

Digital Discovery & e-Evidence

BEST PRACTICES & EVOLVING LAW



<http://ddee.pf.com>

Reprinted from Vol. 6, No. 9 | September 2006

TALKING TECH

No One Likes Surprises In E-discovery Projects . . .

And Quality Assurance and Strategic Planning Can Reduce Their Number

By Dana J. Lesemann and Jessica Reust

The latest surprise in the world of electronic discovery has been the “discovery” of a software bug that causes the body of certain e-mail messages to appear blank. The problem occurs if e-mails created with Microsoft Outlook are opened using an un-patched version of Microsoft Outlook 2003.

This is not a new bug; a patch has been available from Microsoft since January 7, 2004. However, recent media coverage has revealed that some vendors may not have installed this patch. The potential impact that this may have on pending litigation is creating anxiety among lawyers, who are contacting vendors seeking assurances that this issue did not affect any of their electronic production.

Counsel share horror stories about electronic discovery projects run amok to make themselves feel lucky that it did not happen to them. Yet, counsel confronting electronic data discovery projects need to rely on more than just luck to avert an electronic discovery project disaster. Establishing and implementing an electronic discovery strategy at the outset that incorporates the necessary level of quality assurance can greatly increase the efficiency, accuracy and smooth progression of the project.

The recent media coverage of the Outlook bug highlights the fact that electronic data processing and searching is not a one-dimensional, purely technical process, nor should it be taken lightly. Productions that are found to be incomplete or inaccurate can create significant liability problems for the responsive party and drive up the cost of production. Processing data on systems that are patched and up-to-date is a necessary but not sufficient step to take to ensure that the data processed and produced are accurate and complete.

Managing an e-discovery project is not a simple task and, in some cases, it may be prudent to use outside digital forensic experts at the beginning of the process to provide assistance with strategic planning, vendor management, and implementation of the discovery process. Electronic discovery questions quickly become forensic issues: who authored the document? Was it altered? By whom? When?

Gone are the days of WhiteOut and erasers. These are the days when digital forensic examiners are called upon to determine whether bits and bytes have been changed to violate litigation holds issued in the name of Sarbanes-Oxley.

The Role of Forensic Firms

Independent forensic firms can also provide assistance with electronic discovery strategy, independent quality assurance, vendor management, and implementation of the electronic data processing and searching. They can manage the electronic discovery process and perform quality checks on processing protocols and methods, and deliverables of e-discovery vendors. Forensic firms can also ensure that a consistent standard and level of quality assurance is being applied across all aspects of the e-discovery project.

Quality assurance begins with strategic planning at the outset of an electronic discovery project and continues with incorporating the requisite checks and balances throughout the electronic discovery process. Successful quality assurance builds on itself; each part of the process relies on the quality assurance of the previous part to ensure the accuracy of the incoming data.

Phase One

For example, the first general phase of electronic discovery is the identification, collection and processing of data for review by counsel. This is a critical part of the process because at this point counsel must make key decisions that will not only affect the data available for review and production at the end of the process, but also affect a party's ability to mine the data for answers.

However, in many ways lawyers will be making these decisions while blindfolded because the importance of the data available may become clear only much later, sometimes after discovery has closed. There are a number of other hazards involved in this early phase, each of which can result in civil or even criminal sanctions.

Controlling Costs

The most cost-effective solution for preserving, harvesting and producing the necessary data will depend on the scope and requirements of the project, and should be evaluated on a case-by-case basis. When collecting data for electronic discovery, counsel should gather information about the company's underlying systems and their use to ensure that all of the relevant sources of information have been identified and preserved. Failure to meet the requirements of a preservation order can create significant liabilities; some of the items overlooked include backups, home computers, e-mail archives in home directories, and decommissioned computers.

An additional question that arises is whether to create full physical images or logical copies of digital evidence. Full physical preservation of electronic data involves the creation of an exact image of the data, ensuring that active and deleted files, metadata, and critical contextual information about the system usage are preserved. This method will preserve the ability to go back and analyze the media to answer questions, including questions involving spoliation and obstruction.

A logical copy, on the other hand, will preserve only the targeted active files and will limit the amount of forensic analysis that can be performed. However, in some circumstances, such as when preserving large systems like email or database servers, the logistics of creating a full physical image can be prohibitive. Especially in situations where only a small amount of data from each system is relevant to the case, the more effective, cost-efficient and less disruptive method will be to create a logical copy.

Role of Counsel

Once the data has been identified and preserved, the information is harvested and processed for counsel's review and production. This process can involve multiple vendors and tools, depending on the variety of data types and required output. Using an outside vendor to manage the process will often enable counsel to work more efficiently and knowledgeably. Together they can design

a protocol that identifies the tools that will be used, the keywords that will be searched for, ascertain whether deduplication is necessary, and select the procedures that will be followed.

If protocols are poorly designed and filtering techniques are not vetted, counsel can end up receiving thousands of unresponsive documents. Conversely, that same lack of quality assurance can result in counsel failing to produce all responsive materials to the opposing party. Erroneous conversion, interpretation, and adjustments of time zones can produce data with incorrect dates and times. In addition, designing a protocol at the start of the harvesting and processing results in a more organized project and also manages the expectations of the parties involved.

The quality assurance steps undertaken in electronic discovery projects should identify problems in processes created by both technology and human errors. For the technical processes, the reality is that there will always be bugs in software programs and these bugs will vary in complexity and importance. It is vital to verify, test and document the strengths and weaknesses of a tool before using it, and apply approved patches on a timely basis. However, it is not realistic to expect a tool to be completely error free, nor is it always possible to identify and fix the errors before an e-discovery project has been started. Thus, it is essential to have a thorough understanding of the data before the processing has begun, as well as a quality assurance program for the process and the processing results in order to ensure an accurate and complete product.

Without technology, discovery would be back in the paper age. But attorneys must not forget that technology is a means to an end and not an end unto itself. To use technology successfully, attorneys must implement an electronic discovery strategy that incorporates the necessary level of quality assurance, which will greatly increase the efficiency and accuracy of a project – and lead to fewer surprises along the way.

Ms. Lesemann is Vice President and Deputy General Counsel of Stroz Friedberg, LLC, a technical services and consulting firm specializing in digital forensics, electronic discovery and cyber-security investigations. Ms. Reust is a digital forensic examiner and investigator at the firm.