



## Publications

### How The New Electronic Discovery Rules Affect Your Business

(Labor Letter, February 2007)

Recent changes in the Federal Rules of Civil Procedure will have an enormous impact on employment litigation over the next several years. The changes, which went into effect December 1, 2006, are designed to focus more attention on “e-discovery,” the production of electronic documents in court proceedings. These new rules will be a significant challenge for every employer who faces a lawsuit from now on.

#### The “Paperless” Office

The problem with electronic records is that there is so much of them. Two unique features of electronic communication contribute to its proliferation. First, e mail is easy; in many ways it has replaced the telephone as the preferred method of quick communication. By most estimates, the average American office worker sends or receives 24 e mail messages a day. The sheer volume of information, combined with the tendency of workers to be more candid or careless in such communications quickens the pulse of many a lawyer.

The second thing leading to the explosion in e-mail may be the false notion that it can be deleted. More workers, and certainly more attorneys, are coming to realize that that is not the case. The delete function does not immediately make a message irretrievable; it merely marks the message as available to be overwritten by newer information. A “deleted” e mail may remain available for a significant period of time.

E-mail is not the only type of document subject to discovery. Most documents are created electronically now. The combination of sharing documents, saving previously edited versions, and backing up copies on diskettes and tapes means that a discovery request that used to uncover a single paper document will now produce many.

How many? According to one expert, a single electronic document will be backed up 12 times if the company (as is common) makes monthly tapes of its computer system. If the document is shared with three internal recipients, all three employees’ copies are saved on the monthly tapes, bringing the total number of documents to 40. If the document is a work in progress, with five different drafts reviewed by the three recipients, there are 184 copies floating around somewhere. Combine these with the e mails used to circulate the drafts, and the total number of discoverable items for a single document can top 1,000.

#### What’s Really At Stake Here

Documents are “discoverable” if a party can be compelled to produce them during a lawsuit. The focus of most electronic discovery disputes centers not on the discoverability of the information. The main issue is often who should bear the burden of retrieving data.

Electronically-recorded information can include voice mail messages and files, back-up voice mail files, e mail messages and files, back-up e mail files, deleted e mails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and more. Data retrieval can cost millions. The cost of discovery will depend largely on where these items are stored and how much expert knowledge is required to retrieve them. Then they must be reviewed for relevance and attorney-client privilege or work product claims.

But the cost of compliance may be a drop in the bucket compared to the cost of not complying with court orders and discovery obligations. Most courts hold that the duty to preserve evidence arises when one is placed on notice that documents are relevant in pending or reasonably anticipated litigation. Depending on the severity of a party’s conduct, sanctions available under the Federal Rules include payment of the other side’s fees for cost incurred in the discovery dispute, adverse inferences given to the jury against the party who failed to preserve the records, and dismissal or default judgment of an action particularly if the party destroys evidence in the face of discovery requests or court order to preserve documents.

In 2004, a federal judge issued sanctions totaling \$2.75 million against 11 senior executives of the Phillip Morris Company.

The judge noted that at the initial conference in the case, Philip Morris had been directed to preserve "all documents and other records containing information which could be potentially relevant to the subject matter of this litigation." Despite this direction, she wrote, Philip Morris continued its policy of deleting all e-mail that was 60 days old. The judge, finding it "essential that the corporate and legal community understand that such conduct will not be tolerated," sanctioned the 11 executives \$250,000 each.

The CEO of one company was personally fined \$10,000 for his company's inadequate document retention efforts. In *Danis v. USN Communications, Inc.*, the company had been ordered to preserve certain documents pending a lawsuit. The court said it was "plain that USN made efforts to preserve documents," and in fact had produced a "massive volume of hard copy and electronically stored information." But the court still fined the company's CEO \$10,000, finding that the inadequacies in the document preservation program "resulted in documents being discarded without having been reviewed to determine whether they should have been preserved."

The court remarked that the "obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers." The USN Communications CEO had delegated this obligation to another employee, who "did nothing to ensure that all USN employees who handled documents that might be discoverable were aware of the lawsuit and the need to preserve documents: he held no meetings with employees below the managerial level, and he did not issue any written communications to anyone on the subject."

Perhaps the most high-profile example of sanctions to date came in *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.* A Florida Circuit Court Judge found last year that Morgan Stanley had failed to meet its discovery obligations by "overwriting e-mails contrary to its legal obligations to maintain them in readily accessible form for two years and with knowledge that legal action was threatened."

Later, after Coleman complained of more discovery failures, including failure to timely produce thousands of backup tapes, the judge ruled that certain facts alleged in the complaint would be "deemed established for all purposes in this action." Unable to rebut some of Coleman's allegations, Morgan Stanley lost the case, with the jury awarding Coleman more than \$1.4 billion.

### When Is It Safe To Destroy Documents?

If there is a legitimate reason for routinely destroying documents, courts are probably as likely to recognize that reason in electronic discovery situations as in traditional ones; the new Rules are not an order to retain every piece of electronic information forever. But just as in traditional discovery courts will probably inquire as to the business justification for a document destruction policy. Particularly in light of the new Rules, the question will be when, and why, a business decided to destroy documents.

The time to address e-discovery issues is now. Recently, more and more companies have begun deleting e mails over a certain age, usually 60 or 90 days. E mails that no one has taken affirmative measures to save elsewhere may be automatically deleted from the system. While a new rule provides that discovery sanctions should not be imposed on a responding party for information lost as part of a "routine, good-faith operation of a electronic information system," businesses should be aware that once a party is on notice of a potential lawsuit, automatic-delete policies could have negative consequences if the relevant information is not somehow protected from destruction.

### Protecting Your Company

Electronic discovery issues should be addressed long before a complaint is served. As one judge has observed, "[W]ithout a written electronic document retention policy, it may be difficult to explain, let alone justify, the destruction of electronically-stored information sought in the course of discovery."

What should you do to prepare for e-discovery? A few key points are:

1. Develop document retention policies now. Once litigation begins, you may be too late in drafting such a policy, because the court and opposing counsel may conclude that it was developed to avoid discovery obligations.
2. Talk with IT personnel about the legal implications of these amendments and learn about your electronic data storage systems, including among other topics, the effect of auto-delete programs and the policy or practice on the use and retention of back-up tapes. Many of the cases dealing with e-discovery involve litigants whose computer systems were upgraded during the course of discovery. System upgrades can't be avoided, and they can have a significant impact on e-discovery. Don't undertake a system upgrade without discussing document preservation issues that may arise down the road.
3. Once litigation is reasonably anticipated, work with your counsel, IT department, and if practical and necessary, a reputable electronic discovery company, to preserve information that may be relevant or material to the matter at hand.
4. In working with your counsel, prepare and issue "preservation" or "litigation hold" memoranda to appropriate company personnel, including IT department employees and officers, managers, and in some cases, even to employees whose electronic data may be relevant to the litigation. Once you have developed a document that adequately instructs on what should be preserved, *make sure all the appropriate people know about it and*

*comply.*

Develop a follow-up plan to ensure that everyone affected is in fact complying with these instructions. As one judge explained, "It is no defense that particular employees were not on notice of the duty to preserve evidence or what kinds of evidence were material to the potential litigation."

Failure to preserve information or a failure to produce electronic data when obligated to do so will have severe consequences. Making efforts now to learn your company's computer system, talking over these issues with your IT department and counsel, enacting document retention and destruction policies, and being proactive about preserving data in connection with anticipated litigation, are all steps in the right direction. One of the keys is to do this now, rather than delay and wait for litigation to be on your doorstep.

**Authors:**

[Christine Howard](#)

[Rhonda Wilcox](#)

[<< Return to listing](#)

[Back to web version](#)