

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

_____)	
RICHARD G. CONVERTINO)	
)	
Plaintiff,)	Civil Action No. 04-00236 (RCL)
)	
v.)	
)	
UNITED STATES DEPARTMENT OF JUSTICE,)	
<i>et al.</i>)	
)	
Defendants.)	
_____)	

**JONATHAN TUKEL’S MOTION AND MEMORANDUM OF LAW
TO INTERVENE TO ASSERT VARIOUS PRIVILEGES
IN RESPONSE TO PLAINTIFF’S MOTION TO COMPEL PRODUCTION
FROM DEFENDANT UNITED STATES DEPARTMENT OF JUSTICE**

Pursuant to Local Rule 7(j) and Federal Rule of Civil Procedure 24(b), Jonathan Tukul respectfully requests leave of the Court to intervene in the above-caption action. To that end, Mr. Tukul files this Motion and incorporated Memorandum of Law to Intervene in order to assert the attorney-client privilege and invoke the work product doctrine with respect to certain documents sought in connection with plaintiff Richard G. Convertino’s Motion to Compel Production from Defendant United States Department of Justice (“DOJ”) (“Motion to Compel”).

Mr. Tukul was named as a defendant to Count I of the Complaint filed in the above-captioned action on February 13, 2004. Subsequently, on October 19, 2005, the Court dismissed Count I of the Complaint, and in doing so, dismissed the suit against Mr. Tukul.¹ In the spring of 2009, the only defendant remaining, the DOJ, was served with discovery requests and in

¹ At present, only Count II of the Complaint survives; Count II asserts a claim against the DOJ for violations of the Privacy Act. Mr. Tukul ceased being First Assistant U.S. Attorney in May 2005, and thus, per Federal Rule of Civil Procedure 25(d), he was automatically dismissed as an official capacity defendant at that time.

RECEIVED

JUL 31 2009

Clerk, U.S. District and
Bankruptcy Courts

response, asserted various privileges, including the attorney-client privilege, over approximately 3,500 pages of documents. *See* Motion to Compel at 1. Within the 3,500 pages are approximately 37 e-mail communications between Mr. Tukul and his personal counsel, Cadwalader, Wickersham & Taft LLP (“Cadwalader”), sent via his DOJ-provided e-mail address. *See* Motion to Compel, Ex. A at DOJ6000414-419, DOJ6000469-504, DOJ6000508-555, DOJ6000615-616, DOJ7000401, DOJ7002894-2980.

As Mr. Tukul is the holder of privileges regarding these documents, he respectfully seeks to intervene in this case in order to assert all applicable privileges concerning documents DOJ6000414-419, DOJ6000469-504, DOJ6000508-555, DOJ6000615-616, DOJ7000401, DOJ7002894-2980, and any other privileged communications between Mr. Tukul and his personal counsel (“Privileged Documents”). Mr. Tukul’s grounds for asserting these privileges are fully briefed in his Motion and Memorandum of Law in Opposition to Plaintiff’s Motion to Compel, attached hereto as Exhibit A.²

ARGUMENT

Federal Rule of Civil Procedure 24(b) provides for permissive intervention, upon timely motion, “when an applicant's claim or defense and the main action have a question of law or fact in common.” Fed. R. Civ. P. 24(b)(2). In exercising its discretion to consider a motion for permissive intervention, “the court shall consider whether the intervention will unduly delay or prejudice the adjudication of the rights of the original parties.” Fed. R. Civ. P. 24(b)(3). Mr. Tukul meets Rule 24(b)’s prerequisites for permissive intervention.

² Also attached to the instant motion is the Notice of Appearance for James K. Robinson, counsel to Mr. Tukul. *See* Exhibit B.

First, Mr. Tukul's motion is timely. It was not until the spring of 2009 that Mr. Tukul received notice that the plaintiff's document requests to the DOJ called for production of the Privileged Documents. Upon receiving such notice, Mr. Tukul immediately sought to identify and assert all applicable privileges relating to the Privilege Documents.

Second, the privileges that Mr. Tukul seeks to assert are directly implicated by the discovery requests made by the plaintiff. As the plaintiff's Motion to Compel indicates, he argues that the success (or failure) of his case is inextricably intertwined with the Privileged Documents. *See* Motion to Compel at ___. Further, as recognized by the plaintiff in his Motion to Compel, Mr. Tukul is the sole holder of the privileges. *Id.* at ___. Thus, no current party to the litigation can effectively assert the attorney-client privilege and invoke the work product doctrine on his behalf.

Finally, allowing Mr. Tukul to intervene in this action for the limited purpose of asserting his attorney-client privilege and invoking the work product doctrine as to the Privilege Documents will not unduly delay the litigation or prejudice the rights of the existing parties. This case, although filed in 2004, has not progressed past the point of initial discovery. Thus, ample time still exists for the parties to work cooperatively to produce all non-privileged material relevant to the matter. To that end, Mr. Tukul stands ready to cooperate in any way he can to assist in the efficient and timely production of such material.

Thus, Mr. Tukul respectfully requests that the Court grant his intervention in this case for the limit purpose of asserting his attorney-client privilege and invoking the work product doctrine regarding the Privileged Documents.

Dated: July 31, 2009

Respectfully Submitted,

By: /s/ James K. Robinson
James K. Robinson
Cadwalader Wickersham & Taft, LLP
700 Sixth Street, N.W.
Washington, D.C. 20001
(202) 862-2494
Fax: (202) 862-2400
jim.robinson@cwt.com

ATTORNEY FOR JONATHAN TUKEL

CERTIFICATE OF SERVICE

I hereby certify that I have this date caused one true and correct copy of the within documents to be served in the above-captioned case by regular mail on all parties of record.

/s/ James K. Robinson

Exhibit A

**to Jonathan Tukul's
Motion and Memorandum of Law to Intervene
to Assert Various Privileges in Response to
Plaintiff's Motion to Compel Production from
Defendant United States Department of Justice**

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

_____)	
RICHARD G. CONVERTINO)	
)	
Plaintiff,)	Civil Action No. 04-00236 (RCL)
)	
v.)	
)	
UNITED STATES DEPARTMENT OF JUSTICE,)	
<i>et al.</i>)	
)	
Defendants.)	
_____)	

**JONATHAN TUKEL’S MOTION AND MEMORANDUM OF LAW
IN OPPOSITION TO PLAINTIFF’S MOTION TO COMPEL**

COMES NOW Jonathan Tukul, who files this Motion and incorporated Memorandum of Law in opposition to plaintiff Richard G. Convertino’s Motion to Compel Production from Defendant United States Department of Justice (“DOJ”) to assert the attorney-client privilege and invoke the work product doctrine concerning documents DOJ6000414-419, DOJ6000469-504, DOJ6000508-555, DOJ6000615-616, DOJ7000401, DOJ7002894-2980, and any other privileged communications between Mr. Tukul and his personal counsel (“Privileged Documents”) and preclude the production of such documents and states as follows:

On February 13, 2004, the plaintiff filed an action against the DOJ for violations of the Privacy Act, 5 U.S.C. § 552a and for injunctive relief under the First Amendment to the United States Constitution, the Lloyd Lafayette Act and the Administrative Procedures Act. *See generally* Complaint (Dkt. 1). In addition to the DOJ, the Complaint brought a cause of action against Mr. Tukul and others in their official capacity. *Id.* at ¶ 7. The plaintiff alleged that the DOJ, Mr. Tukul, and others disclosed sealed court records to the Detroit Free Press and used sealed court transcripts to attack the plaintiff’s credibility in retaliation for the plaintiff making

statements to Washington, D.C. government officials and testifying before the United States Senate Finance Committee concerning *United States v. Koubriti*. *Generally id.* As to Mr. Tukul, Count I of the Complaint alleged that he, with the DOJ, disclosed confidential, false and misleading information about the plaintiff to the press and failed to properly safeguard confidential personnel records relating to the Office of Professional Responsibility's investigation of the plaintiff. *Id.* at 20-21.

On October 19, 2005, the Court dismissed Count I of the Complaint, and in doing so, dismissed the suit against Mr. Tukul.¹ Subsequently, the only defendant remaining, the DOJ, was served with discovery requests and in response, asserted various privileges, including the attorney-client privilege and work product doctrine, over approximately 3,500 pages of documents. *See* Motion to Compel at 1. Within the 3,500 pages are approximately 37 e-mail communications between Mr. Tukul and his personal counsel, Cadwalader, Wickersham & Taft LLP ("Cadwalader"), sent via his DOJ-provided e-mail address. *See* Motion to Compel, Ex. A at DOJ6000414-419, DOJ6000469-504, DOJ6000508-555, DOJ6000615-616, DOJ7000401, DOJ7002894-2980; *see also* June 15, 2009 Declaration of Jonathan Tukul ("Tukul Decl.") ¶¶ 5, 6. The Privileged Documents span a short time frame, August 2004 and December 2004, and comprise no more than 5% of the total number of privileged documents. Motion to Compel, Ex. A. None of the Privileged Documents have been shared with third parties.

ARGUMENT

I. COMMUNICATIONS BETWEEN MR. TUKEL AND CADWALADER ARE PROTECTED BY THE ATTORNEY-CLIENT PRIVILEGE.

¹ Count II of the Complaint has not been dismissed. Count II only asserts a claim against the DOJ for violations of the Privacy Act.

Communications between Mr. Tukul and Cadwalader are protected by the attorney-client privilege. Mr. Tukul retained Cadwalader in anticipation of litigation in or around 2004. Tukul Decl. ¶ 5. All of the Privileged Documents are between Mr. Tukul and Cadwalader only – no third parties are included on any communications – and are for the purposes of securing legal advice relating to litigation issues implicating Mr. Tukul. Tukul Decl. ¶¶ 5, 7, 8; *see e.g., In re Sealed Case*, 737 F.2d 94, 316-17 (D.C. Cir. 1984) (quoting *United States v. United Shoe Machinery Corp.*, 89 F. Supp. 357, 358-59 (D. Mass. 1950)). Furthermore, the DOJ has produced a sufficiently descriptive privilege log to the plaintiff (Motion to Compel, Ex. A) which fully and accurately describes the nature of the Privileged Documents. *See* Fed. R. Civ. P. 26(b)(5). Mr. Tukul has not waived the attorney-client privilege that exists between him and Cadwalader. Tukul Decl. ¶¶ 8, 9.

II. MR. TUKEL HAS NOT WAIVED THE ATTORNEY-CLIENT PRIVILEGE WITH RESPECT TO COMMUNICATIONS WITH CADWALADER.

Contrary to the plaintiff's argument, Mr. Tukul's attorney-client privilege was not waived by virtue of his use of his DOJ-issued e-mail account and computer. Indeed, "[a]ssuming a communication is otherwise privileged, the use of the company's e-mail system does not, without more, destroy the privilege." *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 251 (S.D.N.Y. 2005).

Federal Rule of Evidence 502(b)² states that no waiver of the attorney-client privilege or

² Rule 502(b) is applied to matters filed prior to September 19, 2008 (the enactment date) where it is "just and practicable" to do so. Pub. L. No. 110-322, 122 Stat. 3537 (Sept. 19, 2008). Here, the request for and production of documents post-dates the enactment of Rule 502(b). Thus, prior to that request and production no privilege issues arose and it is "just and practicable" for this Court to apply the limitations set forth in Rule 502(b) to the Privileged Documents. Consequently, all of the cases cited by the plaintiff in his Motion to Compel are inapposite as all of them pre-date the enactment of Federal Rule of Evidence 502(b) which expressly addresses inadvertent disclosures of otherwise privileged material.

work product doctrine occurs where “(1) the disclosure is inadvertent;” and “(2) the holder of the privilege or protection took reasonable steps to prevent disclosure.” Fed. R. Evid. 502(b) (2008). The Advisory Committee Note to Rule 502(b) provides the following “guidelines” to assist in assessing whether an inadvertent disclosure waived the privilege: “the reasonableness of precautions taken, the time taken to rectify the error, the scope of discovery, the extent of disclosure and the overriding issue of fairness” as well as “the number of documents to be reviewed and the time constraints for production.” Fed. R. Evid 502(b) advisory committee’s note (2008) (citing *U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985) and *Hartford Fire Ins. Co. v. Garvey*, 109 F.R.D. 323, 332 (N.D. Cal. 1985)).

To the extent any disclosure of privileged material occurred, it was most certainly inadvertent. At all times, Mr. Tukul’s e-mail was password protected; thus, no third parties could access any material in his e-mail other than through a collection of data from DOJ’s electronic servers. Tukul Decl. ¶ 4. Although, Mr. Tukul understood that DOJ Information Technology personnel accessed his DOJ-issued computer in connection with maintaining and upgrading the DOJ’s electronic systems, he was aware that performing systems maintenance and upgrades did not involve accessing personal files, including e-mail. Tukul Decl. ¶ 4. Mr. Tukul has not shared any of the Privileged Documents with any third parties. Tukul Decl. ¶ 8.

In addition, Mr. Tukul deleted all e-mail sent or received from Cadwalader from his e-mail inbox immediately after reading it, and it would have been his practice to empty the electronic trash bin where deleted messages are temporarily stored. Tukul Decl. ¶ 10; *see also Curto v. Med. World Commc’ns, Inc.*, No. 03-CV-6327, 2006 WL 1318387, *9 (E.D.N.Y. May 15, 2006) (holding that because plaintiff took affirmative steps to delete personal privileged communications and company had no direct access to her computer, combined with ambiguous nature of company’s policies plaintiff’s privilege remained intact). Thus, he was unaware that

copies of his privileged communications with Cadwalader were located in any DOJ electronic system until receiving notice from DOJ counsel in April 2009 that privileged correspondence had been collected in connection with this case. Tukul Decl. ¶ 10. Consequently, Mr. Tukul reasonably expected that his communications with Cadwalader were confidential and were not being disclosed to any third parties, including the DOJ. *In re Asia Global Crossing, Ltd.*, 322 B.R. at 258 (“the question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable.”); *Id.*

Moreover, “the objective reasonableness of [Mr. Tukul’s] intent will depend on the [DOJ’s] e-mail policies regarding use and monitoring, its access to the e-mail system, and the notice provided to the employees.” *Id.* at 251, 258; *Curto*, 2006 WL 1318387 at *2, 4-5, 7. The DOJ policies concerning e-mail and Internet usage expressly *allow* employees to use their DOJ-provided e-mail mail accounts for personal use. Tukul Decl. ¶ 2. Prior to the collection of the Privileged Documents for this case, Mr. Tukul was not aware that e-mail sent from his DOJ account was monitored by the DOJ, even though DOJ policy permits monitoring under some circumstances not applicable here. Tukul Decl. ¶ 12. Indeed, he was not aware that, in practice, the DOJ randomly audited or monitored employees’ e-mail even though DOJ policy permits monitoring for some purposes. Tukul Decl. ¶ 13; *see also Curto*, 2006 WL 1318387 at *5 (holding that a determination of whether the company enforced its electronic usage policy assists in assessing the reasonableness of the precautions taken by the employee to prevent inadvertent disclosure). Finally, Mr. Tukul was not informed that his e-mail was being collected by anyone

within the DOJ prior to such a collection,³ Tukul Decl. ¶ 14, and therefore, prior to this time, he did not have the opportunity to assert the attorney-client privilege.

In light of Mr. Tukul's understanding that DOJ policies permitted his personal use of his DOJ e-mail address and his reasonable belief that the steps he took to ensure the confidentiality of his communications with Cadwalader were effective, Mr. Tukul's attorney-client privilege has not been inadvertently waived. Thus, the plaintiff is not entitled to the production of the Privileged Documents.

III. COMMUNICATIONS BETWEEN MR. TUKEL AND CADWALADER CONTAIN MATERIAL PROTECTED BY THE ATTORNEY WORK PRODUCT DOCTRINE.

Federal Rule of Civil Procedure 26(b)(3) protects from discovery "documents and tangible things that are prepared in anticipation of litigation . . . by or for another party or its representative (including the other party's attorney . . .)." Work product only may be disclosed upon a showing of "substantial need" and the inability to obtain the "substantial equivalent" without undue hardship. *Id.* Courts "must take particular care to protect the 'mental impressions, conclusions, opinions, or legal theories of an attorney'" which may be reflected in correspondence or "countless other tangible and intangible ways." *Banks v. Office of the Senate Sergeant-At-Arms and Doorkeeper*, 236 F.R.D. 16, 19 (D.D.C. 2006) (citations omitted). Thus, opinion work product is "entitled to special protection" and as a result, a "stronger showing of necessity" is required to overcome the protections of the attorney work product doctrine. *Id.* (quoting *Byers v. Burleson*, 100 F.R.D. 436, 439 (D.D.C. 1983) (citing Fed. R. Civ. P. 26(b)(3))

³ Notably, Mr. Tukul has never provided (or been asked to provide) his DOJ-issued computer to anyone within the DOJ, including anyone in the United States Attorney's Office for the Eastern District of Michigan, DOJ Criminal Division, Executive Office of U.S. Attorneys, Executive Office of U.S. Trustees, or Assistant Attorney General for Administration. Tukul Decl. ¶ 11.

and *Upjohn Co. v. United States*, 449 U.S. 383, 400-01 (1981)); *In re Sealed Case*, 856 F.2d 268, 273 (D.C. Cir. 1988)).

In this case, many of the e-mails exchanged between Mr. Tukul and his counsel include highly confidential opinion work product which should not be disclosed. Indeed, the majority of the Privileged Documents included on the DOJ's privilege log directly pertain to drafts and responses, crafted by Cadwalader and Mr. Tukul, to the Office of Inspector General's ("OIG") draft investigation report.⁴ See Exhibit A to the Motion to Compel entries DOJ7002894-2938 and DOJ7002944-2980. E-mail communications between Mr. Tukul and his counsel exchanging drafts of responses or letters concerning the OIG investigation report constitute opinion work product which should be protected from disclosure. See *Banks*, 236 F.R.D. at 21 (finding that exchanges of drafts between the Office of Sergeant-at-Arms of the United States Senate and its counsel were "clearly" opinion work product because they "tend[ed] to reveal counsel's opinions and mental impressions" and were thus, protected from disclosure).

Furthermore, these documents unquestionably were created in anticipation of litigation. See also Tukul Decl. ¶ 7. At the time of the communications (August to December 2004), the instant suit had already been filed. Moreover, Mr. Tukul retained Cadwalader to represent him in connection with issues directly relevant to this suit and in anticipation of potential litigation surrounding those issues. Thus, all communications between Cadwalader and Mr. Tukul were made in anticipation of litigation.

Finally, the plaintiff cannot demonstrate a substantial need for the protected material. The OIG's investigation report has been made available to the plaintiff. See Dkt. 47 at 4.

⁴ The OIG provided individuals named in or interviewed for the report with the opportunity to comment on a draft of the report prior to it being finalized.

Because Mr. Tukul did not draft the report and was not responsible for compiling the information contained directly therein, any responses or commentary from Mr. Tukul to the report are not likely to assist the plaintiff in proving its case against DOJ and are thus, irrelevant. Indeed, any communications he had with his counsel concerning the report, which were not shared with third parties, would not assist the plaintiff in proving the “existence of a coverup.” *See* Motion to Compel at 17. Because Cadwalader is not part of the United States government (including the DOJ), it stands to reason that communications solely with Cadwalader would not prove the existence of a cover-up by the DOJ.

CONCLUSION

For the foregoing reasons, Mr. Tukul respectfully requests that the Court deny the plaintiff’s Motion to Compel the production of documents DOJ6000414-419, DOJ6000469-504, DOJ6000508-555, DOJ6000615-616, DOJ7000401, DOJ7002894-2980, and any other Privileged Documents.

Dated: July 31, 2009

Respectfully Submitted,

By: /s/ James K. Robinson
James K. Robinson
Cadwalader Wickersham & Taft, LLP
700 Sixth Street, N.W.
Washington, D.C. 20001
(202) 862-2494
Fax: (202) 862-2400
jim.robinson@cwt.com

ATTORNEY FOR JONATHAN TUKEL

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

RICHARD G. CONVERTINO)	
)	
Plaintiff,)	Civil Action No. 04-00236 (RCL)
)	
v.)	
)	
UNITED STATES DEPARTMENT OF JUSTICE,)	
<i>et al.</i>)	
)	
Defendants.)	

DECLARATION OF JONATHAN TUKEL

JONATHAN TUKEL declares and states as follows:

1. In connection with my employment at the United States Attorney’s Office for the Eastern District of Michigan, I was provided with a Department of Justice (“DOJ”) electronic mail account with the following address: Jonathan.Tukel@usdoj.gov.
2. I used my DOJ-provided electronic mail address to send and receive correspondence relating to my job responsibilities and personal correspondence, as permitted by the DOJ’s policies concerning electronic mail and Internet use. (Relevant policies attached hereto as Exhibits A through C).
3. At all times, I was issued a DOJ computer for my use in the office, and which also could be used as a laptop at home and while travelling. When used either inside or outside the office, the computer could access the DOJ email system.
4. At all times, my electronic mail was password protected (*see* Exhibit D, Appendix A); thus, no third parties could access any material in my electronic mail other than through a collection of data from DOJ’s electronic servers. DOJ Information Technology personnel accessed my DOJ-issued computer in connection with maintaining and upgrading the DOJ’s electronic systems. However, I understand that performing systems maintenance and upgrades does not involve accessing personal files, including electronic mail.
5. I retained Cadwalader, Wickersham & Taft LLP (“Cadwalader”) in 2004 in anticipation of potential litigation.
6. Between August 2004 and December 2004, I communicated directly with my personal counsel, James Robinson, Michael Horowitz, and Adam Lurie of Cadwalader using my DOJ-provided electronic mail address (Jonathan.Tukel@usdoj.gov).

7. All communications sent via Jonathan.Tukel@usdoj.gov to Messrs. Robinson, Horowitz, and Lurie (or any other representative of Cadwalader) are privileged communications which directly relate to the issues in the instant lawsuit.
8. I have not shared any communications sent via Jonathan.Tukel@usdoj.gov to Messrs. Robinson, Horowitz, or Lurie (or any other representative of Cadwalader) with third parties, including non-DOJ persons.
9. I have not waived the attorney-client privilege that exists among Messrs. Robinson, Horowitz, Lurie and myself (and any other representatives of Cadwalader).
10. I deleted all electronic mail sent or received from Messrs. Robinson, Horowitz, and Lurie (or any other representative of Cadwalader) from my electronic mail inbox immediately after reading it, and it would have been my practice to empty the electronic trash bin where deleted messages are temporarily stored. Thus, I was unaware that copies of privileged communications between Cadwalader and myself were located in any DOJ electronic system until I was notified by defense counsel in April 2009 that such correspondence was collected.
11. I have never provided (or been asked to provide) my DOJ-issued computer to anyone within the DOJ, including anyone in the United States Attorney's Office for the Eastern District of Michigan, DOJ Criminal Division, Executive Office of U.S. Attorneys, Executive Office of U.S. Trustees, or Assistant Attorney General for Administration.
12. I am not aware that my electronic mail sent from Jonathan.Tukel@usdoj.gov was monitored by the DOJ, as described in DOJ policies, even though DOJ policy permits monitoring under certain circumstances. (*See Exhibits A through C*).
13. I am not aware that, in practice, the DOJ randomly audits or monitors (as described in DOJ policies) employees' DOJ-issued computers to monitor electronic mail even though DOJ policy permits monitoring for certain purposes. (*See Exhibits A through C*).
14. I was not informed that my electronic mail, sent via Jonathan.Tukel@usdoj.gov, was being collected by anyone within the DOJ prior to such a collection.
15. At all times, I took reasonable steps to ensure the confidentiality of my electronic mail, including all electronic mail exchanged between Cadwalader and myself.

I declare under penalty of perjury that the foregoing is true and correct. Executed on July 31, 2009.

/s/ Jonathan Tukel

Exhibit A
to Declaration of Jonathan Tukul dated July 31, 2009

7/31/2009

Misuse of Email and Internet Privil...

U.S. Department of Justice

Washington, D.C. 20530

January 6, 2000

MEMORANDUM FOR JUSTICE MANAGEMENT DIVISION EMPLOYEES

FROM: STEPHEN R. COLGATE, Assistant Attorney General for Administration

SUBJECT: Misuse of Email and Internet Privileges

On several occasions I have written to all Justice Management Division (JMD) employees about the appropriate use of the Internet. These memoranda were intended to apply to the use of email systems, whether internal to the Department or over the Internet. The great majority of JMD employees have clearly understood and complied with the guidance those memoranda offered. Regrettably, a few of you have not.

I have recently become aware that a significant number of offensive electronic messages, some sexually explicit (including pornographic photographs) have been transmitted and received by employees throughout JMD. We know who distributed the offensive material, and we know to whom it was sent.

I am sending this memorandum to all of you as a caution: unrestricted access to the Internet and use of government e-mail for non-work purposes are privileges we have extended to our workforce. In return, we require that employees conduct themselves professionally and refrain from using Department resources for offensive activities. **The use of DOJ systems to view or transmit sexually explicit material is strictly prohibited and we will not tolerate it. Those who disregard this policy face disciplinary action, up to and including their removal from the Federal service.**

JCON is a Department of Justice system. When you use it, you are consenting to monitoring, among other things, to identify improper use and to ensure the safety and security of our workplace. We will be vigorous in our monitoring efforts. Moreover, we encourage employees who receive offensive material over JCON from coworkers to report it to their supervisors. Supervisors should bring such matters to the attention of their Staff Directors and the Personnel Staff's Employee and Labor Relations Section.

Exhibit B
to Declaration of Jonathan Tukel dated July 31, 2009

DOJ 2740.1



USE AND MONITORING OF DOJ COMPUTERS AND COMPUTER SYSTEMS

Approval Date: Nov. 7, 2005

Approved By: PAUL R. CORTS
Assistant Attorney General
for Administration

Distribution: BUR/H-1; OBD/H-1; SPL-23

Initiated by: Justice Management Division
Office of General Counsel

1. **PURPOSE.** This order states the Department's policy on the use of departmental computers and computer systems, the lack of expectation of privacy with respect to such use, and authorized monitoring or access to information on departmental computers and computer systems.
2. **SCOPE.** This policy applies to all classified and unclassified computer systems and peripheral devices (such as Personal Electronic Devices) that are acquired for use by, owned, operated, and managed by a departmental component. Use of a privately-owned computer or device to connect to a departmental computer system constitutes use of a departmental computer system while connected. This policy applies to all Department components. Computer systems owned by other agencies are excluded from this policy and are governed by the policies of those agencies.
3. **POLICY.**
 - a. **Approval for Deviation from Policy.** No component shall issue any less restrictive policy with respect to the acceptable and prohibited use of Department computer systems and Department provided Internet resources (e.g., Internet electronic mail, World Wide Web access, Department Internet

Web site) without written approval of the Department Chief Information Officer. Components may issue further implementing guidance on such use consistent with this policy without written approval. Components may not deviate from the monitoring and access provisions of this order.

b. Use of Department Computers and Computer Systems.

- (1) Use of departmental computer systems, including but not limited to Internet e-mail, departmental e-mail, word processing systems, and connections to Internet sites, is subject to the same restrictions on use as are other government-furnished resources provided for the use of employees. (See 5 C.F.R. §§ 2635.101(b)(9) and 2635.704(a).)
- (2) While departmental computer systems are provided for official use, some personal use of government computer systems is permitted in accordance with existing policy on personal use of government property, where there is negligible cost to the government and no interference with official business. (See 28 C.F.R. § 45.4.)

c. Prohibited Use of Department Computers and Computer Systems.

- (1) The following activities are prohibited on department computers and computer systems during working or non-working hours, except when conducting legitimate departmental business with the express prior permission of the employee's supervisor:
 - (a) Use of Internet sites that result in an additional charge to the government.
 - (b) The obtaining, viewing, or transmitting of sexually explicit material, contraband, or other material inappropriate to the workplace.
 - (c) Use for other than official governmental business that results in operational slowdowns or delays in conducting departmental business (e.g., mass mailings or sending or downloading large files such as programs, pictures, video files, or games).
 - (d) Any otherwise prohibited activity, such as sending out solicitations or engaging in prohibited political activity.

- (2) Downloading and/or installing any program, software or executable file on department computers is prohibited unless approved in accordance with component IT security policy.
 - (3) Employees may not use department computers or computer systems in a way that infringes any copyright, patent, trademark, trade secret or other proprietary right of any party. Further guidance on copyright will be addressed in separate Department policy.
- d. **No Expectation of Privacy.** Individual employees should NOT expect privacy in the use of government computers or computer systems. The Department may access e-mail messages, files, records, or other documents on government computer systems whenever it has a legitimate governmental purpose for doing so.
- e. **Monitoring or Access to E-mail or Documents on Computer Systems.** Use of departmental computer systems constitutes consent to monitoring.
- (1) **Authorized Access.** Monitoring and accessing employees' e-mail messages, Internet activities, documents, files, or other use of departmental computer systems that are restricted by a password or other security mechanism may only be done for authorized purposes. Accessing shared storage (i.e., a public or a shared server disk drive) does not constitute accessing another employee's computer system.
 - (2) **Authorized Purposes for Monitoring or Access** include:
 - (a) For system administration and system security.
 - (b) For investigatory purposes by the Office of Professional Responsibility, the Office of the Inspector General, the Federal Bureau of Investigation, or the Criminal Division.
 - (c) In response to a court order, grand jury subpoena, or search warrant.
 - (d) In order to prevent death or serious injury to any person.
 - (3) **Authorizing Officials.** Access to an employee's computer system for any other reason, such as for

suspected misconduct not connected with an official investigation by one of the offices listed above, must be authorized by:

- (a) The head of the Bureau where the employee works, for Bureau personnel.
- (b) The head of the Executive Office of U.S. Attorneys (EOUSA), for EOUSA personnel.
- (c) The head of the Executive Office of U.S. Trustees (EOUST), for EOUST personnel.
- (d) The head of the National Drug Intelligence Center (NDIC), for NDIC personnel.
- (e) The Assistant Attorney General for Administration for all other components.

This authority may not be delegated below the level of a principal deputy.

- (4) **Notification of Monitoring.** All components are required to provide adequate notice to their employees that their use of the departmental computer system constitutes consent to monitoring. The Standard Warning Banner promulgated by the Department's Chief Information Officer provides such adequate notice.
- (5) **Employee Activities.** Nothing in this policy creates any enforceable rights; however, unauthorized use or monitoring or improper access to an employee's computer system may result in disciplinary action. Employees are prohibited from accessing the e-mail, electronic files or documents, or otherwise monitoring the online activities of another employee except in accordance with this policy.

/s/PAUL R. CORTS
Assistant Attorney General
for Administration

Exhibit C
to Declaration of Jonathan Tukel dated July 31, 2009

DOJ 2740.1A



USE AND MONITORING OF DOJ COMPUTERS AND COMPUTER SYSTEMS

Approval Date: December 2, 2008

Approved By: Lee J. Lofthus
Assistant Attorney General
for Administration

Distribution: BUR/H-1; OBD/H-1; SPL-23

Initiated by: Justice Management Division
Office of General Counsel

1. **PURPOSE.** This order states the Department's policy on the use of departmental computers and computer systems, the lack of expectation of privacy with respect to such use, and authorized monitoring or access to information on departmental computers and computer systems.
2. **SCOPE.** This policy applies to all classified and unclassified computer systems and peripheral devices (such as Personal Electronic Devices) that are acquired for use by, owned, operated, or managed by a departmental component. A privately-owned computer or device that is connected to a departmental computer system is considered to be a departmental computer system while so connected. This policy applies to all Department components.
3. **POLICY.**
 - a. **Approval for Deviation from Policy.** No component shall issue any less restrictive policy with respect to the acceptable and prohibited use of Department computer systems and Department provided Internet resources (e.g., Internet electronic mail, World Wide Web access, Department Internet Web site) without written approval of the Department Chief Information Officer. Components may issue further implementing guidance on such use consistent with this policy

USE AND MONITORING OF DOJ COMPUTERS AND COMPUTER SYSTEMS

without written approval. Components may not deviate from the monitoring and access provisions of this order.

b. Use of Department Computers and Computer Systems.

- (1) Use of departmental computer systems, including but not limited to Internet e-mail, departmental e-mail, word processing systems, and connections to Internet sites, is subject to the same restrictions on use as are other government-furnished resources provided for the use of employees. (See 5 C.F.R. § 2635.101(b)(9) and 2635.704.)
- (2) While departmental computer systems are provided for official use, some personal use of government computer systems is permitted in accordance with existing policy on personal use of government property, where there is negligible cost to the government and no interference with official business. (See 28 C.F.R. § 45.4.)

c. Prohibited Use of Department Computers and Computer Systems.

- (1) The following activities are prohibited on department computers and computer systems during working or non-working hours, except when conducting legitimate departmental business with the express prior permission of the employee's Component Head, Deputy Component Head or Field Office Head:
 - (a) Use of Internet sites that result in an additional charge to the government.
 - (b) Using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

USE AND MONITORING OF DOJ COMPUTERS AND COMPUTER SYSTEMS

- (c) The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials or materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.
- (d) Use that could cause congestion, delay, or disruption of service to any government system or equipment, unless for legitimate departmental business. For example, electronic greeting cards, video, sound or other large file attachments can degrade the performance of the entire network, and should not be viewed or sent on Department computers. Accessing continuous data streams (such as viewing streaming video or listening to streaming audio/radio on a media website) could also degrade the performance of the entire network and is an inappropriate use (except when access is provided by the Department or is otherwise authorized).
- (e) The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- (f) Any use to circumvent security controls on Department or other external systems.
- (g) Knowingly using anonymizer sites (anonymizer sites hide the user's identity from the Internet site being visited; however, in doing so, they also bypass the blocking mechanism designed to protect Department systems from malicious Internet sites).
- (h) Knowingly visiting malicious resources or sites.
- (i) Using peer-to-peer (P2P) file sharing sites on the Internet (e.g., sites dedicated to downloading audio or video files), or using IP telephony sites.

- (j) Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).
 - (k) Any otherwise prohibited activity, such as sending out solicitations, participating in any lobbying activity, or engaging in prohibited political activity.
 - (l) Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate Agency approval has been obtained, or uses at odds with the agencies mission or positions.
 - (m) Downloading, exchanging, e-mailing, or otherwise using or making available any material (such as computer software or music) in a way that infringes upon any copyright, patent, trademark, trade secret or other proprietary or privacy right of any party.
- (2) Downloading and/or installing any program, software or executable file on department computers is prohibited unless approved in accordance with component IT security policy.
- d. **Proper Representation** It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using government office equipment for nongovernment purposes. If there is expectation that such a personal use could be interpreted to represent an agency, then an adequate disclaimer must be used. One acceptable disclaimer is - "The contents of this message are mine personally and do not reflect any position of the Government or

USE AND MONITORING OF DOJ COMPUTERS AND COMPUTER SYSTEMS

my agency." The Standards of Conduct states - "...an employee shall not use or permit the use of his Government position or title or any authority associated with his public office in a manner that could reasonably be construed to imply that his agency or the Government sanctions or endorses his personal activities..." (5 CFR § 2635.702(b)).

- e. **No Expectation of Privacy.** Individual employees should NOT expect privacy in the use of government computers or computer systems. The Department may access e-mail messages, files, records, or other documents on government computer systems whenever it has a legitimate governmental purpose for doing so.

- f. **Monitoring, Disclosing, or Accessing E-mail or Documents on Computer Systems.** Use of departmental computer systems constitutes consent to monitoring and disclosure of information stored on or transiting the departmental computer system as provided below. The Department routinely conducts monitoring and intercepts communications for security purposes and to detect improper use. Such monitoring and interception includes the use of software tools that examine the content of Internet communications and email, and block access to known or suspected malicious Internet sites. The Department may block or otherwise prevent any improper use or activity prohibited in section 3.c. above.
 - (1) **Authorized Access.** Monitoring, disclosing, and accessing another employee's e-mail messages, Internet activities, documents, files, or other information stored on or transiting the departmental computer system may only be done for authorized purposes. Accessing shared storage (i.e., a server or disk drive intended for shared or public access) does not constitute accessing another employee's computer system.

 - (2) **Authorized Purposes for Monitoring, Disclosing, or Accessing:**
 - (a) For system administration and system security.

USE AND MONITORING OF DOJ COMPUTERS AND COMPUTER SYSTEMS

- (b) For investigatory purposes by, or as authorized by, the Office of Professional Responsibility, the Office of the Inspector General, the Federal Bureau of Investigation, or the Criminal Division.
 - (c) In response to a court order, grand jury subpoena, or search warrant.
 - (d) In order to prevent death or serious injury to any person.
- (3) **Authorizing Officials.** Access to an employee's computer system for any other reason, such as for suspected misconduct not connected with an official investigation by one of the offices listed above, must be authorized by:
- (a) The head of the Bureau where the employee works, for Bureau personnel;
 - (b) The head of the Executive Office for U.S. Attorneys, for U.S. Attorneys personnel;
 - (c) The head of the Executive Office for U.S. Trustees (EOUST), for EOUST personnel;
 - (d) The head of the National Drug Intelligence Center (NDIC), for NDIC personnel; or
 - (e) The Assistant Attorney General for Administration for all other components.

This authority may not be delegated below the level of a principal deputy.

- (4) **Notification of Monitoring and Disclosure.** All components are required to provide adequate notice to their employees that their use of the departmental computer system constitutes consent to monitoring and disclosure. The Standard Warning Banner promulgated by the Department's Chief Information Officer provides such adequate notice.
- (5) **Employee Activities.** Nothing in this policy creates any enforceable rights; however,

USE AND MONITORING OF DOJ COMPUTERS AND COMPUTER SYSTEMS

unauthorized use or monitoring or improper access to an employee's computer system may result in disciplinary action or criminal prosecution. Employees are prohibited from accessing the e-mail, electronic files or documents, or otherwise monitoring the online activities of another employee except in accordance with this policy.

- g. **Sanctions for Misuse.** Unauthorized or improper use of Department office equipment could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, and/or criminal penalties.

/s/ Lee J. Lofthus
Assistant Attorney General
for Administration

Exhibit D
to Declaration of Jonathan Tukul dated July 31, 2009

UNITED STATES ATTORNEYS OFFICE

Justice Consolidated Office Network (JCON II)

Security Documentation: System Security Plan

April 21, 2000
Revised: June 14, 2000

LIMITED OFFICIAL USE



Table of Contents

1.	SYSTEM IDENTIFICATION	1
		1
1.A.	Responsible Organization	1
1.B.	System Name/Title	1
1.C.	System Category	1
1.D.	System Operational Status	1
1.E.	General Description/Purpose	1
1.F.	System Environment and Special Considerations	5
1.G.	Information Contact(s)	9
2.	Sensitivity of Information Handled	9
		9
2.A.	Applicable Laws or Regulations Affecting JCON II	9
2.B.	General Description of Information Sensitivity	9
2.C.	Information Handled by the System/Need for Protective Measures	10
2.C.1.	Confidentiality	10
2.C.2.	Integrity	11
2.C.3.	Availability	11
2.D.	Estimated Risk/Magnitude of Harm	12
3.	SYSTEM SECURITY MEASURES	13
		13
3.A.	Risk Assessment and Management	13
3.A.1	Risk Assessment and Management Methodology and Specialist	13
3.A.2.	Items Included in the Risk Analysis	13
3.A.3.	How Risks Were Determined for This System	13
3.B.	Applicable Guidance	14
3.C.	Security Control Measure Status - General Support Systems	15
3.C.1	Management Controls	15
3.C.2.	Acquisition/Development/Installation Controls	17
3.C.3.	Operational Controls	17
3.C.4.	Security Awareness and Training	27
3.C.5.	Technical Controls	27
3.C.6	Controls Over Application Security	29
4.	ADDITIONAL COMMENTS	30
		30
5.	COMPONENT MANAGEMENT INFORMATION	30
		30
5.A.	Plan Development and Review	30
5.A.1.	Plan Developed By	30
5.A.2.	Is System Covered in Component Automated Information Systems (AIS) Tactical Plan?	30
5.A.3.	Are There Any Internal Control Actions Required or Issues Pending	30
5.A.4.	Does Your Component Have Written ADP Security Policies,	30

Procedures, Standards, or Requirements?	31
5.A.5. Computer Systems Security Officer	31
5.A.6. Plan Reviewed and Approved by Component Management	31
APPENDIX A: Rules of Behavior	32
APPENDIX B: EOUSA Field Office Router Bandwidth Table	37
APPENDIX C: USAO Field Office Server Deployment Table	44
APPENDIX D: USAO Contact List	55

APPENDIX A: Rules of Behavior**Automated Information Systems Security Principles**

VIOLATION OF THESE RULES MAY
RESULT IN DISCIPLINARY ACTION

General Principles

The following principles of behavior apply to all EOUSA employees, and to personnel supplying IRM services and using EOUSA's information resources, e.g., contractors and volunteers. Because written guidance cannot cover every contingency, personnel are asked to go beyond the stated principles, using their best judgement and highest ethical standards to guide their actions. Personnel must understand that these principles are based on Federal laws, regulations and DOJ Orders. As such, there are consequences for non-compliance with principles of behavior. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include: suspension of access privileges, reprimand, suspension, demotion, removal, and criminal and civil penalties.

1. **Accountability:** Employees must be accountable for their actions and responsibilities related to information resources entrusted to them.
2. **Confidentiality:** Employees must protect sensitive information from disclosure to unauthorized individuals or groups.
3. **Passwords and User IDs:** Employees must protect information security through effective use of user IDs and passwords. Each system user will be assigned a unique personal identifier and password that shall be used to establish all personal accounts and access privileges for the individual. Protect your passwords!
4. **Hardware:** Employees must protect computer equipment from damage, abuse, and unauthorized use. This includes DOJ-owned hardware located at employees' place of residence and portable personal computers used for business while on travel.
5. **Reporting:** Employees must report security violations and vulnerabilities to their office's Computer Systems Security Officer (CSSO).
6. **Privileged Users:** Privileged users must perform their duties meticulously and reliably in order to preserve information security. Privileged users include: system administrators; computer operators; system engineers (those with control of the operating system); network administrators; those who have access to change control parameters for equipment and software; database administrators; those who control user passwords and access levels; and troubleshooters/system maintenance personnel.
7. **Work at Home And Other Remote Users:** Remote users must establish security standards at their workplace sufficient to protect hardware, software, and information. This includes having

only those resources you really need and have authority to use; establishing a thorough understanding and agreement with your supervisor as to what your security responsibilities are; using software according to licensing agreements; ensuring that sensitive information that is downloaded is properly safeguarded, and that dial-in access is secure; and being alert for anomalies and vulnerabilities, reporting these to their CSSO, and seeking advice when necessary.

8. **Users of Personal Information:** Users must acquire and use personal information only in ways that respect an individual's privacy. This includes: properly destroying personal information contained in hard copy or electronic format; and ensuring that personal information is accurate, timely, complete, and relevant for the purpose which it is collected, provided, and used.

Automated Information Systems Security Rules

These rules of behavior are based on the general principles of behavior.

1. Official Business

- a. Do not steal hardware, software, information, or equipment.
- b. Do not develop computer programs for non-work purposes.
- c. Limit use of the computer for non-work purposes to non-business hours.

[Justice Property Management Regulation (JPMR), 41 CFR pt 28 allows personal use of government equipment, as long as there is negligible cost to the department and it does not interfere with official business. Furthermore, the regulation goes on to state: "In using government property, employees should be mindful of their responsibilities to protect and conserve such property **and to use official time in an honest effort to perform official duties.**" (Emphasis added).

2. Access

- a. Only use data for which you have been granted authorization.
- b. Do not retrieve information from a system for someone who does not have authority to access the information. Only give information to people who have access authority and who need the information for their jobs.
- c. Abide by procedures governing the channels for requesting/disseminating information.
- d. Limit the number of people who can access your files/data.
- e. Do not access external computer systems (such as bulletin boards) unless necessary to perform an official duty.
- f. Do not attempt to gain access to information to which you do not have authority.
- g. Use access control features such as screen saver passwords and password protecting highly sensitive files.

3. Integrity

- a. Discontinue use of any PC or LAN system or software that show indications of being infected with a virus.
- b. Protect against viruses and similar malicious programs. Use only authorized software; do not use shareware, public domain software, or similar programs unless they are authorized.
- c. Never enter unauthorized, inaccurate, or false information.
- d. Do not manipulate information inappropriately.
- e. Create only authorized records or files.
- f. Avoid "data diddling."
- g. Scan all files and disks for viruses before use, especially if they are received from external sources.

4. Availability

- a. Plan for contingencies such as disaster, loss of information, and disclosure of information by preparing alternate work strategies and recovery mechanisms.
- b. Make backups of hard drive files on a regular basis.
- c. Write protect backups.
- d. Store backups away from the originals.
- e. Keep storage media away from devices that produce magnetic fields.
- f. Protect disks from food and drink spills.

5. Hardware/Software

- a. Safeguard computer equipment against waste, loss, abuse, unauthorized use, and misappropriation.
- b. Only use equipment for which you have been granted authorization.
- c. Do not eat, drink, or smoke near computer equipment and media.
- d. Do not store combustible materials near a computer.
- e. Do not remove a PC or other computer hardware from EOUSA premises without a property pass.
- f. Only remove computer equipment from EOUSA premises for official purposes.
- g. Do not allow someone to perform maintenance without proper identification.
- h. Only use software for which you have been granted authorization.
- i. Do not install unauthorized or public domain software without the approval of your systems administrator.

6. Reporting

Report all security violations, incidents, and vulnerabilities to your CSSO.

7. Privileged Users, e.g., Systems Administrators, Case Managers, Database Administrators, Systems Engineers, etc.

- a. Protect the supervisor or root password at highest level demanded by the sensitivity level of the system.
- b. Do not develop programs for non-work purposes.
- c. Help train users on appropriate use and security of system.
- d. Watch for unscheduled or unauthorized programs running on a recurring basis.
- e. Report all security incidents to the CSSO and the EOUSA's Security Programs Manager (SPM).
- f. Track all security incidents occurring within your area of responsibility.
- g. Take action to reduce damage caused by security incidents, as appropriate, e.g., lock up property, log off of a terminal, and disconnect a PC with a virus from the LAN.
- h. Establish a firewall or other means of protection, i.e., separate server, for all servers connected to publicly accessible networks.
- i. Establish security measures to ensure integrity, privacy, and availability of information on publicly accessible systems.
- j. Establish virus protection for servers that are publicly available.

8. Users of Public Access Systems, e.g., Internet, Court Systems, etc.

- a. Do not transmit Limited Official Use or other highly sensitive information across public access systems.
- b. Use virus protection software when receiving information from a public access system.
- c. Ensure that information placed on a public access system presents a professional image.
- d. Ensure that information placed on a public access system is up-to-date, accurate, and true.
- e. Ensure that information placed on a public access system reflects the policies and positions of the EOUSA and DOJ.
- f. Do not distribute or receive documents via public access systems in violation of copyright laws.

9. Managers

- a. Notify SPM whenever an employee terminates or changes status.
- b. Ensure continued availability of data when a employee terminates by assisting the CSSO with completing the *Departing Employees/Contractors/Volunteers EOUSA Automation Clearance Form* on the last day the departing individual is in the office.

- c. Counsel terminating employees on non-disclosure of confidentially-sensitive information.
- d. Request that the SPM or CSSO terminate access to information and computer systems immediately in the event of an unfriendly separation.
- e. Escort employee off the premises when there is likelihood of sabotage, as with an unfriendly termination or separation.
- f. Ensure employees get adequate and appropriate training to do their job.

Exhibit B

**to Jonathan Tukul's
Motion and Memorandum of Law to Intervene
to Assert Various Privileges in Response to
Plaintiff's Motion to Compel Production from
Defendant United States Department of Justice**

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

_____)	
RICHARD G. CONVERTINO)	
)	
Plaintiff,)	Civil Action No. 04-00236 (RCL)
)	
v.)	
)	
UNITED STATES DEPARTMENT OF JUSTICE,)	
<i>et al.</i>)	
)	
Defendants.)	
_____)	

NOTICE OF APPEARANCE

NOTICE IS HEREBY GIVEN that James K. Robinson of Cadwalader, Wickersham & Taft LLP, enters his appearance on behalf of Jonathan Tukel in the above-captioned action. All files, papers, and correspondence should be addressed to:

James K. Robinson
Cadwalader, Wickersham & Taft LLP
700 Sixth Street, N.W.
Washington, D.C. 20001
(202) 862-2494
(202) 862-2400 (facsimile)
jim.robinson@cwt.com

Respectfully submitted this 31st day of July, 2009.

/s/ James K. Robinson

James K. Robinson (D.C. Bar No. 446925)
Cadwalader, Wickersham & Taft LLP
700 Sixth Street, N.W.
Washington, D.C. 20001
(202) 862-2494
(202) 862-2400 (facsimile)
jim.robinson@cwt.com

Counsel for Jonathan Tukel