ROBINSON BRADSHAW & HINSON

LITIGATION ARTICLE OCTOBER 2006

EDITOR'S NOTE
We appreciate your comments as to how we can make our legal alerts more useful to you. If you would like to see articles on additional topics or would prefer to have our legal alerts sent as a Word or PDF attachment, please contact us at LegalAlerts@rbh.com.

DOCUMENT RETENTION POLICIES UNDER THE AMENDED FEDERAL RULES OF CIVIL PROCEDURE

Author: Lawrence C. Moore, III, lmoore@rbh.com

On December 1, 2006, the amendments to the Federal Rules of Civil Procedure addressing electronic discovery go into effect. Two of those amendments have particular significance for document retention policies: Rule 37(f), which can limit a party's exposure to sanctions for the deletion of electronically stored information, and Rule 26(b)(2)(B), which defines a party's responsibility to provide discovery of electronically stored information. Each is considered in turn.

Rule 37(f) The Safe Harbor Provision. As amended, Rule 37(f) provides that "[a]bsent 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." Protection from spoliation sanctions is highly desirable; cases involving draconian penalties are many, including the well-publicized default judgment entered against Morgan Stanley in favor of Ronald Perelman, leading to a $1.45 billion verdict.

Some have suggested that the safe harbor rule represents a significant change in the law, relieving parties of the need to institute a litigation hold to preserve electronic information when a lawsuit or investigation is filed or reasonably foreseen. However, the Note to the Rule states that "[g]ood faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features … to prevent the loss of information, if that information is subject to a preservation obligation." The Note explicitly refers to such intervention as a "litigation hold." The amended Rule therefore does not alter the duty to preserve files that may be relevant to a pending case, and any document retention policy or procedure therefore must provide for a litigation hold procedure to suspend the deletion of files in the event that litigation is foreseen.

The protection offered by the new provision is limited. The safe harbor applies only the "routine" operation of "an electronic information system." Although the term "system" is not defined, it seems to apply only to automated procedures. The Note accompanying the Rule refers only to computer system, and gives as an example "the alteration and overwriting

of information, often without the operator's specific direction or awareness." The provision therefore does not apply to the decision by an employee to delete a file. Accordingly, document retention policies should be automated to the greatest extent possible. Email is usually the greatest source of discoverable information; most email programs can be set to delete messages automatically after a given period of time. Document management software can be employed for other file types, assigning a retention period to a file at its creation, and automatically deleting it when that period is reached.

The capabilities of computer systems vary, but the implication of the rule is clear: to afford protection from spoliation sanctions, the deletion of electronic files should be (i) automatic, and (ii) subject to suspension.

Rule 26(b)(2)(B) and Reasonable Accessibility. Rule 26(b)(2)(B), as amended, provides that "[a] party need not provide discovery of electronically stored information that the party identifies as not reasonably accessible because of undue burden or cost." On a motion to compel, the burden is on the party resisting production to show that the sources of EIS are not reasonably accessible. Even if the court accepts that the files in question are not reasonably accessible, it "may nonetheless order discovery from such sources if the requesting party shows good cause." However, the court may specify conditions under which such files are produced, including shifting the cost of retrieving difficult-to-access files to the requesting party.

The rules do not define "reasonably accessible." Courts are likely to turn to the influential case *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 318-19 (S.D.N.Y. 2003) to flesh out the terms. Although the context was different, *Zubulake* described electronic file types as falling into five categories—the first three characterized as "accessible":

(1) active, on-line data (such as on hard drives or network servers)
(2) near-line (such as robotic libraries of cds or dvds)
(3) offline storage/archives

And two more as "inaccessible:"

(4) backup tapes
(5) erased, damaged, or fragmented data (recoverable after significant processing).

Back-up tapes are frequently responsible for the most difficulty and expense in electronic production. (They figured prominently in the sanctions against Morgan Stanley.) If the *Zubulake* analysis applies, such tapes should be considered "inaccessible," and the burden of searching them should not fall on the producing party. However, the Sedona Conference, a group of academics, judges, and attorneys whose materials on electronic discovery are widely cited, has laid down as a principal that the producing party should bear the expense of producing electronic files that are "reasonably available in the ordinary course of business." THE SEDONA GUIDELINES: *Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*, Principle 13. In other words, whatever documents the company uses in conducting its business are the ones it will have to search and produce, at its own expense, in litigation.

IT departments frequently retain far more backup tapes than are needed for emergency purposes, and use them to recover files when asked—understandably, they like to be able to come through on such requests. But if the company has a practice of resorting to backup tapes during the ordinary course of its business (regardless of what its written policy is), then under the new rules it will likely be required to restore and search those tapes during discovery, at enormous expense.

Accordingly, any files that are difficult or expensive to retrieve—in particular, files on back-up tapes—should *not* be used in the ordinary course of the business. The lesson from amended Rule 26 is that backup tapes should be maintained as "inaccessible""—that is, to restore an entire server in an emergency situation, and for nothing else. The corollary to that rule is that only those tapes needed for such an emergency should be retained, and all others should be recycled (subject to a litigation hold).

Further, because Rule 26(b)(2)(B) provides that a court may order the production of files that are not reasonably accessible, it follows that the parties must preserve those files. In other words, just because the tapes need not be searched without court order does not mean they need not be retained. The litigation hold procedure in a document retention policy should therefore apply to potentially relevant back-up tapes as well.
