PRACTICAL TIPS ON THE DISCOVERY OF ELECTRONICALLY STORED INFORMATION

May 9, 2014

Practices & Industries

Business Litigation

Case law continues to evolve on amendments to the Federal Rules of Civil Procedure that became effective in December of 2006. These amendments stated that parties are required to place a litigation hold on all documents and records relevant to a dispute, including electronically stored information, upon a reasonable expectation that a formal lawsuit will follow. With careful planning, parties can effectively address a number of recurring issues that have resulted from these amendments.

Attorney-client communications and confidential documents

In most cases and prior to advent of electronically stored information (ESI), counsel to the parties reviewed hard copy responsive documents for privilege and trade secrets. Once identified, the offering party would create a privilege log and segregate the documents in the event of a challenge and to avoid inadvertent production. Documents containing trade secrets or highly confidential information were typically addressed in a negotiated protective order. This order would specifically identify who could see the documents, how the documents would be handled in motion practice and at trial, and under what circumstances the documents could be used.

With the generation of literally millions of e-mails each day, individual review for privilege and confidentiality is extraordinarily difficult—if not impossible—in most cases. The number of e-mails exchanged in a signal day exceeds the total number of pieces of mail handled by the United States Postal Service—one can only imagine the volume, scope, and diversity of information electronically stored and exchanged by potential litigants. And this does not even consider the volume of electronic documents that may reside on separate servers, laptops, hard drives, or other storage devices.

As a result of the proliferation of electronic information, many parties have entered into claw-back agreements. These agreements ameliorate part of the risk of inadvertent disclosure of privileged or confidential records. They provide that receiving parties immediately return and erase any document that is recognized as privileged. Additionally, the privileged document is not to be used by the receiving party.

Confidential documents have been handled in a similar way. Parties have attempted to perform word searches in advance of production to identify privileged and confidential records with the hope and expectation that most critical documents can be identified. In some very serious cases, old fashioned e-mail reviews have been undertaken by teams of paralegals, case assistants, associates, and contract personnel at a substantial cost.

Parties can take a number of simple steps in advance to help solve the privilege and confidential disclosure problems recounted above:

• **Include "privileged" or "confidential" in the subject line of an e-mail**. This enables a quick, easy, and comprehensive search that can be done using the
metadata describing the e-mail contents. Because of the way searches are done, these words must be in the subject line, not within the body or conclusion of the e-mail. In-house counsel, in particular, should routinely include a designation like this one in the e-mail subject line, and they should encourage all others who may
initiate e-mail correspondence with counsel to do the same.

• **Consider a separate server**. This may be the answer for companies or entities with more robust and larger legal departments. If configured correctly, privileged
correspondence, documents, or attorney work product can be identified quickly and efficiently on the separate server. Generally, information on the special legal
department server will also generally make it easier to identify privileged documents that also may reside on the company's main server. Backup tapes and legacy
data Backup data generally refers to the disaster recovery snapshots taken of the system data on a regular basis. It allows a company to salvage data on its system
that existed at the time the snapshot was taken and is used in the event of a catastrophe. While not perfect, backup tapes allow an entity to remain in business and to
reconfigure its system after a disaster. Backup data is typically not stored in easily searchable form as it is kept strictly for purposes of catastrophic or unforeseen
events.

Back-up tapes can be created and kept for any period of time.

Some companies keep three months of data, some six, and some more. Backup tapes are typically put in a rotation because of their expensive cost; as such, the oldest data is replaced with the newest data on a regular schedule. After tapes are backed up, they are generally stored somewhere in the IT department for easy rotation.

Legacy data refers to historic data of the company that may have been produced or stored using an old computer system or software. It can be stored in many forms and usually resides in the IT department. It is often stored with other files, papers, or computer equipment.

Both legacy data and back-up tapes can cause substantial electronic discovery problems. Like the privileged document case

recounted above, there are steps parties can take to help solve these problems:

• **Delete legacy data that is not needed**. Legacy data typically cannot be read, searched, or manipulated; often, companies do not even know the contents of their
legacy data. Therefore, if the data is not required to be kept by statue or regulation, or if it is old and merely taking up space in an IT room, destroy it. Do not fall into
the trap of the client who had 187 unlabeled legacy data tapes and did not know what software was needed to access the information or what information was stored
on them. This only encourages electronic discovery mischief.

• **Segregate backup tapes for a particular time period if litigation ensues**. Once tapes are segregated, send them to a secure place—do not keep them in the IT department or at someone's desk. Options include sending the tapes to counsel for safe-keeping, storing the tapes in a secure vault in the company's executive offices with appropriate descriptive labels, or committing them to a forensic custodian for later retrieval.