

UNCLASSIFIED//FOR PUBLIC RELEASE
**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

AE284B(WBA)

Defense Reply to Government Response to
Defense Motion to Compel the Production of
Information Related to the Monitoring and/or
Collection of Attorney-Client Privileged
Information

7 April 2014

1. Timeliness: This reply is timely filed.

2. Law and Argument:

a. Prosecution Duty to Learn of Intelligence Community (IC) Monitoring

The Prosecution in its Response states that it has no obligation to learn of Government efforts to monitor defense communications because “[w]hat some U.S. Government entity not involving the Prosecution or its agents may be doing in the year 2014 outside of government efforts in this case...simply has no logical or legal relevance to these proceedings or the charges before this Commission.” AE284A(GOV) at 2. However, the Prosecution misconstrues its discovery obligations in two important respects.

First, the intelligence community is inseparable from the Prosecution. Mr. bin ‘Attash was held for three years in the exclusive custody of the intelligence community before being transferred to Department of Defense custody at Guantanamo Bay in 2006. The Commission and the Prosecution itself have repeatedly recognized that the intelligence community has important equities in this Military Commission. For

example, in its Motion for a Protective Order to Protect Against Disclosure of National Security Information, the Prosecution attached a declaration from the Director of the Central Intelligence Agency indicating that “the substance of the classified information in this case deals with the sources, methods, and activities by which the United States defends against international terrorist organizations.” AE013 at 1. Protective Order #1 contains provisions wherein the defense may apply to the Original Classification Authorities (representatives of the intelligence community) for classification review. *See, e.g.* AE013DDD at ¶ 4(d). The intelligence community has been actively involved in providing classification guidance directly pertaining to this Commission – for example, guidance on the appropriate handling of open source information. *See, e.g.* AE013II(AAA), Attachment D. Most strikingly, the intelligence community has been an active participant in the Commission itself – unbeknownst even to the Commission. On 28 January 2013, the audio and video feeds were cut during an unclassified session of the Commission. Subsequently, Trial Counsel provided the Commission with guidance directly obtained from the intelligence community indicating that the intelligence community “reviews closed-circuit feed of the proceedings to conduct a classification review to ensure that classified information is not inadvertently disclosed.” Tr. at 1485. The fact that the intelligence community operated a de facto “kill switch” on the Commission was only discovered by accident when the feed was cut on 28 January. The intelligence community also has other important equities in the instant case, for example, as it relates to the destruction or preservation of evidence. *See, e.g.* AE080, Joint Defense Motion to Preserve Evidence of Any Existing Detention Facility.

The Prosecution cannot have it both ways. It cannot use intelligence community involvement as a shield to prevent the disclosure of embarrassing information it deems classified and then at the same time claim that the intelligence community is an “entity not involving the Prosecution.” It cannot force the defense to repeatedly abide by intelligence community guidance on the disclosure of the most basic of information pertaining to this case and then pretend that the intelligence community in fact has no involvement in this case. In reality, this case would not exist were it not for the involvement of the intelligence community.

Given the intelligence community’s inseparable relationship with this case, the Prosecution has a clear duty to learn of intelligence community monitoring, particularly where the defense makes a specific request for such information. Indeed, the intelligence community in this case easily crosses the threshold delineated in *Kyles v. Whitley*, 514 U.S. 419, 437 (1995) to be considered an entity “acting on the government’s behalf in the case,” triggering a duty to learn of material and exculpatory evidence whether or not the defense has made a specific request. Like civilian case law, military case law also is quite clear that the Prosecution cannot maintain willful ignorance with respect to the intelligence community’s investigative files. *See, e.g. United States v. Simmons*, 38 M.J. 376, 381 (C.M.A. 1993) (“[w]hen results or reports of military scientific tests or experiments are requested by the defense... Trial counsel must exercise due diligence in discovering such reports not only in his possession but also in the possession, control, or custody of other ‘military authorities’ and make them available for inspection.”). The Prosecution’s duty is heightened when the defense makes a specific discovery request. *See, e.g. United States v. Williams*, 50 M.J. 436, 441 (C.A.A.F. 1999) (“[t]he scope of the

due-diligence requirement with respect to governmental files beyond the prosecutor's own files generally is limited to: (1) the files of law enforcement authorities that have participated in the investigation of the subject matter of the charged offenses...(2) investigative files in a related case maintained by an entity 'closely aligned with the' prosecution...(3) *other files, as designated in a defense discovery request, that involved a specified type of information within a specified entity...*" (emphasis added) (citing *United States v. Veksler*, 62 F.3d 544, 550 (3d Cir. 1995)).

b. Monitoring by Prosecution Immaterial to Discovery Request

Just as the Prosecution misconstrues its discovery obligations, it also fails to grasp the materiality of the information requested by the defense when it claims that "affirmation that neither the Prosecution nor its agents have ever seen, heard, or learned of any such communications should end the Commission's inquiry and foreclose further distraction, as the Accused are in no way prejudiced in their defense if the Prosecution or its agents are unaware of any such monitoring." AE284A(GOV) at 2. Indeed, the defense discovery request is not founded upon an assertion that the Prosecution itself is monitoring confidential communications to learn defense strategy; the discovery request is based upon the chilling effect of continued monitoring and interference by agencies that formerly abused Mr. bin 'Attash, and it is based upon the potential waiver of privileged communications that may result from monitoring, whether or not the monitoring is at the hands of the Prosecution or another Government entity.

Contrary to the Prosecution's suggestion, the defense is not chasing an "imaginary rabbit" down an "imaginary rabbit hole." In fact, the only truth to the Prosecution's analogy might be the fact that instances of Government monitoring and interference seem

like rabbits replicating out of control. Examples include the October 2011 “baseline review” conducted by JTF-GTMO and documented in AE032, in which JTF-GTMO searched, seized, and translated privileged attorney-client communications under the guise of a search for “contraband.” In February 2013, the Commission’s public feed was cut by an entity that Trial Counsel later revealed to be an Original Classification Authority. *See* Tr. at 1445; 1485. The stoppage was the third such occurrence, none of which involved the actual disclosure of classified information. *See* AE133 (WBA Sup.). Then, during the February 2013 hearings, counsel informed the Commission that listening devices disguised as smoke detectors were discovered in the attorney-client visitation huts at “Echo II.” *See* AE133V(KSM); AE133 (WBA Sup.). Like intelligence community monitoring and disruption of Commissions sessions, the sophisticated listening devices discovered at Echo II were discovered fortuitously and despite the assurances of JTF-GTMO that the area was unmonitored. One month later, in March 2013, the Prosecution was provided with an internal, privileged email pertaining to *Ibrahim Ahmed Mahmoud al Qosi v. United States*. *See* AE154. The *al Qosi* incident was but one in a series of breaches of security and confidentiality that 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. During the September 2013 hearings, it was revealed that the National Security Agency maintains an archive of email encryption keys utilized by defense personnel. Tr. at 5802-03.

Defense concern as to unauthorized monitoring was piqued by events occurring outside of the Commission but directly related to the subject matter of this case. In

March of this year, Senator Dianne Feinstein, head of the Senate Intelligence Committee, noted that the CIA had accessed and removed documents from the Committee's computers. These documents were related to the Committee's investigation of the CIA's controversial rendition, detention, and interrogation (RDI) program. See Greg Miller, Ed O'Keefe and Adam Goldman, *Feinstein: CIA searched Intelligence Committee computers*, Washington Post (March 11, 2014), available at http://www.washingtonpost.com/world/national-security/feinstein-cia-searched-intelligence-committee-computers/2014/03/11/982cbc2c-a923-11e3-8599-ce7295b6851c_story.html. As the CIA has no trepidation about monitoring the activities of the powerful Senate Intelligence Committee and seizing its work product, it appears likely that the CIA and other intelligence agencies would not hesitate to monitor communications between counsel and alleged September 11 conspirators, where those alleged conspirators would also be in a position to reveal embarrassing details about the CIA's activities. The defense would be shirking its ethical duties to protect attorney-client privileged communications and work product were it to ignore this obvious fact. The defense has no doubt that the capability of the United States Government to monitor defense communications exists and extends far beyond the phony smoke detectors and OCA monitoring of court sessions already uncovered during the course of these proceedings.

Where the specter of unauthorized Government monitoring is so pervasive, the free exchange of information between attorney and client is irreparably damaged. For Mr. bin 'Attash, fear of Government monitoring is understandably heightened by the circumstances of his decade-long confinement and mistreatment at the hands of the

United States, including the U.S. intelligence community. Where Mr. bin ‘Attash feels that his confidential communications are not respected, he is unwilling to use, and unwilling to sanction his attorneys to use, modes of communication that might be subject to monitoring. This concern exists irrespective and independent of Prosecution involvement. The chilling effect vitiates the attorney-client relationship and prohibits Mr. bin ‘Attash from participating fully in his own defense. *See Faretta v. California*, 422 U.S. 806 (1975); *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) (purpose of attorney –client privilege is to “encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice.”).

In addition to the chilling effect of actual or potential Government monitoring and interference, the defense must also be concerned with waiver of the attorney-client and attorney work product privileges – a problem that exists when the material in question is disclosed to *any* entity of the United States Government, not merely the Prosecution. Because of the importance of these privileges, the D.C. Circuit and District Courts in particular take an unforgiving approach to waiver, reasoning that “if a client wishes to preserve the privilege, it must treat the confidential attorney-client communications like jewels – if not crown jewels.” *In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989). In *In re Sealed Case*, the D.C. Circuit found that even inadvertent disclosure by counsel or client will waive the privilege, noting that “the confidentiality of communications covered by the privilege must be jealously guarded by the holder of the privilege lest it be waived.” *Id*; *see also Wichita Land & Cattle Co. v. American Federal Bank, F.S.B.*, 148 F.R.D. 456, 457 (D.D.C. 1992) (“the rule in this Circuit is clear. Disclosure of otherwise-

privileged materials, even where the disclosure was inadvertent, serves as a waiver of the privilege.”). In keeping with the D.C. Circuit’s strict view on waiver of the privilege, the Court has found waiver even where, for example, materials are provided to the Government as part of an official Government investigation. *See, e.g. Permian Corp. v. United States*, 665 F.2d 1214, 1220-21 (D.C. Cir. 1981); *In Re Subpoenas Duces Tecum*, 738 F.2d 1367, 1370 (D.C. Cir. 1984). In sum, the law in the D.C. Circuit belies the Prosecution’s assertion that no prejudice can result if the Prosecution is unaware of monitored communications. The law also makes clear that, in order to ensure that this Commission or a future court does not later determine that Mr. bin ‘Attash has waived his attorney-client privilege with respect to monitored communications, Mr. bin ‘Attash must exercise due diligence to insist at every available opportunity that the privilege is upheld. In no case could this be more true than the case at bar, where the Government, the Prosecution, and its allies in the Intelligence community, have demonstrated with respect to these accused and even with respect to powerful outside entities such as the Senate Intelligence Committee that they have an obsession with monitoring and interference when it comes to the subject matter of this case.

Ultimately, materiality is a low threshold easily crossed in the instant case, and wilful ignorance is an unlawful and inappropriate response to a request for information within the possession, custody, or control of the United States Government. In this case, the Prosecution cannot remain wilfully blind. It has a duty to learn of information within the possession of the intelligence community and to share that information with the defense where the information is exculpatory or is responsive to the defense discovery

request. This Commission should compel the Prosecution to search for and obtain the requested information.

3. Oral Argument:

The defense requests oral argument.

4. Attachments:

A. Certificate of Service

//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

Attachment A

CERTIFICATE OF SERVICE

I certify that on 7 April 2014, I electronically filed the **Defense Reply to Government Response to Defense Motion to Compel the Production of Information Related to the Monitoring and/or Collection of Attorney-Client Privileged Information** with the Trial Judiciary and served it on all counsel of record by e-mail.

//s//

CHERYL BORMANN
Learned Counsel

Attachment A