IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF COLUMBIA

NATIONAL SECURITY ARCHIVE,	)	
Plaintiff,	)	
v.	)	**Civil Action No. 07-1577 (HKK/JMF)**
EXECUTIVE OFFICE OF THE PRESIDENT, *et al.*,	)	**(Consolidated with Civil Action No. 07-1707 (HKK/JMF))**
Defendants.	)	

DECLARATION OF AL LAKHANI

I, Al Lakhani, declare as follows:

1. My name is Al Lakhani and I am a Managing Director at Alvarez & Marsal Dispute Analysis & Forensic Services, LLC ("A&M-DAF"). Within A&M-DAF I am the National Practice Leader for the Forensic Technology & Data Mining practice. I specialize in assisting clients with a variety of issues involving electronic discovery, computer forensics, and data mining.

2. I have practiced as a consultant for more than ten years. During my tenure I have led several investigation and litigation assignments involving large volumes of backup tapes, email and file archives, email and file servers, PC hard drives, a variety of external storage devices[1], and databases. I have assisted clients running a variety of email systems including Microsoft Exchange, Lotus Domino, and Novell Groupwise. I have developed and implemented electronic discovery methodologies as well as provided oversight and recommended improvements on existing electronic discovery methodologies.

3. I have been published and have been asked to speak on topics related to electronic discovery. I graduated from the University of Texas at Austin with a bachelor's degree in Management Science and Information Systems.

4. I submit this declaration on behalf of the plaintiff National Security Archive ("the Archive") pursuant to the Order of Magistrate Judge John M. Facciola dated March 18, 2008. The statements contained in this declaration are based on my personal knowledge and documents filed in this litigation[2].

---

[1] A variety of external storage devices including CDs, DVDs, thumb drives, floppy disks, zip disks, etc.

[2] EOP Defendants' Response to March 18, 2008 Order to Show Cause and attached Second Declaration of Theresa Payton [Docket # 64] (March 21, 2008)
Memorandum Order [Docket # 62](March 18, 2008)("Show Cause Order")
Opposition to National Security Archive's Emergency Motion to Extend TRO/Preservation Order and for Depositions [Docket # 60](March 14, 2008)
Emergency Motion to Extend TRO/Preservation Order and for Depositions, and accompanying Declaration of Sheila L. Shadmand and attached Exhibits 1-14 [Docket # 58] (March 11, 2008)
Response to Declaration of Theresa Payton [Docket # 50](March 17, 2008)
Notice of Filing, Declaration of Theresa Payton [Docket # 48](January 15, 2008)
Memorandum Order [Docket # 46] (January 8, 2008)
Reply to Motion to Expedite Service of Discovery Requests and to Compel Rule 26(f) Conference [Docket # 20] (November 21, 2007)

5. Ms. Payton states in her first declaration[3], "*Prior to October 2003 and continuing through 2005 and to the present, this office has regularly created back-up tapes for the EOP Network, which includes the system's email servers. Consistent with industry best practices relating to tape media management for disaster recovery back-up systems, these tapes were recycled prior to October 2003."* Based on this statement backup tapes created prior to October 2003 have been recycled and therefore user mailboxes, journal recipient mailboxes, and personal storage files ("PSTs") that were stored on these backup tapes have been destroyed.

6. Ms. Payton's further states, "*In October 2003, this office began preserving and storing all backup tapes and continues to do so. For that reason, emails sent or received in the 2003-2005 time period should be contained on existing back-up tapes.*" However, I do not believe that all emails sent or received between October 2003 and October 2005 could be preserved on backup tapes based on the information I have reviewed.

INCOMPLETE PRESERVATION OF EMAILS BETWEEN OCTOBER 2003 AND OCTOBER 2005

7. In his response to Chairman Waxman's interrogatories Mr. McDevitt states[4], "*The initial email retention process involved a manual process of copying messages from the*

Order [Docket # 18] (November 12, 2007)
Opposition to Motion to Expedite Service of Discovery Requests and to Compel Rule 26(f) Conference [Docket # 16] (November 9, 2007)
Motion to Expedite Service of Discovery Requests and to Compel Rule 26(f) Conference [Docket # 5 07-1577](October 26, 2007)
Objection to Report and Recommendation [Docket # 12] (October 23, 2007)
Report and Recommendation [Docket # 11] (October 19, 2007)

[3] Notice of Filing, Declaration of Theresa Payton [Docket # 48]

[4] Exhibit 8 to Declaration of Sheila L. Shadmand in Support of Emergency Motion to Extend TRO/Preservation Order and for Depositions [Docket # 58]

Exchange journals to .pst files for storage and retention." A monotonous manual process introduces human error. Therefore, without detailed email logs that match up the counts of emails in the journal recipient mailboxes with the total counts of emails in the various exported PST files, it is not possible to ensure that all emails sent or received between October 2003 and October 2005 have been successfully exported and therefore preserved.

8. In his response to Chairman Waxman's interrogatories Mr. McDevitt states, "*At some point, this process was partially automated using a utility designed for this purpose. The Mail Attender utility was used to automatically copy email message from the journals to the .pst files on a regular basis.*" Mail Attender is a product from the company Sherpa Software. I have used a similar product from Sherpa Software called Discovery Attender. Certain earlier versions of Discovery Attender contained bugs that often created empty and corrupted PST files. Given that both Mail Attender and Discovery Attender use the same framework called Microsoft Data Access Components ("MDAC"), it is highly likely that the same bugs that I faced in Discovery Attender could be prevalent in the earlier versions of Mail Attender. Furthermore, the information I have reviewed does not state when Mail Attender was first deployed or how it was used to "partially automate" the archiving of emails. Therefore, without detailed email logs that match up the counts of emails in the journal recipient mailboxes with the total counts of emails in the various exported PST files and the date of deployment for Mail Attender, it is not possible to ensure that all emails sent or received between October 2003 and October 2005 have been successfully exported and therefore preserved.

9. In his response to Chairman Waxman's interrogatories Mr. McDevitt states, "*In mid-2005, prior to the discovery of the potential email issues, a critical security issue was identified and corrected. During this period it was discovered that the file servers and the file directories used to store the retained email .pst files were accessible by everyone on the EOP network.*" This type of unrestricted and untraceable access to PST files creates the risk of entire deletion of PST files and/or modification of the emails within the PST files. Without knowing the extent to which any deletion or modification was performed to a PST file, it is not possible to ensure that all emails sent or received between October 2003 and October 2005 have been successfully preserved.

10. In his response to Chairman Waxman's interrogatories Mr. McDevitt states, "*The initial set of actions was simply to organize and inventory the .pst files used for EOP email records retention and to put in place a formal process to manage these files. The primary issue was the .pst files were scattered across various servers on the EOP network.*" Without a complete inventory of PST files created it is not possible to determine if certain PST files are missing from the various servers on the Executive Office of the President ("EOP") network. Therefore, it is not possible to ensure that all emails sent or received between October 2003 and October 2005 have been successfully preserved.

11. In his response to Chairman Waxman's interrogatories Mr. McDevitt states, "*I began to notice a few anomalies with these files. These included….inconsistent naming of files that made it difficult to determine the associated component and date to which the file was associated.*" A major drawback of inconsistent file naming is that more than one file with the same name could be created. When these files are copied from one location to another

manually it is highly likely that files with the same name are overwritten due to human error. Given that files could be accidentally overwritten it is not possible to ensure that all emails sent or received between October 2003 and October 2005 have been successfully preserved.

12. In the response to Chairman Waxman's interrogatories, Mr. McDevitt's states, "*If my recollection is correct, at that time there were over 5,000 .pst files with an average size of approximately 2 Gigabytes.*" A common limitation of an American National Standards Institute ("ANSI") based .PST file is that it has a maximum size limit of 1.937 GB. Therefore, if emails totaling more than 1.937 GB are copied into a PST file, the excess emails are lost. Unless there are programmatic or manual checks to ensure that emails totaling more than 1.937 GB are not copied into a PST file, it is not possible to ensure that all emails sent or received between October 2003 and October 2005 have been successfully preserved.

13. An EOP document made available to and made public by Chairman Waxman's Oversight Committee[5] includes a presentation slide with the heading, "*…to close exposures to risk.*" This presentation further states, "*Upgrade Exchange servers to Exchange 2003 (for "enveloping" capability).*" With Exchange 2003 and Exchange 2000 SP3, Microsoft introduced a new "envelope-level" capability as part of their journaling feature. However, based on this EOP document it is clear that this envelope-level journaling capability was not enabled on the EOP network; instead message-level journaling was enabled. Message-level journaling does not capture messages where recipients were blind carbon copied

[5] Exhibit 6 to Declaration of Sheila L. Shadmand in Support of Emergency Motion to Extend TRO/Preservation Order and for Depositions [Docket # 58]

(Bcc), recipients that received automated replies, and recipients whose emails were automatically forwarded. Additionally, message-level journaling does not capture the list of email addresses that received an email sent to distribution group[6]. Since envelope-level journaling was not enabled, it is not possible that all emails sent or received between October 2003 and October 2005 have been successfully captured.

14. Based on reasons provided regarding the loss of emails in paragraphs seven through 13 of this declaration, and the fact that Ms. Payton's Congressional testimony and two declarations do not address a resolution to the procedural and technical issues faced by this email archiving process, it is highly likely that emails sent or received between October 2003 and October 2005 have not been successfully preserved via the journaling and export to PST file processes.

FULL RECOVERY OF MISSING EMAILS

15. It is certain that without envelope-level journaling, emails where recipients were Bcc'd, emails with automatic reply and forward, and emails sent via distribution lists were not captured. Other emails that were initially captured but due to procedural and technical issues were lost, also need to be re-captured.

16. It is common practice for users to archive emails from their Exchange mailboxes to a separate PST file on their PC or an external storage device. Exchange users often use this "archiving" capability to manage the size of their Exchange mailbox.

[6] Distribution groups are created by companies to enable the mass emailing of information to certain pre-defined groups.

Organizations typically establish limits on the size of the user mailboxes and turn off delivery of email when these mailbox sizes are exceeded.

17. To the extent users have archived emails, including those received as a Bcc recipient, received based on an the automatic reply and forward, or received as part of a distribution list, it is possible that these emails could be recovered from the user's PC or external storage devices. Therefore, in order to capture all emails sent or received between October 2003 and October 2005, it is necessary to capture all PST files from the user PCs and/or external storage devices.

18. Ms. Payton states in her second declaration[7], "*When workstations are at the end of their lifecycle and retired from the EOP Network under the refresh program, the hard drives are generally sent offsite to another government entity for physical destruction in accordance with the Department of Defense guidelines.*" Hard drives from the retired workstations can contain recoverable PST files to the extent the hard drives have been warehoused and not destroyed. Therefore, if workstations and their hard drives were retired as a result of the termination of an employee, the hard drives should be retrieved and all PST files from these hard drives captured to ensure that all emails sent or received between October 2003 and October 2005 are captured.

19 An asset tracing system, which is often used by many organizations to keep track of their IT assets, can be used for the identification and recovery of hard drives that are warehoused as a result of the termination of the employee. Industry best practices

[7] EOP Defendants' Response to March 18, 2008 Order to Show Cause and attached Second Declaration of Theresa Payton [Docket # 64]

often include labeling warehoused workstations and/or hard drives with a barcode label to facilitate the tracking of the asset.

MANAGING COSTS DURING THE RECOVERY OF EMAILS

20. An EOP document made available to and made public by Chairman Waxman's Oversight Committee includes a presentation slide with the heading, "*This risk can be mitigated.*" This presentation further states, "*Update Mail Attender; Automated scheduling of the .pst creation and storage process; Better and consistent naming support; More reliable performance.*" In another EOP document labeled MEMORANDUM FOR JOHN STRAUB, Mr. McDevitt states under the FUNDING PROFILE sub-section, "*Mail Attender has been purchased.*" Both these statements indicate that Mail Attender has been purchased by the Office of Administration ("OA"). However, an updated version of Mail Attender needs to be procured in order to improve the PST file archiving process.

21. Mail Attender, as mentioned earlier, is a software product from the company Sherpa Software. In addition to the current role that Mail Attender fills with the OA, the latest version has the capability to silently and remotely crawl a user's PC and report the number of PST files and certain metadata about the emails contained in these PST files. Additionally, Mail Attender also has the capability to copy the emails contained in these PST files to a central location while maintaining the integrity of the email message. Since the OA already owns Mail Attender it is possible to create and automate a process by which emails from PST files stored on networked PCs are automatically located, inventoried, copied to a central location, and QC'd for accuracy.

22. Given the fact that the OA currently owns a version of Mail Attender, it is highly unlikely that the OA would have to buy a full version of Mail Attender for all their 3,000 customers. Instead, they might have to only purchase an upgrade for their current version of Mail Attender, which is typically significantly cheaper than having to purchase a full version. However, in the event the OA has to purchase a full version, the total cost of the software for 3,000 users should be approximately $25,000.

23. Retired hard drives (discussed in paragraph 18) and external storage devices such as USB drives, thumb drives, zip drives, writeable CDs and DVDs, etc. can change certain metadata when they are connected to a PC. Therefore, data from these devices should be collected using a forensic collection method. Depending on the type of data and the sensitivity of the collection, the following three paragraphs list the types of forensic collection methods that are available.

24. Forensic imaging creates a "bit-by-bit" copy of the entire retired hard drive or external storage device using specialized forensic software such as Guidance Software's EnCase and AccessData's FTK. This type of a forensic collection method allows the search of the unallocated space[8] as well as the recovery of any deleted files. The typical cost of forensic imaging a 100 GB hard drive is between $400 and $1,000 and it takes approximately two to three hours to complete the imaging. Imaging of smaller external storage devices can cost between $50 and $250 and take between 15 and 30 minutes.

---

[8] Unallocated space is space that is typically labeled "Free" by a PC's operating system. However, this space is often used by programs to write temporary user and system data. Deleted files are also part of unallocated space.

25. Forensic copying, which is different than forensic imaging, also uses forensic software such as EnCase and FTK, but instead of creating a bit-by-bit copy of the entire hard drive or external storage device, it loads the device in "preview" mode and enables the extraction of the necessary files. The typical cost of forensically copying PST files from a 100 GB hard drive is between $50 and $250. Copying of PST files from smaller external storage devices such as thumb drives, zip drives, etc. can cost between $50 and $250. Depending on the size of the PST it can take 15 to 30 minutes to copy the file from a hard drive or an external storage device. However, forensic copying does not capture unallocated space from the hard drive or the external storage device.

26. "Write-block copying" is one way to extract the files from a hard drive or external storage device without the use of forensic software such as EnCase and FTK. Write-block copying uses a hardware device that is attached to a hard drive or external storage device to "freeze" the device into a read-only mode. This enables the user to extract files without writing to the hard drive or external storage device. The cost of one write-block device is between $250 and $500. A write-block device can be used multiple times to extract PST files from hard drives or external storage devices. However, write-block copying does not capture unallocated space from the hard drive or the external storage device.

I declare under penalty of perjury, the foregoing to be true and correct to the best of my knowledge.

Executed the 25th day of March, 2008.

_____

Al Lakhani
Managing Director
Alvarez & Marsal Dispute Analysis & Forensic Services, LLC