BNA, INC.

DIGITAL DISCOVERY & E-EVIDENCE

BNA Employee-Owned Since 1947

VOL. 7, NO. 6 PAGES 93-114

REPORT

JUNE 1, 2007

HIGHLIGHTS

Admissibility Problems with ESI? Help Is at Hand

In dealing with admissibility issues and electronically stored information (ESI), do you ever feel like the prince with the glass slipper in ''Cinderella''? You know it should fit somehow but you can't really figure it out? A groundbreaking decision that explains how the Federal Rules of Evidence apply to ESI is analyzed by Kevin F. Brady of the Delaware office of Connolly Bove Lodge & Hutz LLP. **Page 96**

Evidence Rules Committee Approves New Fed. R. Evid. 502

The Advisory Committee on Evidence Rules approves a new Evidence Rule 502, ''Attorney Client Privilege and Work Product, Limitations on Waiver.'' The new rule is a partial response to complaints that reviewing electronically stored documents for privilege is becoming cost-prohibitive. **Page 99**

Number of E-Documents Complicates Decision on Congressional Privilege

A decision on whether documents seized from a congressional office are constitutionally protected from a search warrant is hampered by the time it is taking to review the documents produced, many of which are in electronic form. **Page 104**

Judge Uses E-mail Subject Lines in Privilege Determination

Sustaining the ruling of a magistrate judge, the U.S. District Court for the Eastern District of New York holds that two draft memorandums authored by the plaintiff in an employment action and then e-mailed as attachments from her work e-mail account to her private e-mail account are protected from discovery by virtue of the work-product privilege. **Page 105**

Apparent Consent Saves Search of Computer Not Checked for Passwords

The Fourth Amendment does not require police officers to inquire into whether computer files are protected by a password before relying on a person's apparent authority to consent to a search of the computer, according to a split U.S. Court of Appeals for the Tenth Circuit. **Page 105**

Tyco Receives Fine for Problems With Worker Database, Transfers

The French Data Protection Authority (CNIL) issues a €30,000 ($40,972) fine against a local subsidiary of U.S.-based medical equipment manufacturer Tyco Healthcare for improper storage and cross-border transfer of employee data. **Page 112**

ANALYSIS & PERSPECTIVE

UNDERSTANDING TECHNOLOGY: Aptara's John P. Collins explains why and how counsel should conduct a methodical review of the target organization's Microsoft Exchange/Outlook system. He discusses several technical elements of Exchange, in order to assist counsel with developing an effective plan for discovery involving this leading e-mail platform. **Page 100**

ALSO IN THE NEWS

SANCTIONS: Sanctions are imposed against a defendant, even though her non-party husband committed the actual spoliation at issue. **Page 107**

PRIVILEGE: Routinely labeling a particular class of documents ''privileged''—whether or not the label is warranted—strengthens the argument that a corporate defendant actually waived the privilege it sought to protect. **Page 106**

ETHICS OPINION: The unauthorized mining of metadata to uncover confidential information in electronic documents constitutes professional misconduct, according to the Alabama State Bar's ethics panel. **Page 109**

 ISSN 1537-5099

Industry Insight

UNDERSTANDING TECHNOLOGY

An Introduction to Discovery Involving Microsoft Exchange/Outlook

BY JOHN P. COLLINS

Microsoft[1] Exchange/Outlook[2], a popular e-mail messaging and collaboration platform, presents challenges to counsel seeking or defending discovery of e-mail and other items[3]. Counsel should conduct a methodical review of the target organization's Exchange system to develop a clear understanding of both the physical infrastructure and policies which shape how Exchange is used and managed. Generalizations about how Exchange works may be dangerous if applied to specific questions such as ''does a custodian have e-mail located somewhere other than the Exchange Server'' or, ''is a custodian's deleted e-mail captured on backup tapes?''

Developing a clear understanding of how an organization operates Exchange requires investigating the unique combination of policies, technical features, and user habits which vary from one organization to the next. Failing to understand fully how a client operates Exchange could result in failing to identify, preserve, and produce relevant evidence—leading to sanctions, adverse inferences, or other penalties. This article provides a general discussion of several technical elements of Exchange, in order to assist counsel with developing an effective plan for discovery involving this leading e-mail platform.

[1] This article is based on Microsoft Exchange Server 2003 and Outlook 2003. Some of the functions discussed in this article may not be applicable to other versions of Exchange and Outlook. The purpose of this article is to provide a starting point for discovery involving Exchange and Outlook.

[2] For brevity, this article will refer to the Microsoft Exchange/Outlook as ''Exchange'' unless otherwise noted.

[3] While e-mail is the focus of this article, all Exchange user data may be discoverable, including: calendar items; tasks; and contacts.

John P. Collins, J.D. is a discovery consultant with Aptara, a national provider of litigation support services. In this role, he works with law firms and corporate legal departments to develop defensible and cost effective approaches to electronic discovery. Collins has educated hundreds of attorneys and other legal professionals on fundamental technologies related to electronic discovery, and may be reached at john.collins@aptaracorp.com

Primary Elements of a Microsoft Exchange/Outlook E-mail System

The Server Component: Exchange Server. Exchange Server[4] is Exchange/Outlook's ''central nervous system,'' providing critical functions such as system administration, security, and message routing. Exchange Server also provides services to the Outlook client[5], including storage of e-mail and attachments, appointments, tasks, calendar items, and contacts.

From a discovery perspective the most significant aspect of Exchange Server is the Exchange Information Store (EIS), which processes and stores e-mail. The foundation of the EIS is the storage group, a system paradigm through which Exchange Server can support thousands of e-mail users in extended enterprises. Each EIS contains at least one storage group but may contain a maximum of five[6]. In turn, storage groups consist of two elements: a processing element and a storage element.

The processing element consists of the Extensible Storage Engine (ESE) and log files. Using log files[7], the ESE writes e-mail to the storage element (the private store which is discussed below). It's important to note that, in order to capture all of a custodian's Exchange Server based e-mail, it's necessary to collect e-mail residing in both the private store and log files; a collection not targeting both the private store and log files may omit some e-mail messages[8]. The storage element of a

[4] A server is a computer which provides services and functions to other computers (usually referred to as ''client'' computers).

[5] A client computer accesses shared resources and services from other (usually server) computers. Client computers are typically the desktop or laptop computers used by an organization's employees.

[6] One of the five storage groups is used only for recovery purposes.

[7] A key design paradigm of the ESE (and Exchange/Outlook) is ''fault tolerance,'' which is a computer programs ability to withstand the failure of one of its components. Exchange Server, as the backbone of a company's e-mail system, requires a high level of fault tolerance. To attain a high level of fault tolerance, ESE employs Log Files as a buffer to hold e-mails, prior to their being written (what Exchange calls committed) to the database. This design means a complete snapshot of a custodian's Mailbox must include both the contents of the .EDB/.STM files and the Log Files.

[8] ''Any uncommitted transaction log entries are also considered part of a current Exchange database. . .'' Technical Refer-

  DDEE ISSN 1537-5099

storage group consists of a private store (also called mailbox store) and a public store[9].

The private store contains each user's mailbox. The public store does not contain user mailboxes, but rather, contains shared folders serving as public ''filing cabinets,'' holding items (documents, spreadsheets, and presentations) intended to be shared among users. The private and public stores each contain a pair of files: .EDB and .STM[10]. The private store is the focus of discovery when individual user e-mail is sought.

The Client Component: Outlook and Outlook Web Access

In an Exchange environment, users access e-mail via client[11] software (Outlook), a web browser (Outlook Web Access), or both. Outlook and Outlook Web Access are the client interfaces most likely to be encountered in corporate environments. Another interface, Outlook Express, is encountered less frequently in corporate environments. Exchange Server also supports some non-Microsoft software clients, such as Netscape Messenger and Eudora Mail (non-Microsoft clients are not covered in this article).

Outlook[12], as client software, is installed on each user's computer. offers a variety of configurations which specify where e-mail resides: locally, (on the user's computer); on the Exchange Server; or, in both locations. Understanding how Outlook is configured is critical to framing discovery requests seeking e-mail, since where the e-mail resides will vary from one organization to another (indeed, from one user to another). Because Outlook has multiple configurations, determining how the organization has configured Outlook is critical to conducting effective discovery. Unless an organization completely ''locks down'' Outlook or has unlimited mailbox storage space, it is probably going to be necessary for discovering counsel to look for e-mail in multiple locations. This article discusses, in detail, these various configurations.

Outlook Web Access (OWA)[13] is a method for accessing e-mail without using client software, but rather, via a web browser. A user launches his/her web browser (such as Internet Explorer), enters a unique OWA address, logs-in, and is connected to the Exchange Server. Once connected, a user can: send and receive e-mail; create and access contacts; schedule appointments and tasks—most Outlook functions are available in OWA. However, unlike Outlook client software, OWA does not provide any mailbox access unless the user is connected to the Exchange Server.

Outlook Express, like Outlook, is client software installed on each user's computer. Outlook Express, however, is not a stripped down version of Outlook, but rather, an entirely different application[14]. Outlook Express is not widely used in corporate environments, largely because it lacks some of the functionality of Outlook, especially in the area of appointment scheduling and tasks[15]. This article does not address discovery involving Outlook Express; it is mentioned here to distinguish it from the Outlook client.

Where is E-mail Located?[16]

Due to the flexibility of Exchange, a multitude of storage locations, and the variability of user habits, e-mail may be found in obvious places such as the Exchange Server, and not so obvious places, such as the trunk of an IT Manager's 1993 Honda Civic. Following is a discussion regarding locations counsel should consider investigating when conducting discovery involving Exchange. The locations discussed are not exclusive; that is, e-mail may—and probably does—reside in more than just one of the locations discussed; it's possible counsel may encounter situations in which e-mail is located in all the locations discussed (and some not discussed).

As will become apparent, counsel should pay particular attention to custodian's use of .PST[17] files. Since .PST file creation by users is usually subject to little or no IT oversight, such files may be found in multiple locations and in multiple Exchange configurations. For example, users whose only mailbox is on the Exchange Server may still have one or more .PST files to which they've copied or moved e-mails from their Exchange Server mailbox. In the case of a ''move,'' the e-mail is removed from one repository (the Exchange mailbox) and placed in another (the .PST file). In the case of a

---

ence Guide for Exchange Server 2003 at http://technet.microsoft.com/en-us/library/bb124808.aspx

[9] Minimum of one each of the private and public stores in each storage group with a maximum of five stores possible. See http://technet.microsoft.com/en-us/library/bb125025.aspx for more information about the private and public stores.

[10] The .STM file has been removed from Exchange 2007 (Vista).

[11] Client software accesses services and data from another computer (typically a server.)

[12] A comprehensive list of Outlook versions is available at: http://en.wikipedia.org/wiki/Microsoft_Outlook.

[13] An interesting consideration regarding OWA is it provides user's access to their Exchange Mailbox from virtually anywhere—a home or personal computer, a public computer, or any internet enabled device with an internet connection and web browser. For example, consider an employee who, six months prior to leaving his job, starts stockpiling proprietary company data to use on behalf of a company recruiting him. One way to capture this proprietary company data is using OWA. The employee, using his home computer, could access his Mailbox via OWA and download proprietary company documents to his home computer hard drive.

[14] For example, while Outlook uses .PST files, .OST files, or Exchange based mailboxes, Outlook Express uses .DBX files to store e-mail (DBX files have a different technical structure than .PST, and .OST files).

[15] Outlook Express is usually provided at no charge on computers with a Windows operating system and Internet Explorer. Outlook Express is sometimes used by non-profits, government entities, and educational organizations where the absence of a licensing fee is attractive.

[16] This article excludes e-mail found in cellular devices, PDA's, Blackberry's, and other hand-held devices.

[17] A .PST file is an Outlook data storage file, typically, (but not always), created by an Outlook user to store e-mail subject to deletion from the user's Exchange mailbox. Many organizations impose mailbox limits on users; once their mailbox limit is reached, user's may no longer send or receive e-mail—thus prompting users to move e-mails to a location (.PST file) which is exempt from deletion. Outlook users may have multiple .PST files, and a key hallmark of .PST files is their somewhat random occurrence throughout an organization's IT infrastructure. An interesting note: there does not seem to be a consensus on what the acronym .PST actually stands for; some of the contenders include: personal store, personal information store, personal storage table, personal storage template, personal folder.

''copy,'' the e-mail is replicated (that is, a copy of the e-mail remains on the Exchange Server) and a second (or third, or fourth, or fifth copy) placed into one or more .PST files.

To guide discovery efforts, and minimize the risk of missing relevant e-mail, counsel should strive:

1. To understand how users interact with Exchange (essentially, their document management habits). There should be a special focus on how users employ .PST files specifically, and how they manage e-mail generally.

2. To understand how the company in question has configured Exchange/Outlook. Exchange/Outlook is an exceptionally flexible system offering dozens of different configuration options. Counsel operates at risk when making broad assumptions regarding how Exchange/Outlook stores data, and should strive to understand the specifics of how the targeted Exchange/Outlook is configured.

The following list of locations where e-mail may be found is provided to assist counsel with the challenging task of identifying all the locations where a custodian's e-mail may reside in an Exchange environment.

1. Exchange Server Mailbox. [18] Exchange may be configured so a user's mailbox resides solely on the Exchange Server. A user must be logged into the Exchange Server to access their mailbox; there is no ''local'' copy or replica of the user's mailbox. If this configuration is employed, users may still store e-mail locally, if they are permitted to create .PST files on their computer's hard drive[19]. User created .PST files often contain e-mail that has been moved or copied from the user's mailbox to the .PST file due to mailbox storage limits or retention policies. .PST files are discussed in more detail below.

2. Exchange Server Mailbox and User's Computer. In this configuration, users have two mailboxes: one on the Exchange Server (#1 above) and one on the user's computer[20]. This configuration is found in organizations providing users access to their mailbox while away from the office or in a disconnected mode (remote users). There are two options in this configuration: Offline mode and Cached Exchange Mode, explained below.

Offline mode. In Offline mode, users have a mailbox on the Exchange Server (in an .EDB file) and on their computer (in an .OST[21] file.) The user works from the mailbox located on their computer, and thus has access to their mailbox whether or not they are connected to the Exchange Server. New messages, contacts, appointments, etc. made by the user or received on the Exchange Server are synchronized between the two mailboxes[22]. To preserve and collect all of a user's e-mail requires targeting the contents of both the Exchange Server mailbox and the mailbox residing on the user's computer.

Cached Exchange Mode. Cached Exchange Mode is similar to Offline mode: users have two mailboxes and a synchronization process ensures changes to each mailbox are reflected in the other. The difference between Offline and Cached Exchange Mode is the synchronization process. In Cached Exchange Mode synchronization is automatic, versus user initiated in Offline mode. In Cached Exchange Mode, Outlook senses whether a connection is available with the Exchange Server. If a connection is available, Outlook operates in a connected state with the Exchange Server; if the connection to the Exchange Server drops, access to the local mailbox remains while Outlook continuously seeks re-connection with the Exchange Server. As in Offline mode, to preserve and collect all of a user's e-mail requires targeting the contents of both the Exchange mailbox and the mailbox residing on the user's computer.

3. PST file on User's Computer. An Exchange configuration infrequently used in corporate environments entails the direct transfer of e-mail from an Exchange Server mailbox to a .PST file on the user's computer. In this configuration, e-mail and other data passes through the Exchange Server, (copies of the data do not remain on the server), with a locally stored .PST file the user's mailbox. As in Offline and Cached Exchange Modes, to preserve and collect all of a user's e-mail at a moment in time requires targeting both the Exchange mailbox and the .PST file on the user's computer.

---

[18] Mailbox versus non-mailbox e-mail. In Exchange, users have a default mailbox which is where each user's e-mail is delivered. In most instances, the default mailbox resides on the Exchange Server. E-mail (and other Outlook data) may be copied or moved out of the user's default mailbox to other locations, (such as .PST files), which are not associated with a mailbox—thus constituting ''non-mailbox'' e-mail.

[19] It is important to note that users may save single or multiple e-mail messages outside of Exchange and or Outlook on their local computer (or elsewhere). Outlook permits users to save single messages as either text files or as .MSG files; groups of messages saved together may only be saved as a text file. For more information, see *Microsoft Office Outlook 2003 Inside Out*, Jim Boyce, Microsoft Press, 2004, Redmond, Washington, page 193.

[20] Exchange/Outlook may be configured to take advantage of ''Roaming Profiles.'' If Roaming Profiles is enabled, a user's non-Exchange Server mailbox (.PST or .OST file) may be stored on a centrally accessible network file share rather than the user's computer. Roaming Profiles enables users to access their Mailbox from multiple computers.

[21] An .OST file is, (similar to a .PST file), a data storage file. An .OST file is essentially a complete replica of an Outlook user's Exchange Server mailbox. The .OST file exists to provide users with access to their mailbox when in an offline mode. Offline mode refers to users who access Outlook when disconnected from the Exchange Server; the classic example of this would be an individual on an airplane who has no access to a data connection. .OST files are generally not user created; hence, there is little likelihood .OST files will proliferate throughout an organization's IT infrastructure like .PST files. Each active .OST file is, by definition, the replica of a user's Exchange mailbox—it is a one-to-one relationship (unlike .PST files which the vast majority of the time have no direct relationship with a user's Exchange mailbox).

[22] The Exchanger Server mailbox and the local (on a user's computer) will likely, due to the vagaries of synchronization, not be exact ''mirrors'' of one another. Rather, data may reside in one location (or both) which has not been synchronized; this dynamic should prompt counsel to target preservation and collection at target custodian's mailboxes on both the Exchange Server and user's computer.

  DDEE ISSN 1537-5099

4. Loose .PST Files. Loose .PSTs may be characterized as under-managed .PST files, created by users to save e-mail subject to deletion[23] or mailbox quotas (organizations employ deletion and mailbox quotas to control storage costs). Users, if permitted[24], may create .PSTs using a variety of methods, and often, with minimal restrictions or guidelines as to where these .PST files may be saved, how often they may be created, and how long they may be retained. As a result, .PST files are often scattered randomly throughout an organization's IT infrastructure, because each user may store .PST differently. Loose .PST files may be found in any location or on any media to which users may save files.

5. Backup Tapes. Many organizations now consider e-mail mission critical data requiring a comprehensive backup plan. An Exchange backup plan typically includes nightly replication of the organization's Exchange Server data (which includes e-mail) to backup tapes. Organizations generally do not backup desktop/laptop computers, which means e-mail residing on these computers (usually in .PST files) is not included in the organization's backup plan. Users, (fearing data loss) often save or copy .PST files to network file shares (or other storage locations) which are backed up. Generally—and there are exceptions—organizations do not have tools in place which monitor or track movement of .PST and other mail files throughout the organization's computer storage infrastructure. As a result, IT staff may not know the location or volume of .PST files existing on network file shares; counsel should carefully examine and probe assertions regarding the presence or absence of .PST files on storage media accessible to users. Also, counsel should probe each custodian's usage of .PST files. The objective is for counsel to have a clear picture of where .PST files are being stored, which facilitates understanding what backup media may contain relevant e-mail. The following framework is offered to assist counsel with discovery involving e-mail on backup tapes.

a. Tapes backing up the Exchange Server. Tapes used to backup an Exchange Server will contain the mailboxes of users on that Exchange Server. Thus, counsel should investigate the locations discussed above, and also, probe the organization's backup policies for their Exchange Servers, with a particular emphasis on the rotation and retention schedules for tapes, and which, (if any), tapes have been taken out of the tape rotation schedule. Another consideration is whether or not the organization engages in duplicating (vaulting[25]) tapes for disaster recovery purposes. Organizations using backup tapes for disaster recovery have additional challenges in managing the flow of tapes.

b. Tapes backing up other file servers and other storage media. As discussed earlier, organizations usually do not have tools that monitor or track movement of .PST files from a user's desktop/laptop computer to other storage locations; as a result, when user's copy .PST and other mail files to storage locations included in the organization's backup plan (network file shares), those .PST files are subsequently replicated onto backup tapes. IT staff may not even be aware .PST files exist on non-Exchange Server backup tapes. Without a systematic inventory of every server which is backed up to tape and contains .PST files, it is difficult for organizations to state with reasonable certainty they have identified, preserved, and collected all relevant e-mail.

6. Hard Copy/Printed E-mail. In some organizations, users may print out e-mails constituting business records to place into a paper filing system. Some organizations mandate printing out record e-mails, while other organizations have no such policy. In organizations without a policy requiring printing of e-mail, some users may nevertheless implement such a system on an individual basis. Regardless of whether printing e-mail is mandatory or discretionary, counsel should determine whether the company has processes and procedures in place to eradicate all electronic copies of printed e-mail. Counsel should also probe the application and enforcement of the organization's e-mail printing policies to determine the consistency of such polices. An inconsistent application of policies or haphazard enforcement should alert counsel to the need to carefully evaluate the organization's claims regarding the electronic version of e-mail supposedly deleted.

7. E-mail Archiving Systems. [26] E-mail archiving systems are specialized storage systems designed to help organizations manage the long term storage and retention of e-mail. Exchange Server is not optimized for long term mass storage, but rather, for efficient and reliable messaging. E-mail archiving platforms, on the other hand, are optimized for storage, and employ advanced compression and storage techniques which reduce storage costs and streamline (in theory) the management and retrieval of e-mail. Counsel should consider the following points:

- *Is the e-mail archive capturing e-mail for all mailboxes or a sub-set of mailboxes? (For example, senior executive's e-mail is archived but manufacturing workers is not).*
- *Is all e-mail archived or are there rules which select certain e-mails to be archived?(For example, any e-mail with the word ''stock'' in the subject or message text fields.)*
- *When was the e-mail archiving system put into service? Has pre-archive e-mail been migrated to the e-mail archive?*

This article has attempted to assist counsel in conducting effective discovery of e-mail and other data residing in Exchange. While Exchange is a complex system, its basic operating principles should—and can be—mastered by those conducting diligent discovery. Counsel, after attaining a reasonable level of familiarity with Exchange, can direct discovery based on the input and guidance of consultants and experts.

---

[23] Exchange's Mailbox Manager utility enables organizations to purge e-mail messages based on message age and or message size. For example, a policy could be set up which deletes all e-mail residing in a user's mailbox which is older than 90 days.

[24] Outlook can be configured so users are prevented from being able to create and open .PST files.

[25] Vaulting is the process of creating duplicate backup tapes, usually for disaster recovery purposes. One tape is kept locally while another tape is transported to a disaster recovery site (such as those maintained by Iron Mountain).

[26] E-mail archive platforms include: EMC EmailXtender; Symantec Enterprise Vault; Zantaz EAS.