



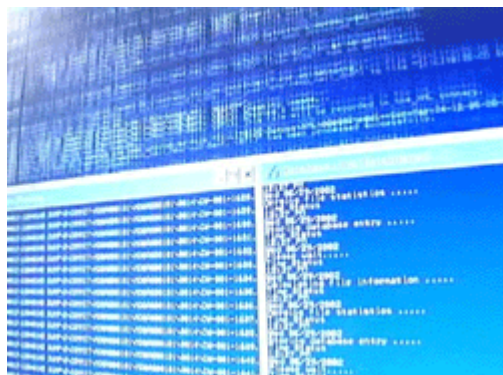
Litigation e-Newsletter



Examining E-Evidence

Steps to Creating Retention and Collection Policy

In 2002, American employees exchanged 2.8 billion e-mail messages¹. It is no wonder that electronic evidence has become a predominant topic of concern for both corporate executives and attorneys alike. The manner in which this data is located, prepared and reviewed can present a daunting challenge. With the penalties, severe sanctions and evidentiary misconduct actions being issued by more judges within recent months, it is imperative that corporate counsel and defense attorneys take a proactive stance when it comes to handling electronic data.



Retention Policy

Clients should be advised to create retention/destruction policies for all electronic data with a focus on business needs such as elimination of unnecessary and duplicative documents, protecting and preserving critical business documents, and maintaining efficient access to old correspondence.

An effective policy would also take into account key factors necessary to prepare the data for delivery upon request. For example, it would be prudent to create an electronic reference for all original documents including application files and e-mails. Make provisions in the system for review fields to accommodate the future examination of data by attorneys who may wish to categorize documents and create subsets according to author or subject. Another way to store the data would be to normalize it and convert each document into a

CLE PROGRAMS

Register now for
**Using Technology at
 Trial**
 on June 20th!
 Go to
www.DOAR.com/CLE2

Space is limited. Reserve
 your spot today!

Recent Topics

[A Day of Jury Research](#)

[Tips for Using Court Technology](#)

[Enron - Lessons in Document
 Management](#)

[Enron - A Practical Mental
 Exercise](#)

Contact

Paul Neale, VP/GM



PNeale@DOAR.com
 or by telephone at
 (516) 823-3997.

common format. This way, the information would be encapsulated to prevent unwanted alteration of data and stored so that all references to originating locations is preserved. Therefore, if a review is conducted, the appropriate data can be easily sorted and made available to opposing counsel.

Collection Policy

Knowing the appropriate actions to take and especially when to take them is critical in developing a collection policy that avoids potential sanctions due to an inability to provide data. There are several steps required in the process, including:

- **Notify Personnel**

The obligation to preserve any and all related information should be communicated throughout an organization. When the determination is made that a litigation or investigation matter is pending, every employee that may be affected by the imminent action should be made aware of the situation and educated on the type of information and subject matter that would potentially apply to the company's duty to preserve electronic documents under the applicable rules of evidence.

- **Map Environment**

Map out the important areas of operation and how they interact with each other. Critical systems will most definitely include centralized e-mail systems, database tracking systems for clients, products or institutional knowledge, accounting and financial systems, archival and disaster recovery. Don't overlook supporting systems; for example, fax servers sometimes save copies of all transmissions in and out of an organization, anti-virus applications allow logging of every file that passes through the network and other systems like proxy servers often retain Internet traffic and e-mail forwarding information. Aside from the central systems, get a sense of the user environments to determine if data can be stored locally, hosted on an ASP or even transferred off site for remote access.

- **Acquire Data**

Systems administrators, under the guidance of counsel, should create copies of relevant information that is stored on file servers. Typically, user's e-mail accounts are stored centrally and the creation of an exact portable copy should be a straight forward process. It may be necessary to invest in the services of a third party professional to be able to document and testify as to the collection process. When

preserving electronic files, it is important to remember that copying information for the purpose of creating data sets may inadvertently change the file system properties for those files. Special copy routines or archiving software should be utilized to ensure the authentication of these properties and attributes. Finally, special care should be taken in organizing and storing related data. The need for a clear labeling scheme, naming convention, storage location and documentation will allow for an easy transfer and preservation of the chain of custody.

In some circumstances, it may be necessary to forensically image data so that further investigation can take place, for example, if there is a possibility that information resides in the form of deleted files or fragments of temporary memory. In addition to creating images of user systems, it may be necessary to collect a full set of backup tapes for the network servers and to preserve tapes on an ongoing basis. This would be determined at the onset of the case due to the fact that the costs associated with such preservation methods often meet or even exceed the amount in dispute.

- **Process & Convert**

Before the data is prepared for review, every document will be accessed and vital metadata extracted. Each piece of information would then be saved in a central database for sorting, searching and use in the review process. After this database of information has been created, there are several options available that alleviate the burden of reviewing so many documents. The first and sometimes controversial option is de-duplication. This is the process of removing exact duplicates from a given population by first generating a unique identifier based on information going down to the bit level. The second option is to define a set of terms to be used as search criteria across the collection. This usually involves a consensus from all parties to ensure that the terms are not too narrow in scope. Once these terms are established, the universe of information to be reviewed can be significantly reduced.

Now that the data has been culled, de-duplicated and searched, it is converted into a single format, usually TIFF or PDF, to facilitate an efficient review. Conversion removes the need for native applications to be installed, avoids potential

problems with viruses embedded in the documents and keeps the file formatting intact. There may be some formats that will require the use of native applications for accurate representation of information such as database files, dynamically linked web pages or complex spreadsheets that reference data from many locations. Nevertheless, conversion should allow for the specification of formatting and pagination from the native application for commonly used business applications. Whether it pertains to revealing columns in spreadsheets or exposing the changes tracked in word processing documents, it is important to know that these settings may limit the amount of information displayed or extend the number of pages to considerable quantities.

- **Review the Documents**

After conversion, it is often the practice to inspect every document for privileged information, trade secrets or relevancy. One of the methods available for reviewing these converted documents is to print out the images to paper along with the metadata information of where the document came from or when it was created. Another method is to import the converted data into an in-house litigation support system. There are many popular applications available that allow for the import of a database filled with the information extracted during the conversion process in addition to linking each document record to a corresponding image. These systems allow attorneys to establish categories or classifications in which documents can be placed so after a review is completed, entire categories of documents can easily be accessed for further review or production. Lastly, all of the information as well as the images can be hosted on a secure web based repository. This eliminates the need for high end internal systems and allows multiple parties to access the same information from any place that has an Internet connection. In addition, these sites provide complex searching and retrieval, coding of information and the creation of production sets for purposes of print or delivery to opposing counsel. Think of it as a supply chain of information that can be accessed and shared by all members of the trial team and/or all outside counsel

- **Make the Production**

At this last stage of the process, given that one of the described methods was chosen for the review of all information, the creation of production sets

in any form is relatively straight forward. The data now exists in a structured environment with all documents referenced back to the original information. Attorneys can choose to produce in paper form, native file format or image format (TIFF or PDF). The entire process boils down to this last step with special care taken to ensure consistency, so that the creation and management of production sets can be straight forward and hassle free.

It is the fiduciary responsibility of corporate and outside counsel to arm themselves with the knowledge necessary to make educated decisions about the way in which electronic evidence is collected and produced.

1. National Law Journal (2/10/03).

[Go to top](#)

This document is provided for informational purposes only. The information contained in this document is provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and freedom from infringement. The user assumes the entire risk as to the accuracy and the use of this document.

(c)2003 DOAR - All Rights Reserved