

IF YOU HAVE QUESTIONS REGARDING THIS MATTER, PLEASE CONTACT:



STEPHEN A. ROBERTS
Partner, Austin
600 Congress, Suite 1600
Austin, Texas 78701
512.499.3624
stephen.roberts@strasburger.com

EDITORS

Kathryn Midboe Darling
Brian G. Hamilton
Laura Reilly O'Hara

HEALTHCARE GROUP

Tejal P. Banker
Debra W. Biehle
Thomas W. Burton
Renee Chafitz
Merritt M. Clements
Joseph F. Coniglio
Kathryn Midboe Darling
William Duane Darling
Rebecca L. Davis
R. Bradley Fletcher*
Brian G. Hamilton
John R. Lowry
Bryan J. Maedgen
Cynthia Schafer Marietta
Stuart Miller
David G. Moore
Craig H. Myers
C. Scott Nichols
Laura Reilly O'Hara
Jeffrey S. Osgood
David L. Ovard
Donald Patrick Owens
Paul W. Sheldon
Joseph A. Turano
Melissa Webb
Carol D. Williamson
Ivan Wood
Kevin M. Wood

*Not licensed to practice in the state of Texas

IN A NUTSHELL: THE PRACTICAL IMPACT OF THE NEW FEDERAL EDISCOVERY RULES ON LITIGANTS

Many of you have been inundated with seminars, webinars and vendors' pitches on the new "eDiscovery" Federal Rules of Civil Procedures which often cause more bewilderment than enlightenment. Let me boil it down for you.

WHY YOU NEED TO PAY ATTENTION

In the past few years, there have been numerous high profile cases where parties have suffered severe sanctions for failing to actively preserve "electronically stored information," or "ESI." The Sarbanes Oxley Act of 2002 criminalizes the knowing alteration, destruction or falsification of any record with the intent to impede the administration or investigation of a federal agency. The new Federal "eDiscovery" Rules of Civil Procedure go into effect on December 1, 2006. In the Texas state courts, the often overlooked eDiscovery rules in the Texas Rules of Civil Procedure will likely be the new weapons of choice for tech-savvy parties intent on setting up their less sophisticated opponents on charges of intentional spoliation of electronic evidence.

The confluence of these developments mandates a new approach to litigation which will require an *immediate, active and thorough* effort to identify, locate and preserve ESI when litigation or an investigation can be reasonably anticipated. Parties who ignore this fundamental shift, do so at their own peril. Ignorance of technology is no longer an acceptable excuse. Technological sophistication is increasingly presumed by the courts and is required under the new rules.

As we know, electronic documents, unlike paper documents, cannot be found in a specific file cabinet but are scattered throughout a computer system on servers, desktops, notebooks, personal digital assistants, telephones, personal email accounts and other remote places. Unlike paper documents, ESI is often altered, modified or destroyed through the normal operations of a computer system unless a party affirmatively acts to stop the destruction. Moreover, ESI still exists in bits and pieces scattered throughout the system even after it has been deleted and overwritten.

Moreover, the preservation of the electronic documents themselves is not always enough to avoid sanctions; the preservation of metadata is mandated when it is relevant. Metadata can provide information to ascertain the authenticity of the documents, who modified the document and when, how and where the document was accessed, and a wide variety of other information.

IN A NUTSHELL, THIS IS WHAT LITIGANTS NEED TO KNOW:¹

YOU MUST IMPLEMENT AN EFFECTIVE LITIGATION HOLD. When you reasonably anticipate litigation or a government investigation, you have a duty to put an effective “litigation hold” on any relevant ESI so it will not be materially altered or destroyed. Sending a letter to employees advising them to save relevant information is not enough. You must determine what to save, and how to save it, and you must give specific instructions to key players to prevent their accidental destruction of evidence. You must determine whether to have images or clones made of critical hard drives to preserve evidence in its pristine form, or to capture the “active” data but not the “deleted” data by ghosting the hard drive, or to allow the alteration of metadata (such as “last date accessed” or even “date created”) by allowing the transfer of the data files to other folders for future production. Some courts go so far as to put the responsibility on outside litigation counsel to educate their clients and to oversee the preservation effort. Other courts impose a continuing duty to see that the preservation efforts remain in place. In any event, the implementation of a litigation hold requires the active participation of the legal department, management, and IT personnel.

YOU SHOULD IMMEDIATELY CRAFT AND SEND A PRESERVATION LETTER. When you intend to file a lawsuit or when you receive a lawsuit filed against you, you should send a carefully crafted preservation letter to your opponent educating them on their affirmative duty to locate and preserve ESI relevant to the case. This will either cause them to preserve evidence that may otherwise be lost by the routine use of computers or document destruction policies or it may serve to deprive them of the ability to plead ignorance if they fail to heed your warning and allow the spoliation of evidence. Be careful; if your demands are too onerous, you may find a mirror preservation demand in the return mail and the costs of litigation can escalate rapidly.

YOU MUST CONFER WITH THE OPPOSITION AS SOON AS PRACTICABLE TO ADDRESS ESI ISSUES. You must quickly get a handle on what ESI in your possession or control may be relevant, where your own ESI is stored, whether the metadata is relevant and must be preserved, and the format in which you prefer to produce the ESI in the particular litigation at issue. At the same time you must quickly determine what demands you are going to make on your opponent regarding preservation, production, and the format in which you want the ESI produced (paper, images, native applications, etc.). Why? Because new Federal Rule of Civil Procedure 26(f) requires the parties to confer “as soon as practicable” and at least 21 days before the court’s initial scheduling conference to discuss (among other things) issues relating to preserving discoverable information and developing a discovery plan addressing “...any issues relating to disclosure or discovery of electronically stored information, *including the form or forms in which it should be produced*”; and any issues relating to claims of privilege or protection of trial preparation materials. The risk of inadvertent disclosure of privileged information is heightened where large volumes of ESI are involved and so parties may want to agree on the ground rules for protection of inadvertently disclosed privileged information (although some attorneys counsel against this). If you have focused on your preservation obligations and crafted an

¹ Disclaimer: The new Federal Rules of Civil Procedure and Official Comments are over 60 pages long and the cases and commentators addressing eDiscovery issues cover thousands of pages; therefore, although I attempt to touch on the most important issues, you should seek specific legal advice before acting.

appropriate preservation letter to the opposition as discussed above, then you may have created an effective road map for the 26(f) conference. If you are tempted to ignore your duty to meet and confer, beware, the court may set the rules for you. Rule 26(b)(5) and (b)(6). In light of the potentially enormous cost and complications involved in preserving and producing gigabytes or terabytes of data, do you trust the judge to get it right?

YOU MUST DISCLOSE THE DESCRIPTION OF ALL ESI TO YOUR OPPONENT IN YOUR INITIAL DISCLOSURES WITHOUT WAITING FOR A DISCOVERY REQUEST. More specifically, Rule 26(a)(1)(B) requires that a party in its initial disclosure provide "...a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment." This may be impractical in most cases. Initial disclosures are not required until after the pre-trial conference and parties have a right to seek a modification of this requirement at the pre-trial conference. See Rule 26(a). As a practical matter you may wish to seek a modification of this requirement as appropriate in each case.

THE RULES PROVIDE A GREAT DEAL OF FLEXIBILITY TO ENCOURAGE THE PARTIES TO AGREE ON METHODS TO PRODUCE ESI; YOU SHOULD TAKE ADVANTAGE OF THESE RULES TO REDUCE YOUR COST. What if relevant data is maintained in a massive proprietary database? Rule 33(d) allows you to respond to interrogatories by offering access to your system under appropriate circumstances. Rule 34(a) allows you to compel access to the other party's system when appropriate to sample, test, or search for relevant information. Rule 34(b) permits parties to designate how they want ESI produced. Opposing parties can object and then propose the manner in which they intend to produce it. A party only has to produce ESI in one form.

IF THE PARTIES CANNOT AGREE ON HOW ESI WILL BE PRODUCED, THEN IT MUST BE PRODUCED IN ITS NATIVE FORMAT OR IN A FORM THAT IS "REASONABLY USABLE." Rule 34(b) states that "...if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable." Based upon the Committee comments to this Rule and prior case law, some commentators interpret it to prohibit production of static images of ESI (i.e., .TIFF, .PDF) or printouts of ESI because such formats are not as usable as the native format. For example, emails may have to be produced electronically in the Outlook format to preserve Outlook's search and sort features, and Excel spreadsheets must be produced electronically with all formulas accessible.

A PARTY DOES NOT HAVE TO INITIALLY PRODUCE ESI THAT IS NOT "REASONABLY ACCESSIBLE" BUT MUST DISCLOSE THAT IT EXISTS AND MAY BE COMPELLED TO PRODUCE IT BY COURT ORDER. Rule 26(b)(2)(B) states:

A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably

accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Rule 26(b)(2)(C) sets out a multi-factor balancing test to determine whether the party must produce the documents and allows the court to shift costs. However, you should know that the courts have been very inconsistent and less likely to shift costs than one might expect.

What is “not reasonably accessible”? A common example is back-up tapes used for disaster recovery purposes because there is considerable cost involved in finding and restoring relevant data. Other examples may include deleted data that has not been overwritten and data on “legacy” programs where the party no longer has the program needed to read the data.

Note: Just because you may not have to *produce* inaccessible ESI does not mean you are relieved of your obligation to *preserve* it. Your preservation obligation is much broader and includes relevant ESI that is not reasonably accessible.

DO NOT TAKE TOO MUCH COMFORT IN THE RULE 37(f) “SAFE HARBOR.”

Rule 37(f) was purportedly drafted to be a “safe harbor” to protect parties from the inadvertent destruction of ESI through routine computer operations:

“Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”

However, in reality, this is a watered down version of earlier proposals. The key phrase is “good-faith operation.” In light of the mandate in existing case law that requires parties to impose an effective litigation hold on ESI when they reasonably anticipate litigation or a government investigation, it is questionable that the continuation of routine destruction of ESI after such time could be done in “good-faith.” More likely, this provision may protect litigants who take all reasonable measures to preserve relevant ESI but lose some anyway due to the operation of routine processes. However this may play out, you do not want to be the test case.

THE BEST WAY TO PROTECT YOURSELF AND REDUCE THE COSTS OF EDISCOVERY IS TO SET UP A WELL-DESIGNED DOCUMENT RETENTION POLICY AND SYSTEM IN THE FIRST PLACE.

In a paper filing system, documents are normally organized in folders and placed in file cabinets, so when relevant documents are requested, one merely has to go to the file cabinet and pull out the specified folders; however, most companies have gotten ahead of themselves by migrating to the electronic transmission and storage of information without setting up a similar electronic filing system or updating their document retention policies to address electronically stored information. As a result, relevant information is organized haphazardly by individual employees and scattered across systems and individuals’ computers. This exponentially

Austin • Collin County • Dallas • Houston • San Antonio • Washington D.C. • Mexico City*

increases the cost of ediscovery. To compound the problem, users continue to labor under the myth that email is private, and therefore, write comments in emails that they would never write in a letter. Spam and other trivial emails can slow down and clog systems and make finding relevant information more expensive and laborious. Data which is deleted may reside in the system indefinitely, creating unnecessary risks and costs in litigation.

EDocument retention systems and policies must be customized to fit each company's specific needs; however, sound policies and systems share some common features:

- Compliance with all laws requiring retention of documents;
- Creation of "electronic file cabinets" to facilitate locating relevant information;
- Distinguishing between "official" documents, which explain how and why decisions are made and should be saved, and "transient" documents, which should be deleted;
- Organized training to change the "reckless" email culture and to train users on what to save and where to save it;
- Automatic deletion of email which is not intentionally saved; and
- System design to cause deleted data to truly be gone as soon as practicable rather than becoming indefinitely stored as scattered bytes of "not reasonable accessible" but discoverable information.

KNOW WHEN TO GET HELP. These new rules require a heretofore rare combination of legal expertise and a detailed knowledge of technology. They also require you to take immediate action when you learn of a potential claim or lawsuit. Strasburger and Price LLP has assembled a team of experienced trial lawyers, paralegals, litigation support staff, and information technology personnel to form the Strasburger eDiscovery and eRetention Team, or eTeam, to assist clients and other firm attorneys on issues regarding the retention, preservation and discovery of ESI. We can assist in all aspects of the process including advising clients how to strategically structure ESI retention policies, how to effectively implement a technology hold, and how to use the new rules to your advantage. We can also work with technology vendors and forensic specialists as needed to meet our clients' needs. Do not hesitate to call us.