

E-DISCOVERY MADE EASY AND COST-EFFECTIVE FOR THE SMALL “ROUTINE” CASE



BY SUSAN ARDISSON, ESQ.
bit-x-bit, LLC

Electronic discovery does not need to be daunting for counsel or expensive for the client. Consider a typical breach of contract claim where the key issues in the case are whether a supplier delivered the quality of goods contracted for under the agreement, and whether the parties agreed to an amendment to the original agreement to allow the supplier to provide substitute materials. The supplier claims that

the parties exchanged various emails last fall which will establish that substituted materials were agreed to under certain circumstances.

The likely repositories of electronically stored information include the following: the contract documents (prepared in Microsoft Word), Excel spreadsheets and email maintained by the client in Microsoft Outlook. There are no issues relating to document metadata or file system metadata. Both parties have communicated with their respective counsel by email concerning issues in the case raising questions of privileged material. What are the next steps?

1. Collection and Preservation: The first issue to consider is how should the ESI be collected and preserved? With smaller cases, involving a limited number of employees and a limited number of potentially relevant documents, collection by the client can be an easy and cost-effective solution. There are several things to consider in client collection: properly document the collection process, including who conducted the collection, the identity of the computer and email systems, the identity of employee-custodians; and create a proper chain of custody, including relevant dates and times, so that the electronic documents can be properly authenticated for use in a deposition or at trial.

To collect and preserve Word and Excel documents, make a copy of the relevant files to a “read only” media such as CD-R or DVD-R. To collect the relevant email, copy them to .MSG format² in Outlook which will preserve the recipient list, relevant dates, message body and attachments. To eliminate irrelevant email, consider “date filtering” so that only the email from the relevant time period is copied. If the client elects to have a vendor do the collection and preservation, then be sure to explain the “scope” of the anticipated discovery, so that unnecessary electronic data is not collected, complicating an otherwise straightforward document review for the contract case.

2. Make a “Working” Copy: Once the original evidence has been collected and preserved, the next step in the process is to make working copies of all of the collected evidence, and to secure the originals. Quite simply, never work with the original. Documents can be changed inadvertently, deleted and, of course, in cases where metadata is important, the metadata can be altered. Instruct the client to refrain from opening and reviewing potentially relevant documents and email until they have been copied and preserved.

3. Attorney Review: Once the electronic documents have been preserved, the next step is to review them for relevance and privilege. Since the email, Word and Excel documents have been collected in their native format,³ they may be reviewed using the software applications for Word, Excel and Outlook that most lawyers have available to them in their office. The documents may be “coded” for issues, privilege, and relevance by using a spreadsheet log listing the documents’ file name and providing check boxes for designated categories. Many firms, however, are investing in stand-alone electronic discovery review and production software, such as CaseLogistix or Concordance recognizing the necessity for in-house capability. Another alternative is to use a “hosted solution” on a case-by-case basis to conduct review and production. More often hosted solutions are used in

complex cases involving large repositories of documents, multiple parties and multiple law firms needing access to a common set of electronic data.

4. Production of Electronic Documents: Once the review is complete, and the relevant documents are identified, make a copy of the relevant documents onto a read only CD-R or DVD-R which will preserve the documents in a read only state. Producing the documents in native format will eliminate any expense associated with “tiffing” or making paper copies of the documents. Be sure to make at least two copies of the production CD-R/DVD-R; one to provide to opposing counsel and one for a record of the production. ■

About the Author: Susan Ardisson is the CEO of bit-x-bit, LLC, a computer forensic and e-discovery consulting firm in Pittsburgh. Since 2008, bit-x-bit, has been the Allegheny County Bar Association’s exclusively endorsed provider of computer forensic and e-discovery consulting services to the ACBA’s members. For more information about bit-x-bit, please visit www.bit-x-bit.com.

¹ If document or file system metadata is important in the case, and the parties agree that it should be preserved, then proper collection requires that special procedures and software be used to insure that all relevant metadata is preserved. In such instances, the client may not have the proper tools for collection and preservation, and referral to a company with this expertise would be necessary.

² “MSG” is the generic format in which email can be saved.

³ “Electronic documents have an associated file structure defined by the original creating application. This file structure is referred to as the ‘native format’ of the document.” *The Sedona Conference Glossary (Second Edition)*

(Re-printed with permission of the Pittsburgh Legal Administrators Association (PLAA) originally appearing in the April/May/June 2010 Issue of “To the Point”)