

New E-Discovery Rules Take Effect Today

You have to know what information your company is storing and where it's located. And if you think it's going to be too difficult or expensive to find court-requested data, you'll need to prove it.

By [Larry Greenemeier](#)
[InformationWeek](#)

Dec 1, 2006 10:24 AM

The U.S. legal system on Friday made good on its promise to get stricter in compelling companies to produce electronically stored information as evidence in civil court cases. As of Dec. 1, companies and their IT departments must produce information earlier in the litigation process, and if they can't, they'd better be ready to explain why.

If you're not a fan of ambiguously worded legal documents, what follows is an executive summary of the [amended Federal Rules of Civil Procedure](#).

You have to know what information your company is storing and where it's located. If you have a policy governing how long your company stores information before it's purged, be prepared to prove that policy was in effect and enforced before the court's request for information. And if you think it's going to be too difficult or expensive to find court-requested data, you'll need to prove it.

[E-mail](#) has been used as evidence in court cases for years; the amended rules also cover electronic documents, spreadsheets, image and sound files, and [database](#) info. The language is inclusive enough to cover any electronic media developed in the future. The amended rules explicitly state that requested information must be turned over within 120 days after a complaint has been served on a defendant. If this deadline isn't met, it's possible that electronic evidence could be ruled inadmissible. Or in the instance of a defendant sitting on potentially damaging evidence, courts can levy fines and other penalties.

The amended rules are to CIOs what Sarbanes-Oxley was to CFOs, says Riki Fujitani, a former attorney who's now president of IT service provider Hoike. While the rules apply to federal cases, state courts tend to follow the higher courts, he adds.

The courts are showing their understanding that information is much easier to retrieve from modern [storage](#) technologies, while at the same time acknowledging that finding the right information on obsolete media could be just as difficult as digging up a paper [document](#) in a warehouse of filing cabinets.

Noticeably missing in the amended rules are guidelines that quantify what it means for data to be too time-consuming or expensive to produce. The courts prefer to let judges create case-based rules as such cases are tried.

The larger the company, the more likely it's already been subject to requests for electronic discovery. In a survey by Enterprise Strategy Group, 91% of 568 e-mail, database, and [compliance](#) pros at companies with more than 20,000 employees said their organizations had been issued a discovery request for e-mail last year.

One thing that's anything but ambiguous is the legal system's disdain for companies that intentionally destroy electronically stored information. Morgan Stanley in May paid \$15 million to settle Securities and Exchange Commission charges that it destroyed more than 200,000 e-mails and failed to cooperate with SEC investigators looking into Wall Street business practices. As part of the probes, the SEC between 2000 and 2004 asked Morgan Stanley to hand over copies of e-mail it believed to be relevant, but "Morgan Stanley did not [search](#) diligently for [backup](#) tapes containing responsive e-mails until 2005," according to an SEC statement in May.

Electronically stored data is fast becoming more timely and relevant than paper evidence. While the amended rules give the courts the flexibility to determine accessible versus inaccessible data, don't expect much sympathy when judges suspect you may be withholding potentially important evidence. Paul Lewis, director of the data forensics practice of risk analysis firm Protiviti, testified in May 2005 before the rules committee: "If information exists in bits and [bytes](#) on a medium, it's accessible." You must look under every stone to find the truth, Lewis added, not just the stones in plain view.

IT departments will want to use document-management and other systems to give their lawyers specifically what they ask for, rather than mountains of data. Some law firms are charging their clients as much as \$5 per e-mail to evaluate and organize information for a court case, says Hoike's Fujitani.

Courts have over the past six years or so changed their views on the credibility of electronic documents, says Diego Maldonado, senior VP of the government technology group within consulting firm The Newberry Group. "Courts today are more than ready to accept digitized evidence because security has evolved over the past several years with digital signatures and certificates evoking more confidence in the [integrity](#) of data," he says. "The technology itself will actually make these rules enforceable."

While the IT departments of most large companies likely already have some data retention policy in place, "the amended rules really push these requirements down into

the market, making them applicable to companies of any size," says Keith McCall, CTO and co-founder of Exchange e-mail management appliance provider Azaleos.

Despite the amendments, there are still gray areas related to e-discovery. If a company has a policy of destroying data after 36 months, "what happens if information that's older than 36 months and sent out as part of an e-mail resurfaces during a trial?" asks Protiviti's Lewis. The answer is that companies have to consider the chance that any of their data could be requested by the courts at any time.