Electronic Discovery: Be Careful of What You Delete

By Thomas J. Shroyer

Thomas J. Shroyer counsels and advocates for clients on a wide range of legal issues and is certified by the Minnesota State Bar Association as a Civil Trial Specialist. He can be reached at ShroyerT@moss-barnett.com or 612.877.5281.

Trial lawyers have always pursued the other side's "smoking guns" through investigation and court discovery procedures. Before the digital age, this quest often led to the organization, production, and inspection of reams and reams of paper ("box car discovery"). Indeed, one of my first assignments as a lawyer was to spend months in a warehouse in San Jose, California, reading and organizing millions of pages of literally moldy and disintegrating business records in a cold storage warehouse in what proved to be a futile search for evidence of fraud.

Today, document discovery infrequently requires extensive travel or time out of the office, as information is increasingly and exclusively stored electronically, and even hard copy documents are efficiently and effectively scanned into electronic media for examination on CD, hard drive, or through an application software provider on the internet. Electronic key word and subject matter searches have also replaced the laborious and extraordinarily costly process of human inspection of each scrap of paper. The digital age, however, has come with a price: More and more harmful information is being kept in an ever increasing number of locations and it is virtually impossible to eliminate. Thus, there is even more incentive to search for the proverbial smoking gun, and efforts by clients to discard (or even cover up) harmful information has itself become the focus of scrutiny.

Invoking the old adage that the lie to cover up is far worse than the underlying crime, trial attorneys now routinely search electronic databases for evidence of tampering or destruction of information. This is because the act of covering up a wrong naturally leads to the conclusion that the underlying act was reprehensible and because our courts have recently imposed draconian sanctions on parties caught hiding, altering, or destroying electronic and other information. Perhaps the most high profile such case involved the prosecution of Arthur Andersen in the wake of Enron's collapse. A year ago, a federal judge assessed liability and punitive damages against parties alleged to be responsible for the failure of Sunbeam Corporation – without a trial – based solely upon the efforts of the defendants to hide or destroy evidence.

Clients are sometimes tempted to think that by hitting the "delete" button, they eliminate potentially incriminating evidence, such as email. The fact is that the delete function merely hides the data on a relatively inaccessible part of the hard drive, leaving it fully exposed to routine forensic examination. Even the application of sophisticated, national security quality "scrubbing" software programs leaves evidence of its application, and state-of-the-art forensic software can often reconstruct virtually all of the purportedly scrubbed information. Further, laypersons often forget that their PDAs (*e.g.*, Blackberry, Treo) retain email on their drives – even after they are officially "deleted." Attorneys and investigators now routinely request the production of PDAs for forensic examination.

The federal courts have now offered some guidance to parties and their attorneys, in the form of new rules of discovery that took effect on December 1, 2006. While the new rules hold much technical interest for lawyers, the key points for clients are:

- A party who does not retain electronically stored information due to the "routine, good faith operation of an electronic information system" may not be assessed with court sanctions unless "exceptional circumstances" are present.

Continues on page 5

Continued from page 4

Electronic Discovery: Be Careful of What You Delete

- A "litigation hold" needs to be placed on information that would normally be lost due to the "routine operation" of an electronic information system as soon as a party is aware of pending or "reasonably anticipated litigation."

As a practical matter, the new rule means that clients should have an internally adopted policy governing the backup, storage, and retention (or loss) of electronically stored information in the ordinary course of business operations. That policy should include a clear mandate to "lock down" all information pertinent or likely to be pertinent to the subject matter of a reasonably anticipated or just commenced lawsuit. It almost (but not quite) goes without saying that these policies must be strictly and consistently followed. While it would be tempting to suggest that these protocols are limited to federal court lawsuits, history shows that courts of virtually all states quickly follow suit in adopting the federal rules of court procedure.

The new federal rules governing electronically stored information reflect both the increasing importance of that information and the need to more closely regulate the storage and production of that information for court proceedings. While the new rules themselves will doubtless occasion controversy and more jurisprudence, they are a useful first step toward the governance of this increasingly important focal point of modern litigation.