KANSAS CITY BUSINESS JOURNAL

VOL. 25, NO. 4 kansascity.bizjournals.com OCTOBER 6-12, 2006

GROWTH STRATEGIES

Federal courts will alter production of electronic evidence

BY CHRIS GRENZ | STAFF WRITER

DAVE KAUP | KCBJ

Madeleine McDonough, a partner at Shook Hardy & Bacon LLP, says some companies could "really be caught by surprise."

The federal court system is booting up sweeping changes to how it treats electronic documents that could have far-reaching — and costly — consequences for companies that fail to comply and could catch unprepared businesses and lawyers off guard.

The rule changes will formalize practices related to data stored on computers and backup systems, including database files, word processing documents and e-mail. The rules will take effect Dec. 1, barring unlikely congressional action to stop them.

Current practices have evolved through a series of court rulings that have created a patchwork of informal rules of thumb that lawyers said sometimes differ from one judge to the next.

The changes have shortened deadlines to produce data, moved up key duties related to electronic document disclosure to the beginning of a lawsuit and delineated more clearly the requirements to divulge certain data. Lawyers and companies will be under the gun to quickly and efficiently produce a broad range of electronic data, sometimes within weeks of a case being filed.

Failure to comply could be costly. When companies fail to produce required electronic documents, judges will be free to give juries "adverse inference" instructions — essentially telling jurors they can assume the companies failed to produce the documents because of intentional fraud. In one key case that spurred the changes, Morgan Stanley was fined $1.45 billion, half of which was punitive, in May 2005 after a judge ruled that it had failed to preserve pertinent information and gave jurors the adverse inference instructions.

"These rule changes are pretty significant," said Jim Ward, of counsel with Kansas City-based Rasmussen Willis Dickey & Moore LLC.

"The bottom line is: If a company's IT people and their in-house lawyers aren't on top of their data system, then they're way behind the curve, and they're going to be scrambling to respond to a discovery request with these rules."

The rules relate to electronic discovery, "e-discovery" for short. Discovery is the period of a lawsuit before trial during which opposing sides gather relevant documents, information and depositions. The new policies fine-tune how and when electronic information must be produced and require parties to identify potential obstacles in producing the data, including excessive cost.

"A big purpose is to get the parties focused on it and not just sort of pour this huge problem into the lap of the court," Ward said. "If you don't deal with it upfront, it could spiral out of control, and the parties would be running to the court and saying, 'We have this huge problem.' This puts the burden on the parties."

Ward, a business litigator who mostly defends insurance companies, said even companies not expecting to face a lawsuit anytime soon should be working now to prepare. The new compressed schedules and deadline pressures don't allow for much of a learning curve.

"This sounds a bit dramatic, but it really becomes a race against the clock (after a suit is filed)," he said. "At this stage of the game, anybody who's not either ready or positioning themselves and working to get ready is facing a pretty serious risk."

Although the changes pertain only to federal court, area lawyers said it's probably only a matter of time before most state and local courts adopt similar rules. The changes mean lawyers will have to be intimately familiar with clients' electronic archiving systems.

"Large companies and extra-large companies have been doing this for a long time," said Madeleine McDonough, a partner with Shook

DISCOVERY: 'A pretty serious risk'

Hardy & Bacon LLP. "What's different now is that medium-sized and small companies are having to take care of this."

McDonough, a litigator who concentrates mostly on defending pharmaceutical and medical device manufacturers, recently moderated a Shook-sponsored panel discussion about the changes.

"We had over 350 people at our seminar, and many were lawyers from small companies who said: 'I have to tell you, I haven't done any of this. I've never talked to IT,'" she said. "There are just a lot of companies that are not tuning in to the fact that these rules are changing. They could really be caught by surprise."

Some lawyers said they think the new rules go a long way toward evening the playing field when an individual or small company sues a big corporation. Rich McLeod of Kansas City law firm McLeod & Heinrichs has been a civil litigator for 27 years, primarily as a plaintiff's attorney. He said the changes will help prevent large companies from drawing out discovery for months or years until they "wear plaintiffs down."

"Electronic discovery is pretty much a one-way street when it comes to David vs. Goliath litigation," McLeod said. "David doesn't have anything that he cares about hiding or is very hard to access. Goliath has both."

Judges also will be able to decide whether one side of a lawsuit is making overly broad requests for data and information that unfairly burden the other side. Or, if certain data would be exceedingly expensive to produce, a judge can order the side requesting the information to help pay for its recovery.

"Federal judges are going to be able to use common sense about who should get what and who should pay for it," McLeod said. "Overall, the rules will be good for plaintiffs and good for the system."

Defense lawyers also said the rule changes would shift much of their costs to the beginning of a suit's life. But the new rules also add some policies to temper the burden for businesses that have been sued, defense lawyers said. For example, they clarify that a company doesn't waive confidentiality privileges if it accidentally discloses a protected document. And companies can't be penalized for destroying relevant documents if they did so as part of a routine data management policy.

Another element of the new rules requires the disclosure of "metadata," which are bits of hidden information embedded in an electronic file that can reveal its author, when it was created and what changes were made.

"That is somewhat important in word processing, but in a database, where you're putting in numbers that are calculating information for you, it can be critical," said Max Carr-Howard, a partner with Blackwell Sanders Peper Martin LLP. "I've seen several cases in my own practice and elsewhere where smoking guns are revealed because the data is changed at a later date."

Failing to comply with the new rules could bring enormous consequences. A suit against UBS Warburg involving employment discrimination allegations eventually centered on electronic discovery issues. In April 2005, after three years of litigation, a jury awarded the plaintiff more than $29 million in damages. Then came the $1.45 billion Morgan Stanley bombshell.

In both cases, judges gave juries "adverse inference" instructions, raising the possibility of intentional fraud.

"That is a very harsh result," said Rick Bien, chairman of Lathrop & Gage LC's litigation division. "And that should give everyone pause in seriously considering their electronic document retention and deletion policies."

cgrenz@bizjournals.com | 816-421-5900

DISCOVERING E-DISCOVERY

Madeleine McDonough, a partner with Shook Hardy & Bacon LLP, offers tips for companies to consider before changes in federal evidentiary rules pertaining to electronic documents take effect Dec. 1:

- **Develop** a document-retention policy. A simple policy might say, "The company will retain any documents that have a business, legal or regulatory purpose; all others will be destroyed."
- **Communicate** the policy to employees, and make sure they know what can and cannot be saved to or deleted from their computer hard drives, a company server or taken home on a company laptop or transferred to a home computer. Because the policy must be meaningfully enforced, offer regular training about the policy, and require employees to acknowledge, in writing, that they've received it.
- **Follow** the policy. Make sure business, legal and regulatory papers are not destroyed. The rest, for logistical and legal reasons, should be destroyed in a regular, routine manner.
- **Assemble** a core team responsible for knowing where all documents are stored. The team should include someone from legal, information technology and perhaps a librarian or the person responsible for managing hard copy documents. Ensure that in-house and outside lawyers speak with IT staff so that the lawyers have a clear understanding of how and where electronic data are stored.
- **Save** documents. If a company is sued or reasonably can expect a lawsuit, it cannot destroy any relevant documents.