Exhibit "D"

The Metropolitan
Corporate Counsel®

Times Are Changing - The World Of ESI

Linda G. Sharp and Joel J. Vogel
Kroll Ontrack

Linda G. Sharp, Esq., *MBA is a legal consultant for Kroll Ontrack Inc., a company specializing in electronic discovery, ESI consulting and computer forensics.* ***Joel J. Vogel*** *is the Director of Practice Support at Paul, Hastings, Janofsky & Walker LLP, a leading international law firm with over 1,200 attorneys in 18 offices.*

In the old days, plaintiffs would request business records from boxes in dusty warehouses. Attorneys would then review an inventory list of the boxes and pull those that were potentially relevant. Today, employees organize their own electronic data, but neither the records manager nor the IT representatives understand what each individual is really doing. This is the world of "electronically stored information" (ESI). The following article is designed to better equip you to evaluate your current environment and establish routine processes so that you are prepared the next time ESI is sought.

1) Be Proactive

Proactive steps are critical in preparing for electronic discovery. Looking at the types of documents you have and gaining an understanding of the various locations where data is stored will prove beneficial if and when litigation or a regulatory matter arises.

Step 1 - ESI Task Force

Establish an ESI task force comprised of members from the legal department, IT, records, outside counsel and an ESI vendor. This team should begin by comparing paper retention periods to that of electronic data. In addition, they should also familiarize themselves with the network environment and the appropriate locations to preserve and collect data when needed. The team should then focus on streamlining and minimizing the preservation and collection process, and removing personal and administrative garbage from business records.

Step 2 - Evaluation of Network Configuration

Create/Maintain a diagram of the network environment. This will assist in implementing preservation holds. When creating this diagram it is important to consider:

- Home computers - Do employees have information at home? Consider what happens to proprietary information if the employee donates or sells the computer, and what if the employee leaves the organization?
- VPN connections - Can employees use any computer (i.e. hotel business centers or homes) to access their files and email?
- PDA devices - Does the company provide PDA devices such as BlackBerrys or Trios? How is the data transmitted?
- Instant Messenger - Is Instant Messenger backed up?
- Laptops for departing employees - Are departing employees allowed to take their laptop? Allowing them to leave with computer equipment may subject you to explaining why you let them take the information and, later, trying to recover the computer to produce data. There may also be issues with claiming privilege or trade secrets if departing employees are allowed to maintain proprietary information. Furthermore, proprietary information may become broadcasted across the Internet if

the computer is improperly discarded.

Step 3 - Litigation Readiness Plan

The Task Force should know what their responsibilities are in locating and preserving relevant data. Delays may subject you to defending a spoliation claim.

Step 4 - Electronic Records Management

Is your electronic retention consistent with its paper counterpart? Many corporations have decided that "emails are not business records." When was the last time you actually received a paper memorandum or letter? Email, by nature of its use, is a business communication and thus may be subject to the same retention requirements as paper.

Step 5 - Service Provider Relationship

Reduce costs by establishing a relationship with a few valid ESI service providers. They will get to know your IT personnel and environment. This will reduce costs by utilizing economies of scale in negotiating services, and the number of meetings getting providers up to speed.

Step 6 - Outside Counsel Education

Confirm whether your outside counsel is qualified to handle ESI matters. What are their processes? Are they repeatable, defensible and cost effective? How many tiers of subcontractors are going to be used? Does your data require a security audit? Does the specific attorney have the technical acumen to argue and/or explain to a court your environment? Make sure that you fully understand how they plan to process and review your data.

2) Preservation

In general, under the FRCP, a duty to preserve ESI exists when litigation is imminent, anticipated, filed, pending, reasonably foreseeable or when required by statute, regulation or court order. You must move quickly. The faster the preservation notice is prepared and distributed, the less risk of a spoliation claim.

The ESI Task Force should have access to the following:

1. Current organizational charts

2. Document retention policies and schedules (electronic & hard copy)

3. Diagrams of network topology and infrastructure

4. Electronic disaster recovery policy

5. Hardware rotation information

6. Telecommuting policy

With a litigation readiness plan, the above documents and knowledge of the situation triggering the preservation event, you can quickly prepare the preservation notice, which should answer the following questions:

1. What is the nature/scope of the situation based on the triggering document?

2. Which department or divisions will be effected?

3. Who are the members?

4. How many sites in how many countries will be effected?

5. What are the possible devices/media on which the ESI must be preserved?

6. Who in IT is responsible for the management, backup and maintenance of those items?

7. Which document retention policies should be stayed?

8. What are the penalties of non-compliance?

9. Who should send the preservation notice?

Starting your preservation too narrowly then expanding it later increases the likelihood of a spoliation claim. The best practice is to create a sufficiently broad preservation to encompass all possible relevant evidence, then release groups of individuals or sets of documents and ESI as the facts unwind.

3) Collection vs. Preservation

The difference between collection and preservation is that preservation casts across the broadest group of

potentially relevant data while collection is a subset of what is preserved. When possible, it is important to negotiate with the other side to "collect" a sample for processing and review, and agree on what data can be released from preservation.

Collection is the most important phase of discovery. If improperly conducted, you may not be able to use the evidence. When collecting, corporations can save money by having their IT department do the collection. If this is possible, be sure your IT department has the time, understands the type of collection sought and is qualified to testify if needed because there are inherent risks with doing it yourself. Likewise, there are similar risks with having the firm collect for you.

It is also important to note that the destruction of metadata, the portion of the document that allows us to track when it was created, last accessed or last modified, can lead to spoliation sanctions. Therefore, when collecting, it is imperative to make sure metadata is preserved in its original state.

4) Processing

The collection of data comes from hard drives and servers, email, backup tapes, forensic images and much more. Processing is the step in which raw data is converted into easily useable information, so that each document can be managed throughout the project. Initially the files are separated so the metadata and text can be extracted from each document and a database created in which the fact finders can search for relevant documents.

To curtail costs, reduce the size of the raw data which must be processed to create useable information consider the following:

- Exclusion of file types, i.e. system files and programmatic files
- De-duplication of exact duplicates, preferably within a custodian
- Date range parameters
- Inclusionary or exclusionary filter terms
- Data sampling to assess anticipated volumes for negotiation.

Negotiation with the opposing party is advised to avoid costly discovery disputes, additional and/or double processing of data.

A decision regarding whether the post processed documents will be directly converted to TIFF image or native format for review, with a smaller sub-set converted to TIFFs will also need to be made. Most document reviews today are conducted via databases that support native review through an image viewer. This reduces the costs of converting all documents to TIFF to just those documents deemed responsive. For smaller document sets it may be more cost effective to merely TIFF. For larger document sets native file review is the trend. Think of the process as a funnel in which methods are applied to reduce the population from a large RAW data set to a smaller production set.

Some corporations and law firms are processing internally. This is something that should be carefully considered. The risks associated with incorrectly handling and processing data are great. That is not to say that with the right infrastructure, staffing, procedures and protocols this could not be done.

5) Review

Reviewing the post filtered/processed data is one of, if not, the most expensive part of the discovery process. There are different strategies that can be applied to reducing these costs.

The review format should not be taken lightly. In document review, time is money. If the format or system chosen for the review slows the process, money is wasted. Fortunately, the systems used for review have improved tremendously. There are now systems that assist in automating the review process through the use of knowledge management and quasi-artificial intelligence logarithms. In addition, the speed in which the documents or pages of documents are delivered to the reviewers has also greatly increased.

When evaluating a review tool, some time-saving criteria to consider include:

-

- the time delay between advancing to the next document
- the time delay between advancing to the next page
- the time delay between clicking on a review category flag and the next flag
- the time required to run a single term search across 500,000 records.

Lastly, where the data will be hosted for review is important. Because of the large volume of documents and ESI, the trend is to host the data with a vendor. For the corporation, this represents a cost savings in overhead because creating a separate technical environment and adding staff to support the users of this system is expensive. In addition, corporations see an indirect cost savings because law firms do not need to increase their staffing or charge for dedicated servers.

6) Production

The production of ESI has become more complex since the days of copying and Bates stamping. Currently, the debate about production is whether it must be in native format or in image format, such as TIFF. The pages of a native document cannot be individually Bates stamped for control, redacted for privacy or branded with a confidentiality legend. Furthermore, with a native document, only the Bates number and confidentiality legend can be appended to the name of the file. This does not guarantee it will be included on the hard copy when printed. Opening a native document could change the document's metadata, which could result in potential authentication disputes. However, the native file is how the document is kept in the ordinary course of business and makes the creation of a fully searchable database easier. This is not to say that certain ESI formats may need to be produced in their native format to produce all the relevant information; however, those should be the exceptions to the rule, not the rule.

The FRCP state that if the format is not specified in the request or otherwise agreed, the responding party must produce the documents in the format originally maintained OR in a format that is reasonably useable. TIFF format, with an associated load file, is reasonably useable and allows for the petrifaction of the document prior to production as well as the application of redactions, confidentiality legends and Bates number overlays.

In negotiating the production format during the initial case management meeting, a good practice is to offer TIFF format with an associated load file, reserving the right to request specified documents in native later. This allows for a useable form of the document that can be tracked as well as a mechanism for searching the content of the document. If for example, the formulas in certain spreadsheets are relevant, then allowing for a secondary production of specified documents in native is reasonable.

The world is ever changing. As businesses embrace new technology, we must better prepare for how this affects litigation practices.

Please email the authors at lsharp@krollontrack.com or joelvogel@paulhastings.com with questions about this article.