamo Naval Base, Guantanamo, Cuba:

(1) The Expeditionary Legal Center (ELC) including, but not limited to, courtrooms, client meeting rooms, attorney offices, buildings AV 29 and/or AV-34, and the telephonic and network communication lines.

(2) All living spaces provided for Defense teams including, but not limited to, the tents, Cuzco Trailers, Bachelor Officers' Quarters, and townhomes in East Caravella.

(3) Camp 7.

(4) Echo II, including, but not limited to, all meeting rooms, the surveillance room, all audio and video transmittal and recording equipment regardless of whether the equipment is currently connected, and the repairs and/or upgrades to any equipment before or after hurricane damage in October 2012.

(5) All government owned vehicles provided to the Defense team while staying at Guantanamo Bay

3. The aforementioned documents are material to the preparation of the defense, and/or are relevant and necessary to bin 'Attash's defense. Communications to and/or from members of the Defense team must remain privileged and confidential. Any monitoring of these communications by the U.S. Government constitutes a violation of both international and U.S. law. Accordingly, the Defense requests these documents in order to provide Mr. bin 'Attash with full and effective assistance of counsel. The Defense is entitled to these documents, and believes that such documents exist, based on an analysis
of 50 U.S.C. 1861 and recent disclosures by the U.S. Government on this topic.

a. Under 50 U.S.C. 1861, the Government applies to the FISC for "an order requiring the production of any tangible things…for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[2] The Government must provide the FISC with "a statement of facts showing that there are reasonable grounds to believe that the tangible things

[1] This request is based on the testimony of Mr. Brent Glover who stated, when asked about the encryption keys of Defense team members, "the encryption key is archived…under the NSA control program. It is in a store…the store is controlled by NSA and the DoD." (Trial Tr. 5802:17-5803:12.)

[2] 50 U.S.C. 1861(a)(1).

sought are relevant to an authorized investigation."[3] The Government interprets the statute broadly, believing it can collect seemingly limitless amounts of data and information without meeting the relevancy standard in 50 U.S.C. 1861(b)(2) because the relevancy standard applies only when "the data [is] queried for intelligence purposes" and that query only occurs when "there is reasonable suspicion, based on specific facts, that a particular query term…is associated with a specific foreign terrorist organization."[4] Thus, by the Government's own admission, it is routinely monitoring and collecting information, and it is viewing that information if it is connected to a known terrorist organization. In this case, the Defense team is representing an alleged member of Al-Qaeda and an alleged terrorist. Additionally, agents of the U.S. Government accessed privileged email communications and privileged work product from the Defense team's official government computer system, all of which served as the basis for the AE155 series motions. It is reasonable to believe that communications among the Defense team and communications to and from the Defense team have been monitored, collected, and viewed by the Government.

b. Recent reports from American and European news organizations have detailed the IC's use of surveillance and their ability and willingness to monitor the communications of U.S. citizens.[5] These reports have caused the U.S. Government to confirm, through white papers, declassified FISC opinions, and declassified documents, the existence of invasive surveillance programs within the IC.[6] Given the nature of this case and the fact that the Defense utilizes communication through several of the companies referenced in both news articles and declassified documents, it is highly likely that Defense communications were the subject of monitoring.

4. The aforementioned documents are material to the preparation of the defense, and are requested on the grounds that Mr. bin 'Attash cannot prepare potential motions, conduct an appropriate investigation, and properly prepare for trial, including any sentencing proceeding, without production of the documents requested. The disclosure of the items requested is paramount to ensure a "full and fair trial" as mandated by the Military Commissions Act of 2009 and to afford

---

[3] 50 U.S.C. 1861(b)(2).

[4] *See* Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney General to Rep. James Sensenbrenner (July 16, 2013).

[5] *See* Robert O'Harrow Jr., Ellen Nakashima, and Barton Gellman, *U.S., Company Officials: Internet Surveillance Does Not Indiscriminately Mine Data*, Washington Post, June 8, 2013; Siobhan Gorman and Jennifer Valentino-Devries, *Government is Tracking Verizon Customers' Records*, Wall Street J., June 6, 2013; Kathleen Hennessey, *Obama Administration Defends Collecting Verizon Phone Data*, L.A. Times, June 6, 2013; Nicole Perlroth, Jeff Larson, and Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. Times, Sep. 5, 2013.

[6] *See* Administration White Paper: *Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act*, Aug. 9, 2013; Letter from Peter J. Kadzik, Principal Deputy Assistant Att'y Gen., Dep't of Justice, to Rep. F. James Sensenbrenner Jr. (July 16, 2013); Letter from Ronald Weich to Sens. Dianne Feinstein and Saxby Chambliss, Feb. 2, 2011; Office of the Dir. of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosures of Classified Information* (June 6, 2013); Mark Landler and David Sanger, *Obama May Ban Spying on Heads of Allied States*, N.Y. Times, Oct. 29, 2013.

Mr. bin 'Attash all the judicial guarantees which are recognized as indispensable by civilized people, as mandated in the Manual for Military Commissions and well established principles under the United States Constitution, death penalty jurisprudence, and international law. The ability of an attorney to fully represent his or her client depends on the "full and frank communication between [them]."[7] The firmly established attorney-client privilege is "founded upon the necessity…of the aid of persons having knowledge of the law and skilled in its practice, which assistance can only be safely and readily availed of **when free from the consequences or the apprehension of disclosure**."[8]

5. Point of contact for this discovery request is the undersigned at cheryl.bormann@osd.mil.

Respectfully submitted,

//s//
CHERYL T. BORMANN
Learned Counsel for Walid bin 'Attash

[7] *Upjohn Co. v. U.S.*, 449 U.S. 383, 389 (1981).
[8] *Hunt v. Blackburn*, 128 U.S. 464, 470 (1888) (emphasis added).

DEPARTMENT OF DEFENSE
OFFICE OF THE CHIEF PROSECUTOR OF MILITARY COMMISSIONS
1610 DEFENSE PENTAGON
WASHINGTON, DC 20301-1610

OFFICE OF THE
CHIEF PROSECUTOR

November 26, 2013

MEMORANDUM FOR Defense Counsel for Mr. Bin 'Attash

SUBJECT: Prosecution Response to 6 November 2013 Request for Discovery

1. The Prosecution received the Defense request for discovery on 6 November 2013. The Prosecution hereby responds to the Defense request.

2. The Defense in its memorandum on 6 November 2013 requests documents, records, recorded communications, papers, photographs and/or tangible objects pertaining to what counsel characterizes as the IC's monitoring or collection of information regarding Defense team telephone numbers, email accounts, Skype handles/addresses, or any other means of identification. *See para. 1(a)-(h).*

3. The Defense request assumes that privileged and confidential communications to and/or from members of the Defense team have been unlawfully monitored by the United States government thereby depriving Mr. Bin'Attash with full and effective assistance of counsel. The Defense request indicates that it is highly likely that Defense communications were the subject of monitoring based upon recent reports from American and European news organizations that have detailed the IC's use of surveillance and their ability and willingness to monitor the communications of U.S. citizens.

4. The Prosecution respectfully declines to provide the items in the request as the premise for the Defense request is simply inaccurate. Whatever the contours of any electronic surveillance that the United States may or may not be conducting, no member of the prosecution team at the Office of the Chief Prosecutor has come upon, reviewed, seen, heard, or in any way learned of any communications (metadata or content) of any of Mr. Mohammad's defense counsel. Further, none of the prosecutors or law enforcement agents assigned to this matter have come across, reviewed, seen, or otherwise learned of any such communications (metadata or content).

5. The Defense also requests all information pertaining to NSA's storage and usage of archived encryption keys associated with any member of the Defense team. This request includes NSA's standard operating procedure for storing, decrypting, and/or reviewing emails containing privileged information. It also includes any information NSA reviewed or derived from Defense team encryption keys. *See para. 1(i).*

6. The Prosecution respectfully declines to provide additional information other than that previously provided through the testimony of Brent Glover. In an effort to educate the Defense on the availability of encryption as a method of safeguarding confidential communications, the United States government elicited from Mr. Glover that the PKI (public key infrastructure) program was jointly administered by DISA and NSA and that the private encryption keys were archived by NSA. Mr. Glover also explained that there were safeguards in place to ensure that a private encryption key could not be accessed unless specific provisions were met. There is not a shred of evidence to support any contention that the private encryption key in any Defense team member's Common Access Card (CAC) has been tampered with or otherwise compromised. Indeed, the Military Judge in his order in AE155 specifically rejected the Defense contention that their communications had been intercepted or monitored in any way.

7. Finally, the Defense requests all information pertaining to the IC's involvement, whether past or present, in the construction, design, monitoring and/or operation of the detention facilities, Defense living spaces, government provided vehicles, the ELC complex, and attorney client meeting facilities at Guantanamo Naval Base, Guantanamo, Cuba. *See para. 1(j).*

8. The Prosecution respectfully declines to provide any additional discovery beyond what was provided in connection with AE133 and AE155. The unsubstantiated Defense claims of monitoring have been previously litigated in AE133 and AE155 and were soundly rejected by the Military Judge after two lengthy motion hearings.

Respectfully submitted,

//s//
Joanna Baltes
Deputy Trial Counsel